

The Division Algorithm and the Hilbert Scheme

A thesis presented

by

David Allen Bayer

to

The Department of Mathematics
in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy
in the subject of
Mathematics

Harvard University
Cambridge, Massachusetts

June, 1982

Abstract

In this thesis, a division algorithm is studied, following work of Macaulay, Hironaka, Buchberger, and others, which generalizes row reduction and the euclidean algorithm, in the same way that elimination theory generalizes the determinant and the resultant.

The main result is a cohomological interpretation of the complexity of this algorithm, for a fixed number of variables. This follows from a new result on the vanishing of coherent sheaf cohomology, which generalizes previous work by Gotzmann, and Macaulay.

The Hilbert scheme offers a setting in which results about this algorithm can be understood; this relationship is described.

The theory of the division algorithm is related to the problem of manipulating objects in algebraic geometry by computer. The problem of computing coherent sheaf cohomology is considered, as a guiding example.

Finally, explicit equations are given for the Hilbert scheme.

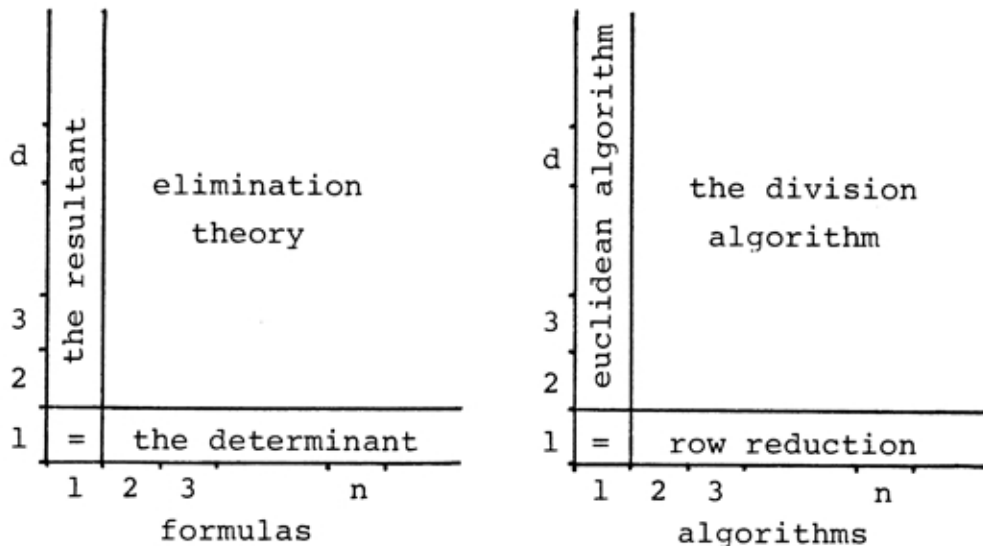
Table of Contents

<u>Introduction</u>	i
<u>Chapter I: The Division Algorithm</u>	1
§1 Multiplicative Orders	1
§2 The Division Algorithm	8
§3 Systems of Polynomial Equations	20
<u>Chapter II: A Vanishing Theorem</u>	27
§1 Hilbert Polynomials	27
§2 m -Regularity	36
§3 Borel Ideals	43
§4 Saturated Ideals	52
§5 The Wild Card Partition	55
§6 m -Regularity of Borel Ideals	63
§7 The Lexicographic Ideal	70
§8 The Extreme Behavior of the Lexicographic Ideal	78
§9 Characteristic Zero Results	85
§10 Characteristic Free Results	93

<u>Chapter III: On the Complexity of the</u>	
<u>Division Algorithm</u>	101
§1 Problems Arising from Algebraic Geometry	101
§2 Problems Arising from Complexity Theory	107
<u>Chapter IV: An Algorithm for Coherent</u>	
<u>Sheaf Cohomology</u>	117
§1 Computing the Saturation of a Submodule	117
§2 Computing the Hilbert Function of a Module	121
§3 Computing Coherent Sheaf Cohomology	126
<u>Chapter V: Orbits of Hilbert Points</u>	129
§1 The Structure of Maximal Torus Orbits	129
<u>Chapter VI: The Hilbert Scheme</u>	134
§1 Equations for the Hilbert Scheme	134
<u>Bibliography</u>	148

Introduction

Suppose that one wants to determine the solvability of a system of inhomogeneous polynomial equations $f_1 = \dots = f_s = 0$, of maximum degree d , in n variables, over an algebraically closed field k . When $d = 1$, the determinant can be used to provide a criterion for solvability. When $n = 1$, one can instead use the resultant. In the intersection of these cases, $d = n = 1$, the two criteria obtained are identical. Elimination theory, described in [vdW50], generalizes these criteria to the case of arbitrary d, n , and has found many applications beyond the specific question of solvability.



If one instead considers the algorithms given by row reduction, and the euclidean algorithm, as criteria for solvability in the cases $d = 1$, $n = 1$, respectively, one again finds that in the overlapping case $d = n = 1$, these

algorithms are identical. This thesis studies the corresponding algorithm for the case of arbitrary d, n , called here the division algorithm, which specializes to row reduction, and the euclidean algorithm.

This theory has been studied in different forms in several streams of work. Macaulay [Mac27] first realized the algebraic significance of ordering the monomials in a polynomial ring, and inspired in particular the subsequent work [Got78], [Sta78], [DEP82]. Hironaka [Hir64] developed a division procedure as part of his proof of the resolution of singularities in characteristic zero, which is isolated as an object of study in the subsequent work [Bri73], [Gal79], [Sch80]. Buchberger [Buc70], [Buc79] independently studied this division procedure, and is responsible for making it computationally effective as an algorithm. His work has been followed by the work [Spe77], [Tri78], [Zac78], [Mor81], [PoY81].

We give a unified presentation of the division algorithm, incorporating the points of view of each of the above schools. The technique of row reduction is ubiquitous in settings where linear equations are found. This author believes that the division algorithm, and the associated ideas of algebraic geometry, could become as ubiquitous in settings involving polynomial equations, if its fundamental role is recognized.

The main theoretical contribution of this thesis is a cohomological interpretation of the complexity of the

division algorithm, in the setting of interest in algebraic geometry. We give a vanishing theorem for coherent sheaf cohomology, which generalizes a result given by Gotzmann [Got78] in the case of ideal sheaves. From this result, and a generalization of related machinery contained in Macaulay's original work [Mac27], the termination of the division algorithm is related to the structure of the zero locus of its input polynomials. The bound obtained is often exact.

A motivation behind this work is the author's desire to computerize the study of examples in parts of algebraic geometry. Specifically, given a projective space P^n over the field k , objects in the categories either of subschemes $X \subset P^n$, or coherent sheaves F on P^n , can be represented by exact sequences

$$0 \longrightarrow I \longrightarrow M \longrightarrow F \longrightarrow 0,$$

where M is a free \mathcal{O}_P -module. Thus, these objects admit concise, finite descriptions which are amenable to computer manipulation. The division algorithm provides a uniform tool for carrying out a wide range of constructions on these objects. The most fundamental one is the calculation of free resolutions. The cohomological interpretation of the division algorithm's complexity has a practical application here: it indicates how prior knowledge of the structure of the input objects can be used to yield significant savings in computation.

The Hilbert scheme is a parameter space for the possible zero sets in P^n with a given set of integer invariants; see [Har66]. Many of the results given in this thesis can be understood as statements about the structure of the Hilbert scheme. In the other direction, this point of view has motivated many of the ideas presented here. We indicate this relationship between the division algorithm and the Hilbert scheme.

Chapter I develops the division algorithm. Some familiarity with commutative algebra is assumed, as can be found in [AtM69], but little algebraic geometry is needed.

Chapter II contains the main technical work. The results of Macaulay [Mac26], Gotzmann [Got78], and this author are uniformly derived as consequences of the characteristic zero theory of ideals fixed by the Borel subgroup of the special linear group, which is developed here. Many previous arguments relied on specializing from arbitrary ideals to monomial ideals, yet monomial ideals can be unwieldy to work with. In terms of the Hilbert scheme, one might as well specialize as far as possible when using specialization arguments; the Borel ideals described above are geometrically the most special points on the Hilbert scheme. This was the starting point for Hartshorne's proof of the connectedness of the Hilbert scheme [Har66]. We first obtain our results for Borel ideals, taking advantage of their combinatorial simplicity, and then lift these

results to the general setting, in arbitrary characteristic. A familiarity with algebraic geometry on the level of [Har77] is assumed; other results are developed as needed.

Chapter III consists of two parts. In the first, we apply the machinery of chapter II to determining the complexity of the division algorithm on inputs arising from algebraic geometry. The second part discusses relationships with complexity theory, when the number of variables is arbitrary. This section is self-contained, and speculative.

The rest of this thesis is quite sketchy, and is included primarily to provide the reader with a context for the preceding theory. Chapter IV describes an algorithm for computing ranks of coherent sheaf cohomology groups. Chapter V describes the relationship between the division algorithm and the Hilbert scheme. Chapter VI gives explicit equations for the Hilbert scheme, providing a different application of the theory developed in chapter II.

Acknowledgements

Lauren Naslund typed this thesis. Her contribution to its realization is greatly appreciated.

I want to thank my family, friends, and roommates for their continual support and encouragement.

I am indebted to James W. England, who was my undergraduate mathematical advisor, and to Herbert S. Wilf, who first introduced me to mathematical algorithms, while I was at Swarthmore.

I want to thank Bob Friedman, Ed Griffin, Tony Iarrobino, Amnon Neeman, Michael Rabin, Frank Schreyer, Joe Silverman, Gail Zacharias, and my other colleagues at Harvard, for many helpful conversations.

Discussions with Ian Morrison played a pivotal role in the development of this work, as indicated in chapter V. I am grateful for his permission to indicate here the point of view arising from these discussions. Similarly, a collaboration with Michael Stillman, seeking a computer implementation of the division algorithm, has influenced this thesis in many ways. Chapter IV owes much to him, and will appear in final form as joint work.

I greatly appreciate the mathematical guidance, and friendship, that David Eisenbud has provided me this year.

I owe much to David Mumford for his continual mathematical support, and friendship. His encouragement

of the goal to actively involve computers in algebraic geometry is particularly appreciated.

Finally, I want to thank my advisor, Heisuke Hironaka, for teaching me algebraic geometry, for showing me much patience, energy, and friendship throughout my graduate studies, and for his continual guidance and encouragement of this work.

Chapter I

The Division Algorithm

§1 Multiplicative Orders

(1.1) Let Q, Z, N, N_+ denote the rationals, integers, nonnegative integers, and positive integers, respectively.

Let k be a field, and let $A = k[x_1, \dots, x_n]$ be the polynomial ring in n variables over k . Associate N^n with the monomials of A by associating $w \in N^n$ with $x^w \in A$.

Let E^r be the subset of N^r consisting of the r vectors $e_1 = (1, 0, \dots, 0), \dots, e_r = (0, \dots, 0, 1)$. Let M be the free A -module $A^r = \bigoplus_{i=1}^r Ae_i$. Then the elements of $N^n \times E^r$ can be associated with a k -basis for M , which will be called the monomials of M .

$N^n \times E^r$ inherits a natural partial order from N^{n+r} : if $u = (u_1, \dots, u_{n+r})$ and $v = (v_1, \dots, v_{n+r})$, then $u > v$ if $u_i \geq v_i$ for $i = 1$ to $n+r$, with strict inequality for at least one i .

Corresponding to the action of A on M there is a natural action of N^n on $N^n \times E^r$, which will be written multiplicatively. It is given by $w(u \times e_i) = (w+u) \times e_i$, for $w \in N^n$ and $u \times e_i \in N^n \times E^r$.

Definition: A multiplicative order $>$ on M is a total order on $N^n \times E^r$ such that

(a) $>$ refines the natural partial order on $N^n \times E^r$;

(b) for all $u, v \in N^n \times E^r$, the order relation $u > v$ only depends on the difference $u - v \in Z^{n+r}$.

Condition (b) implies in particular that for all $w \in N^n$ and $u, v \in N^n \times E^r$, $u > v$ if and only if $wu > wv$. This will be referred to as the multiplicative property of $>$.

(1.2) Definition: The lexicographic order $>_{\text{lex}}$ on M is defined, for $u \times e_i, v \times e_j \in N^n \times E^r$ where $u = (u_1, \dots, u_n)$ and $v = (v_1, \dots, v_n)$, by $u \times e_i >_{\text{lex}} v \times e_j$ if

(a) $i < j$, or

(b) $i = j$, and for some s , $u_1 = v_1, \dots, u_{s-1} = v_{s-1}$,

but $u_s > v_s$.

The lexicographic order is clearly a multiplicative order, so multiplicative orders exist for any M .

Let $A = k[x, y, z]$, and let $M = A^2$, with A -basis e_1, e_2 . Then the following monomials of M are listed lexicographically:

$$\begin{aligned} & x^3 y^2 z^8 e_1, \quad x^3 y^2 z e_1, \quad x^3 y z^9 e_1, \\ & x z^6 e_1, \quad x e_1, \quad y^3 z e_1, \quad z^4 e_1, \quad e_1, \quad x^3 e_2, \\ & x y z^2 e_2, \quad y^3 z e_2, \quad z^5 e_2, \quad z e_2, \quad e_2. \end{aligned}$$

(1.3) Fix a multiplicative order $>$ on M .

Definition: The initial form $\text{in}(m)$ of an element $m \in M$ is the greatest term of m with respect to $>$. The leading exponent $\text{exp}(m)$ of m is the underlying monomial in $N^n \times E^r$ of $\text{in}(m)$. Specifically, if $m = \sum a_i u_i$, with $u_i \in N^n \times E^r$ and nonzero $a_i \in k$, such that $u_1 > u_i$ for each $i > 1$, then $\text{in}(m) = a_1 u_1$ and $\text{exp}(m) = u_1$.

The module $\text{in}(I)$ of initial forms of a submodule $I \subset M$ is the submodule of M generated by all initial forms $\text{in}(m)$ of elements $m \in M$.

Thus a multiplicative order $>$ associates with each submodule $I \subset M$ a submodule $\text{in}(I) \subset M$ generated by monomials in M .

Let $A = \mathbb{C}[x, y, z]$, and let $M = A^2$, with A -basis e_1, e_2 . Then under $>_{\text{lex}}$,

$$\text{in}(3x^2e_1 + yze_1) = 3x^2e_1;$$

$$\text{in}(2e_1 + x^2e_2 + e_2) = 2e_1;$$

$$\text{in}(4ye_2 + z^4e_2) = 4ye_2.$$

(1.4) Example: Let $A = k[x, y, z]$, and let $M = A$. Take $>_{\text{lex}}$ as multiplicative order. If

$$I = (x^2, xy, xz + y^2),$$

then

$$\text{in}(I) = (x^2, xy, xz, y^3).$$

y^3 is the initial form of $y(xz+y^2)-z(xy)$. Thus, the initial forms of a generating set for I need not generate $\text{in}(I)$.

(1.5) Each element $d \in \mathbb{N}_+^n \times \mathbb{Z}^r$ induces a grading on M , by assigning to each $u \in \mathbb{N}^n \times \mathbb{E}^r$ the degree $d \cdot u$. Let I be generated by homogeneous elements with respect to d . The Hilbert function $f : \mathbb{Z} \rightarrow \mathbb{N}$ of I is defined by $f(z) = \dim(I)_z$, where $(I)_z$ is the k -vector space of degree z elements of I .

The following result is due to Macaulay [Mac27]:

Proposition: Let I, d be as above. Then I and $\text{in}(I)$ have the same Hilbert function f .

Proof. Every monomial in $\text{in}(I)$ is itself an initial form of some element of I : if $u = \text{in}(m)$ for some $m \in M$, then $wu = \text{in}(x^w m)$ for each $w \in \mathbb{N}^n$, by the multiplicative property of in .

Choose a k -basis for $(I)_z$ so no two elements have initial forms a scalar multiple of one another. Then the initial form of any element of $(I)_z$ is a scalar multiple of one of the initial forms of this k -basis, so $(I)_z$ and $\text{in}(I)_z$ have the same dimension, for each integer z . \square

In (1.4), if M is graded by $d = (1,1,1) \times 0$, then I is homogeneous, and both I and $\text{in}(I)$ have the Hilbert function

$$f(z) = \binom{z+2}{2} - 3, \quad z \geq 2;$$

0, otherwise.

(1.6) Proposition: A multiplicative order $>$ on M is a well-ordering of $N^n \times E^r$.

Proof. If not, then there exists an infinite sequence of $u_i \in N^n \times E^r$, so $u_i > u_{i+1}$ for each $i \in N_+$. No u_i is a multiple of a previous u_j , $j < i$, since $>$ refines the natural partial order on $N^n \times E^r$. Thus the submodule of M generated by all the u_i requires infinitely many generators. This is impossible, since M is noetherian. \square

(1.7) Let $>$ be a multiplicative order on M , and define the subset $B \subset Z^{n+r}$ by

$$B = \{ u-v \mid u, v \in N^n \times E^r \text{ and } u > v \}.$$

The order $>$ is determined by this set B .

Lemma: No equation $\sum n_i b_i = (0, \dots, 0)$ is possible for $n_i \in N_+$ and $b_i \in B$.

Proof. By allowing repetitions among the b_i , assume that all $n_i = 1$. Let $p_2 : Z^n \times Z^r \rightarrow Z^r$ be the second projection.

Associate a directed graph G to the equation $\Sigma b_i = \vec{0}$, with vertex set E^r , and an edge from e_{j_1} to e_{j_2} for each b_i with $p_2(b_i) = e_{j_2} - e_{j_1}$. For each vertex of G , the indegree equals the outdegree, since $\Sigma b_i = \vec{0}$. Thus the edge set of G is a disjoint union of directed cycles. We reduce G to the graph on E^r with no edges, by replacing in the sum each set $\{b_i\}$ forming a cycle by a single b_i with $p_2(b_i) = \vec{0}$:

Let b_1, \dots, b_s be such a cycle, so for indices $j_1, \dots, j_s, j_{s+1} = j_1$ and $i = 1$ to s , each $p_2(b_i) = e_{j_{i+1}} - e_{j_i}$. Choose $u_1 \in N^n \times E^r$ with

$p_2(u_1) = e_{j_1}$, so if u_i is defined inductively by

$u_i = u_{i-1} + b_{i-1}$ for $i = 2$ to $s+1$, then each

$u_i \in N^n \times E^r$. By construction, $u_{s+1} > \dots > u_1$, so

$u_{s+1} - u_1 = \sum_{i=1}^s b_i \in B$. Also, $p_2(u_{s+1} - u_1) = \vec{0}$. Replace

the cycle b_1, \dots, b_s by the single element $u_{s+1} - u_1$.

Now, given an equation $\sum_{i=1}^t b_i = \vec{0}$ with

$p_2(b_i) = \vec{0}$ for each i , again choose $u_1 \in N^n \times E^r$ so if

u_i is defined inductively by $u_i = u_{i-1} + b_{i-1}$ for

$i = 2$ to $t+1$, then each $u_i \in N^n \times E^r$. By construction

$u_{t+1} > \dots > u_1$, but $u_{t+1} = u_1$, which is a contradiction. \square

(1.8) Proposition: Let $>$ be a multiplicative order on M , and let U be a finite subset of $N^n \times E^r$. Then

there exists a grading of M given by $d \in N_+^{n+r}$, such that for each $u, v \in U$, $u > v$ if and only if $d \cdot u > d \cdot v$.

Proof. Define $B \subset Z^{n+r}$ as in (1.7) above. Define the finite subset $B_U \subset B$ by

$$B_U = \{ u-v \mid u, v \in U \text{ and } u > v \}.$$

We want to find a d so $d \cdot b > 0$ for each $b \in B_U$.

Adjoin to B_U the elements $(1, 0, \dots, 0) \times \vec{0}$,
 \dots , $(0, \dots, 0, 1) \times \vec{0}$, which belong to B since $>$ refines the natural partial order on $N^n \times E^r$.

Consider the convex hull of B_U in Q^{n+r} . Any equation $\sum q_i b_i = \vec{0}$ with $q_i \in Q$, $q_i \geq 0$, $\sum q_i = 1$, and $b_i \in B_U$ can be reduced to an equation of the form precluded by the lemma, so $\vec{0}$ is not in the convex hull of B_U . Since B_U is finite, we can separate B_U from $\vec{0}$ by some $d \in Z^{n+r}$ so $d \cdot b > 0$ for all $b \in B_U$. Because of the elements adjoined to B_U , d must actually belong to $N_+^n \times Z^r$. Since adding $\vec{0} \times (j, \dots, j)$ to d does not affect any $d \cdot b$, d can in fact be chosen from N_+^{n+r} . \square

(1.9) Example: Consider the multiplicative order $>_{\text{lex}}$. Given a finite subset $U \in N^n \times E^r$, choose $t \in N_+$ which strictly bounds any coordinate of any $u \in U$. Then the grading

$$d = (t^n, \dots, t^2, t^1, rt^{n+1}, \dots, 2t^{n+1}, t^{n+1})$$

induces the same order as $>_{\text{lex}}$ on U .

§2 The Division Algorithm

(2.1) For $u \in N^n \times E^r$, let $N^n u$ denote the set of all multiples wu of u , for $w \in N^n$. Fix a multiplicative order $>$ on the free A -module M .

The following definition is from [Gal79].

Definition: Given p elements m_1, \dots, m_p of M , let $\Delta_1, \dots, \Delta_p, \bar{\Delta}$ denote the following partition of $N^n \times E^r$:

$$\Delta_i = N^n \exp(m_i) \setminus \bigcup_{j < i} \Delta_j, \text{ for } i = 1 \text{ to } p;$$

$$\bar{\Delta} = N^n \times E^r \setminus \bigcup_{i=1}^p \Delta_i.$$

Thus, if $u \in N^n \times E^r$, then $u \in \Delta_i$ for the least i so u is a multiple of $\exp(m_i)$, if such an i exists. Otherwise, $u \in \bar{\Delta}$.

Note that some of the $\Delta_i, \bar{\Delta}$ may be empty. $\bar{\Delta}$ is the complement in $N^n \times E^r$ of the monomial submodule of M generated by $\text{in}(m_1), \dots, \text{in}(m_p)$.

(2.2) The following result is a special case of a result in [Hir64, III7], which is isolated in [Bri73], [Gal79]. It is also implicit in [Buc70], [Buc79].

Proposition: Let $m_1, \dots, m_p \in M$, and define $\Delta_i, \bar{\Delta}$ as above. For each $m \in M$, there exist unique quotients $g_1, \dots, g_p \in A$ and a unique remainder $h \in M$ such that

$$(a) \quad m = g_1 m_1 + \dots + g_p m_p + h;$$

(b) if $g_i = \sum a_j w_j$ with $a_j \in k$ and $w_j \in N^n$,
then $w_j \exp(m_i) \in \Delta_i$ for each j ;

(c) if $h = \sum a_j u_j$ with $a_j \in k$ and $u_j \in N_n \times E^r$,
then $u_j \in \bar{\Delta}$ for each j .

Proof. The result holds trivially when $m = \vec{0}$. Since $>$ is a well-ordering of $N^n \times E^r$ by proposition (1.6), we can also assume the result for all $n \in M$ with $\exp(m) > \exp(n)$. Write $\text{in}(m) = au$ with $a \in k$ and $u \in N^n \times E^r$.

If $u \in \bar{\Delta}$, let

$$m - \text{in}(m) = g_1 m_1 + \dots + g_p m_p + h$$

be the unique expression for $m - \text{in}(m)$. Then

$$m = g_1 m_1 + \dots + g_p m_p + (h + au)$$

is an expression of the desired form for m .

If $u \in \Delta_i$, then $u = w \exp(m_i)$ for some $w \in N^n$. Write $\text{in}(m_i) = bv$ with $v \in N^n \times E^r$ and nonzero $b \in k$.

Let

$$m - \frac{a}{b} x^w m_i = g_1 m_1 + \dots + g_p m_p + h$$

be the unique expression for $m - \frac{a}{b} x^w m_i$. Then

$$m = g_1 m_1 + \dots + (g_i + \frac{a}{b} x^w) m_i + \dots + g_p m_p + h$$

is an expression of the desired form for m .

In either case, uniqueness follows by induction. \square

We say that the expression $g_1 m_1 + \dots + g_p m_p + h$ is obtained from m by division by m_1, \dots, m_p .

(2.3) Definition: Let m and m_1, \dots, m_p be elements of M . Define the remainder operator R by

$$m \ R \ m_1, \dots, m_p = h$$

where h is the remainder of m with respect to m_1, \dots, m_p given by (2.2).

The proof of (2.2) gives an iterative procedure for computing $m \ R \ m_1, \dots, m_p$. There it is seen to terminate because $>$ well-orders $N^{n \times r}$. One can also see this using (1.8): choose a grading $d \in N_+^{n+r}$ on M so for each i , $\text{in}(m_i)$ is of higher degree than any other term of m_i . Then each step in the computation of $m \ R \ m_1, \dots, m_p$ replaces a term of m by terms of lower degree.

(2.4) The remainder operator R is k -linear in its left argument, with kernel contained in the submodule of M generated by its right arguments. However, this containment can be proper.

Example: Choose the multiplicative order $>_{\text{lex}}$ on

$M = A$, where $A = k[x, y]$. Then

$$\begin{aligned} x^3 y \ R \ x^3, x^2 y - y^3 &= 0, \text{ but} \\ x^3 y \ R \ x^2 y - y^3, x^3 &= xy^2. \end{aligned}$$

Thus, the remainder operator can vary with the order of its right arguments.

Let $I \subset M$ be the submodule generated by x^2y-y^3, x^3 . Then $x^3y \in I$, but $x^3y \notin \langle x^2y-y^3, x^3 \rangle$ is seen above to be nonzero.

(2.5) Definition: A set of generators m_1, \dots, m_p for a submodule $I \subset M$ is a standard basis for I if $\text{in}(m_1), \dots, \text{in}(m_p)$ generate $\text{in}(I)$.

This is the terminology of [Gal79]; these sets are called Gröbner bases in [Buc70].

(2.6) The following result is a continuation of (2.2), from the same sources.

Proposition: Let m_1, \dots, m_p generate the submodule $I \subset M$. Then the following conditions are equivalent:

- (a) m_1, \dots, m_p is a standard basis for I .
- (b) $m \in I \implies m \in \langle m_1, \dots, m_p \rangle$ for every $m \in I$.

Proof. (a) \implies (b) : Consider the quotient A -module M/IM as a k -vector space. M/IM is spanned by the monomials $N^n \times E^r$. A monomial $u \in N^n \times E^r$ is linearly dependent on lower monomials with respect to the well-ordering $>$ if and only if $u = \exp(n)$ for some $n \in I$. Since $\text{in}(m_1), \dots, \text{in}(m_p)$ generate $\text{in}(I)$, $\bar{\Delta}$ is the complement of $\text{in}(I)$ in $N^n \times E^r$. Thus $\bar{\Delta}$ is a k -basis for M/IM . Therefore each element $m \in M$ has a unique expression as a linear combination of monomials in $\bar{\Delta}$, modulo I , which

must be $\vec{0}$ if $m \in I$.

(b) \implies (a): If m_1, \dots, m_p is not a standard basis for I , then for some $m \in I$, $\exp(m) \in \bar{\Delta}$. For this m , $m \notin R \langle m_1, \dots, m_p \rangle$ is nonzero. \square

The proof of (a) \implies (b) above shows that the remainder of $m \in M$ is the same with respect to any standard basis for I . This remainder can be considered to be a well-defined remainder of m with respect to the submodule I .

(2.7) We next strengthen (2.6) to yield an effective criterion for generators m_1, \dots, m_p of the submodule $I \subset M$ to be a standard basis. Let $\text{in}(m_i) = a_i u_i$, with $u_i \in N^n \times E^r$ and nonzero $a_i \in k$. Let $u_i = v_i \times e_{t_i}$, with $v_i \in N^n$ and $e_{t_i} \in E^r$.

Let $v_i \vee v_j$ denote the join of v_i, v_j in the lattice N^n , with coordinates each equal to the maximum of the corresponding coordinates of v_i and v_j .

Consider the pair of initial forms $a_i u_i, a_j u_j$ of m_i, m_j . If $t_i \neq t_j$, then $a_i u_i, a_j u_j$ generate a free submodule of M , and do not have a syzygy. If $t_i = t_j$, then $a_i u_i, a_j u_j$ have the syzygy s_{ij} given by

$$s_{ij} = a_j (v_i \vee v_j - v_i) a_i u_i - a_i (v_i \vee v_j - v_j) a_j u_j.$$

If J is the submodule of M generated by the initial forms $a_1 u_1, \dots, a_p u_p$ of m_1, \dots, m_p , then

$$(*) \quad \bigoplus_{i,j} A s_{ij} \longrightarrow \bigoplus_i A a_i u_i \longrightarrow J \longrightarrow 0$$

is an exact sequence of A -modules. Choose a minimal set $\{s_{ij}\}$ of syzygies so $(*)$ remains exact.

Definition: The syzygy operator S is defined, when $t_i = t_j$, by

$$m_i S m_j = a_j (v_i v_j - v_j) m_i - a_i (v_i v_j - v_j) m_j.$$

When $t_i \neq t_j$, then

$$m_i S m_j = 0.$$

Note that the initial forms of the two expressions on the right cancel each other, in the first case.

(2.8) Consider the order $>_{lex}$ on $M = A = k[x,y,z]$.

Then

$$\begin{aligned} xy^2 S x^2 y &= 0; \\ xy^{2+1} S x^2 y &= x; \\ xz+y^2 S xy &= y^3. \end{aligned}$$

Compare the last equation with (1.4).

(2.9) The following result is due to Buchberger [Buc70], [Buc79].

Proposition: In (2.6), conditions (a), (b) are each equivalent to

(c) for each pair (i,j) corresponding to a

syzygy in the set $\{s_{ij}\}$, $(m_i \ S \ m_j) \ R \ m_1, \dots, m_p = \vec{0}$.

Proof. (b) \Rightarrow (c): $m_i \ S \ m_j$ belongs to I .

(c) \Rightarrow (b): Suppose that for some $m \in I$, $m \ R \ m_1, \dots, m_p = h$ is nonzero. h is itself an element of I , and can be written as $h = g_1 m_1 + \dots + g_p m_p$ for g_1, \dots, g_p elements of A . Define the height of such an expression to be $\max_i \{\exp(g_i m_i)\}$ with respect to the well-ordering $>$, and choose an expression for h of minimal height.

Let L be the set of indices j so $\exp(g_j m_j) = \max_i \{\exp(g_i m_i)\}$. For each $j \in L$, let w_j be the term of g_j involved in $\exp(g_j m_j)$, so $\text{in}(g_j m_j) = w_j \text{in}(m_j)$. $\sum_{j \in L} w_j \text{in}(m_j) = \vec{0}$, since h is a linear combination of monomials in $\bar{\Delta}$. Thus by the exactness of the sequence (*) of (2.7),

$\sum_{j \in L} w_j \text{in}(m_j) = \sum_{i,j} f_{ij} s_{ij}$ for single terms $f_{ij} \in A$ and syzygies $s_{ij} \in \{s_{ij}\}$. It follows that

$\sum_{j \in L} w_j m_j = \sum_{i,j} f_{ij} (m_i \ S \ m_j)$, considered as expressions in the symbols m_1, \dots, m_p . Since each $m_i \ S \ m_j$ has remainder $\vec{0}$, we can rewrite $\sum_{j \in L} w_j m_j$, and thus

$g_1 m_1 + \dots + g_p m_p$, into an expression of lower height.

Thus no such h can occur. \square

(2.10) Proposition (2.9) gives a constructive procedure for obtaining a standard basis from an arbitrary set $m_1, \dots, m_p \in M$. For each pair (i, j) corresponding to a syzygy in a minimal set of syzygies for $\text{in}(m_1), \dots, \text{in}(m_p)$, calculate

$$(m_i \ S \ m_j) \ R \ m_1, \dots, m_p = h.$$

If h is nonzero, then adjoin $h = m_{p+1}$ to the set m_1, \dots, m_p , extend the minimal set of syzygies, and also check the new pairs $(i, p+1)$.

The following is due to Buchberger [Buc70], [Buc79].

Proposition: The above process terminates.

Proof. If not, then the sequence of monomials $\text{exp}(m_i)$ for $i \in \mathbb{N}_+$ generates a submodule of M requiring infinitely many generators, which is impossible since M is noetherian. \square

When this process terminates, condition (c) of proposition (2.9) is satisfied, and we have constructed a standard basis.

If m_1, \dots, m_p are homogeneous with respect to some grading $d \in \mathbb{N}_+^{n+r}$, then by considering syzygies of lowest degree first, this process will enumerate a minimal generating set for $\text{in}(I)$ as it adjoins remainders. Thus, the complexity of this process is closely connected to understanding the relationship between minimal generating

sets for homogeneous I and $\text{in}(I)$.

The next two propositions reveal a strong relationship between the submodules I and $\text{in}(I)$.

(2.11) The following result was discovered independently by Spear [Spe77], [Zac78], and Schreyer [Sch80].

Proposition: Let m_1, \dots, m_p be a standard basis for the submodule $I \subset M$. Then the syzygies among m_1, \dots, m_p can be explicitly constructed from the syzygies among $\text{in}(m_1), \dots, \text{in}(m_p)$.

Proof. For each syzygy s_{ij} in the set $\{s_{ij}\}$ associated with the exact sequence $(*)$, define the syzygy t_{ij} by

$$t_{ij} = m_i \circ m_j - (g_1 m_1 + \dots + g_p m_p),$$

where $g_1 m_1 + \dots + g_p m_p$ is the expression for $m_i \circ m_j$ obtained by division by m_1, \dots, m_p . $m_i \circ m_j$ has remainder $\vec{0}$ by proposition (2.2), so $t_{ij} = \vec{0}$ taken as an element of M . If $\{t_{ij}\}$ is the set of all t_{ij} obtained in this way, then we want to show that

$$(**) \quad \bigoplus_{i,j} A t_{ij} \longrightarrow \bigoplus_i A m_i \longrightarrow I \longrightarrow 0$$

is an exact sequence of A -modules.

The proof proceeds exactly as in the proof of proposition (2.9). Any expression

$g_1 m_1 + \dots + g_p m_p \in \bigoplus_i A m_i$, which maps to $\vec{0}$ in I , is

equivalent modulo the image of $\bigoplus_{i,j} At_{ij}$ to an expression of lower height. Thus (**) is exact, and $\{t_{ij}\}$ is a set of syzygies for m_1, \dots, m_p . \square

The above result can be used to construct free resolutions. In the graded case, these resolutions are usually not minimal, but can be easily trimmed to yield minimal resolutions.

(2.12) Proposition: Let k be algebraically closed. Let I be a submodule of M . Then $M/\text{in}(I)M$ occurs as the special fiber of a flat family with general fibers all isomorphic to M/IM .

Proof. Let $k[t]$ be the polynomial ring over k in a new variable t , let $A[t] = k[x_1, \dots, x_n, t]$, and let $M[t] = \bigoplus A[t]e_i$. Choose a standard basis m_1, \dots, m_p for each I . By proposition (1.8), choose a grading $d \in \mathbb{N}_+^{n+r}$ on M so for each i , $\text{in}(m_i)$ is of higher degree than any other term of m_i .

For each $m_i = \sum a_j u_j$ with $u_j \in \mathbb{N}^n \times \mathbb{E}^r$ and nonzero $a_j \in k$, let $b = \max_j \{d \cdot u_j\}$ be the degree of $\text{in}(m_i)$, and define $m_i(t) \in M[t]$ by

$$m_i(t) = \sum_j a_j u_j t^{b-d \cdot u_j}.$$

Then $m_i(1) = m_i$ for each i . More generally,

$m_1(c), \dots, m_p(c)$ generates a submodule of M isomorphic to I by a change of coordinates, for nonzero $c \in k$.

$m_1(0), \dots, m_p(0)$ generates the submodule $\text{in}(I) \subset M$, since each $m_i(0) = \text{in}(m_i)$. Let $I(t) \subset M[t]$ denote the submodule generated by $m_1(t), \dots, m_p(t)$.

Extend the multiplicative order on M to a multiplicative order on $M[t]$, by defining $ut^i > vt^j$ for $u, v \in N^{n \times E^r}$ if

- (a) $u > v$, or
- (b) $u = v$, and $i > j$.

Note that t acts as a homogenizing variable of weight one for the grading d , making each $m_i(t)$ homogeneous. Each equation

$$m_i \ S \ m_j = g_1 m_1 + \dots + g_p m_p$$

obtained by division by m_1, \dots, m_p remains valid after homogenizing. Thus,

$$m_i(t) \ S \ m_j(t) = g_1(t)m_1(t) + \dots + g_p(t)m_p(t),$$

where each $g_i(t) \in M[t]$ is defined by the homogenizing process, and satisfies condition (b) of proposition (2.6). Therefore, by (2.6), $m_1(t), \dots, m_p(t)$ is a standard basis for $I(t)$.

$F = M[t]/I(t)M[t]$ is a flat family over $k[t]$, with the properties we seek. It remains to be shown that F is flat. The criterion for flatness we shall use is given in Hartshorne [Har77, III9.1.3]. Since $k[t]$ is a principal ideal domain, a $k[t]$ -module F is flat if no $f(t) \in k[t]$ is a zero divisor in F . Since $k[t]$ is also a unique factorization domain, it suffices to

consider $f(t) = t - c$ with $c \in k$.

Suppose, for $n \in M[t]$ and $c \neq 0$, that $(t-c)n \in I(t)$. Break n into homogeneous parts $n_1 + \dots + n_s$ with respect to d , in degree increments of one. Since $I(t)$ is homogeneous, the homogeneous parts

$$-cn_1, tn_1 - cn_2, \dots, tn_{s-1} - cn_s, tn_s$$

of $(t-c)n$ each belong to $I(t)$. It follows that $n \in I(t)$.

Suppose, for $n \in M[t]$, that $tn \in I(t)$. Then by proposition (2.6),

$$tn = g_1(t)m_1(t) + \dots + g_p(t)m_p(t)$$

with each $g_i(t) \in A[t]$ satisfying condition (b) of proposition (2.2). It follows that each $g_i(t)$ is divisible by t , so $m \in I(t)$. \square

We shall only need this result for k algebraically closed, but it extends easily to arbitrary fields.

§3 Systems of Polynomial Equations

(3.1) Let m_1, \dots, m_p be polynomials in the ring $A = k[x_1, \dots, x_n]$, where k is algebraically closed. Let k^n denote affine n -space over k . We describe an algorithm to

- (a) determine if $m_1 = \dots = m_p = 0$ has a solution $z \in k^n$;
- (b) solve for the coordinates of such solutions $z \in k^n$.

Let M denote the free A -module A^r , as in §2.

Definition: A standard basis $m_1, \dots, m_p \in M$ is reduced if for each $i = 1$ to p ,

- (a) m_i is monic: $\text{in}(m_i) = \exp(m_i)$;
- (b) $m_i \notin \langle m_1, \dots, m_{i-1}, m_{i+1}, \dots, m_p \rangle$.

(3.2) This result is due to Buchberger.

Proposition: For a given multiplicative order $>$ on M , a submodule $I \subset M$ has a unique reduced standard basis.

Proof. Let m_1, \dots, m_q be an arbitrary standard basis for I . Choose from $\text{in}(m_1), \dots, \text{in}(m_q)$ a minimal generating set for $\text{in}(I)$. Throw away each uninvolved m_i , and make the rest monic, leaving a standard basis m_1, \dots, m_p of minimal cardinality. Now replace each m_i by its remainder with respect to $m_1, \dots, m_{i-1}, m_{i+1}, \dots, m_p$.

For each i , no term of m_i except $\exp(m_i)$ belongs to $\text{in}(I)$, since such a term cannot be a multiple of $\text{in}(m_i)$, and by construction is not a multiple of $\text{in}(m_j)$ for $j \neq i$. Thus,

$$m_i = \exp(m_i) - \sum a_j v_j,$$

with $a_j \in k$ and $v_j \in \bar{\Delta}$, where $\bar{\Delta}$ is defined with respect to m_1, \dots, m_p as in §2. Therefore, m_1, \dots, m_p is a reduced standard basis, since each m_i satisfies condition (b) of the definition.

Uniqueness follows from the proof of proposition (2.6), since $\sum a_j v_j$ must be the unique expression for $\exp(m_i)$ as a linear combination of monomials from $\bar{\Delta}$, considered as an element of the quotient M/IM . \square

Together with the results of §2, the above proof gives a constructive procedure for finding the reduced standard basis for $I \subset M$ with respect to $>$, given an arbitrary set of generators for I .

(3.3) Let $M = A$, and thus consider a multiplicative order $>$ defined directly on the polynomial ring A .

Example (row reduction): Suppose that $>$ induces the order $x_1 > x_2 > \dots > x_n$ on the variables of A . Let $m_1, \dots, m_p \in A$ be polynomials consisting only of linear and constant terms. Then the procedures for row reducing m_1, \dots, m_p , and for obtaining a reduced standard basis from m_1, \dots, m_p , are identical.

Example (euclidean algorithm): Let m_1, \dots, m_p be polynomials in $A = k[x_1]$. There is a unique multiplicative order $>$ on A , since the natural order on the monomials N^1 is total. A is a principal ideal domain, so the reduced standard basis obtained from m_1, \dots, m_p will consist of one polynomial, the greatest common divisor of m_1, \dots, m_p . The computation of this reduced standard basis is identical with the euclidean algorithm.

The above examples are special in that they only rely on the operator R . In general, when the m_1, \dots, m_p are of arbitrary degree in $n > 1$ variables, the operator S plays an essential role in constructing standard bases.

(3.4) This result is due to Buchberger [Buc70], [Buc79].

Proposition: Let $m_1, \dots, m_p \in A$ be a reduced standard basis. Then the system of equations $m_1 = \dots = m_p = 0$ has a solution $z \in k^n$ if and only if $\{m_1, \dots, m_p\} \neq \{1\}$.

Proof. $m_1 = \dots = m_p = 0$ has no solutions if and only if m_1, \dots, m_p generate the unit ideal $(1) \in A$. (1) has the unique reduced standard basis $\{1\}$ for any multiplicative order $>$. \square

(3.5) By considering specifically the lexicographic order defined in §1, we can strengthen (3.4). This line of

reasoning was discovered independently by Spear (suggested in [Spe77]), Trinks [Tri78], and this author. See also Pohst and Yun [PoY81].

Proposition: Let $>$ be the lexicographic order on A , and let m_1, \dots, m_p be the corresponding reduced standard basis for the ideal I of A . For $1 \leq s \leq n$, consider the subring $C = k[x_{s+1}, \dots, x_n]$ of A . Then $I \cap C$ is generated as an ideal in C by the m_i contained in C .

Proof. The lexicographic order is uniquely determined as a multiplicative order by the property that for each such C , all of the monomials in $A \setminus C$ are ordered greater than any monomial in C . Thus for any polynomial $m \in A$, we have $m \in C$ if and only if $\text{in}(m) \in C$. Suppose $m \in I \cap C$, and let

$$m = g_1 m_1 + \dots + g_p m_p$$

be the expression for m obtained by division by m_1, \dots, m_p . Since the g_i satisfy condition (b) of proposition (2.6), and $m \in C$, the g_i for which $m_i \notin C$ are zero. Thus the m_i contained in C generate $I \cap C$. \square

(3.6) When $s = n$, so $C = k$, the above result reduces to (3.4).

In general, let $X \subset k^n$ denote the set of solutions to $m_1 = \dots = m_p = 0$. When $s = n-r$, $I \cap C$ is the ideal

of the projection from k^n to k^r of X .

Consider specifically the case $s = n-1$, so $C = k[x_n]$. If $I \cap C = (0)$, then the projection of X to k^1 is Zariski dense. This does not mean that $m_1 = \dots = m_p = 0$ can be solved for an arbitrary value of x_n ; rather, points of X lie above all but finitely many values of x_n . Consider the example $xy - 1 = 0$ in k^2 ; this equation can be solved for every value of y except $y = 0$.

The resolution of this technical difficulty in general is to work in projective space, homogenizing each equation. There, solution sets are proper, so dense projections are onto. In many cases of interest, this difficulty fails to be a problem.

If $I \cap C = C$, then $I = (1)$, and $m_1 = \dots = m_p = 0$ cannot be solved. Otherwise, $I \cap C = (m_j)$ for a unique m_j in the reduced standard basis for I . $m_j \in k[x_n]$, and the roots of m_j are exactly the values of x_n for which $m_1 = \dots = m_p = 0$ can be solved.

If $I \neq (1)$, then let $x_n = a$ be a value for which $m_1 = \dots = m_p = 0$ can be solved. Adjoin the new polynomial $m_{p+1} = x_n - a$, or equivalently make the substitution $x_n = a$, and construct again a reduced standard basis. Iterating, we obtain a solution $z = \vec{a}$ to $m_1 = \dots = m_p = 0$.

We thus have:

Proposition:

Let m_1, \dots, m_p be polynomials in the polynomial ring $k[x_1, \dots, x_n]$ over the algebraically closed field k . Then the process of repeatedly constructing reduced standard bases from m_1, \dots, m_p with respect to the lexicographic order defined in §1, and eliminating variables by admissible substitutions $x_n = a$, will find a solution $z \in k^n$ to $m_1 = \dots = m_p = 0$, or determine that there are none. In principle, any solution can be reached by this algorithm. \square

(3.7) In practice, one cannot work in an algebraically closed field. Thus, to make full use of this algorithm, one must be able to make field extensions as necessary.

See [Rab80] for a discussion of such field operations over finite fields. In characteristic zero, it is proven in [LLL82] that one variable polynomials can be factored over \mathbb{Q} in polynomial time. Susan Landau has extended this result to factorization over algebraic extensions of \mathbb{Q} .

As we shall eventually see, the field operations will not often be the limiting factor in use of this algorithm.

(3.8) Example: Let $>$ be the lexicographic order on $A = \mathbb{Q}[x,y]$, and let

$$m_1 = x^2 + y^2 - 2, \quad m_2 = xy - 1,$$

generate the ideal $I \subset A$. We compute

$$m_3 = (m_1 \text{ S } m_2) \text{ R } m_1, m_2 = x + y^3 - 2y;$$

$$m_4 = m_1 \text{ R } m_3 = y^6 - 4y^4 + 5y^2 - 2;$$

$$m_5 = m_2 \text{ R } m_3 = -y^4 + 2y^2 - 1;$$

$$m_4 \text{ R } m_5 = 0;$$

$$(m_3 \text{ S } m_5) \text{ R } m_3, m_5 = 0.$$

Thus $m_3, -m_5 = x + y^3 - 2y, y^4 - 2y^2 + 1$ is the reduced standard basis for I , with respect to $>$. $y^4 - 2y^2 + 1 = 0$ has the roots $1, 1, -1, -1$. Substituting back into $x + y^3 - 2y = 0$, we find that $m_1 = m_2 = 0$ has the solutions

$$(x,y) = (1,1) \text{ or } (-1,-1),$$

each with multiplicity two.

Chapter II

A Vanishing Theorem

§1 Hilbert Polynomials

(1.1) Let F be a coherent sheaf on P^n . The Hilbert polynomial $p(z)$ of F is defined by

$$p(z) = \chi(F(z)) = \sum_{i=0}^n (-1)^i h^i(F(z)),$$

and we have

$$p(z) = h^0(F(z))$$

for all large degrees z .

We describe a notation for numerical polynomials which facilitates computations, and which will ultimately yield a concise description of which numerical polynomials occur as $\chi(F(z))$ for some coherent sheaf F on P^n .

For background on numerical polynomials, see [Har77,I.7]. We adopt here the notation of [Har66].

(1.2) Definition: $g(m_0, \dots, m_s; z) = \sum_{i=0}^s \binom{z+i}{i+1} - \binom{z+i-m_i}{i+1}.$

For each sequence of integers m_0, \dots, m_s , $g(m_0, \dots, m_s; z)$ is a numerical polynomial in z of degree s , with leading term $(m_s/s!)z^s$.

(1.3) Lemma: Any numerical polynomial $p(z)$ can be expressed as $g(m_0, \dots, m_s; z)$ for unique integers m_0, \dots, m_s , where $m_s \neq 0$.

Proof. Let $p(z)$ be of degree s . $p(z)$ can then be written as

$$p(z) = a_s \binom{z+s}{s} + \dots + a_0 \binom{z+0}{0}$$

for unique integers a_0, \dots, a_s . $\binom{z+s}{s+1} - \binom{z+s-a_s}{s+1}$ has the same leading term $(a_s/s!)z^s$, so its difference with $p(z)$ is a numerical polynomial of lower degree. Setting $m_s = a_s$, the result follows by induction. \square

(1.4) Suppose that each $m_i \geq 0$. Since

$$\binom{z+i}{i+1} - \binom{z+i-m_i}{i+1} = \sum_{j=1}^{m_i} \binom{z+i-j}{i},$$

we can write

$$g(m_0, \dots, m_s; z) = \sum_{\substack{0 < i < s \\ 1 < j < m_i}} \binom{z+i-j}{i}.$$

More generally, let $A = \{a_{ij}\}$ be an array of integers, where $i, j \in \mathbb{N}$, and all but finitely many a_{ij} are zero.

Definition: $g(A; z) = \sum_{i,j} a_{ij} \binom{z+i-j}{i}.$

If $p(z) = g(A; z)$, we can call A a diagram for the polynomial $p(z)$. We say that two diagrams $A = \{a_{ij}\}$, $B = \{b_{ij}\}$ are equivalent, written $A \sim B$, if $g(A; z) \equiv g(B; z)$.

$$\text{Clearly, } g(A+B; z) \equiv g(A; z) + g(B; z).$$

(1.5) Associate the sequence of integers m_0, \dots, m_s , where each $m_i \geq 0$, with the diagram $A = \{a_{ij}\}$ defined by

$$a_{ij} = 1 \quad \text{if } 0 \leq i \leq s \quad \text{and} \quad 1 \leq j \leq m_s;$$

$$0 \quad \text{otherwise.}$$

The definitions for $g(m_0, \dots, m_s; z)$ and $g(A; z)$ then agree as polynomials, by (1.4).

(1.6) Example: Let $X \subset P^3$ be the twisted cubic curve, with Hilbert polynomial $p(z) = 3z+1$. Then $p(z) = g(4,3;z)$. We can picture this polynomial as the following diagram, with zero entries left blank:

$$\begin{array}{c|cccc}
 & 0 & 1 & 2 & 3 & 4 & j \\
\hline
 0 & & 1 & 1 & 1 & 1 & \\
 i & 1 & & 1 & 1 & 1 & \\
 & & & & & & \\
 & & & & & & \\
 & & & & & & \\
 & & & & & & \\
 & & & & & & \\
 & & & & & &
 \end{array}$$

(1.7) Definition: A diagram A is reduced if $a_{ij} = 0$ or $a_{ij} = 1$ for each i, j .

(1.8) Definition: A diagram A is monotonic if there exists integer bounds $m_0 \geq \dots \geq m_s > 0$ so $a_{ij} > 0$ when $1 < j < m_i$, and $a_{ij} = 0$ otherwise.

Example (1.6) is both reduced and monotonic. If A is reduced, and monotonic with bounds $m_0 \geq \dots \geq m_s > 0$, then A is the diagram associated with m_0, \dots, m_s , as in (1.5).

(1.9) Lemma: The following diagrams A have $h(A; z) \equiv 0$, for any choice of u, v :

$$\begin{aligned}
 \text{(a)} \quad & a_{uv} = -1; a_{u-1,v} = a_{u,v+1} = 1; \\
 & a_{ij} = 0 \text{ otherwise.}
 \end{aligned}$$

$$(b) \quad a_{uv} = -1; a_{w,v+1} = 1 \quad \text{for } 0 \leq w \leq u; \\ a_{ij} = 0 \quad \text{otherwise.}$$

Proof. (a) follows from Pascal's identity:

$$\binom{z+1-j}{i} = \binom{z+i-1-j}{i-1} + \binom{z+i-1-j}{i}.$$

(b) follows by repeated application of (a). \square

(1.10) Example: If $u = 2, v = 1$, then lemma (1.9) refers to the following diagrams:

$$(a) \quad \begin{array}{cccc} & & & j \\ & & 0 & 1 & 2 \\ i & 0 & \left| \begin{array}{ccc} & & \\ & & \\ & & \end{array} \right. & & \\ & 1 & & 1 & \\ & 2 & & -1 & 1 \end{array}$$

$$(b) \quad \begin{array}{cccc} & & & j \\ & & 0 & 1 & 2 \\ i & 0 & \left| \begin{array}{ccc} & & 1 \\ & & 1 \\ & & 1 \end{array} \right. & & \\ & 1 & & & 1 \\ & 2 & & -1 & 1 \end{array}$$

Each of these diagrams yields the zero polynomial.

(1.11) Lemma (1.9) can be used to compute equivalences between diagrams, since adding either diagram (1.9a) or (1.9b) to a given diagram corresponds to adding the zero polynomial.

Example: A degree d hypersurface $X \subset P^n$ has Hilbert polynomial

$$p(z) = \binom{z+n}{n} - \binom{z+n-d}{n}.$$

We compute integers m_0, \dots, m_s so

$$p(z) = g(m_0, \dots, m_s; z).$$

By adding a sequence of diagrams first of type (1.9a), then of type (1.9b),

$$\begin{array}{ccc}
 \begin{array}{c} 0 \\ 1 \\ \dots \\ n-1 \\ n \end{array} \left| \begin{array}{cccc} 0 & 1 & & \\ & & d-1 & d \\ & & & \\ & & & \\ & & & \\ 1 & & & -1 \end{array} \right. & \sim & \begin{array}{c} 0 \\ 1 \\ \dots \\ n-1 \\ n \end{array} \left| \begin{array}{cccc} 0 & 1 & & \\ & & d-1 & d \\ & & & \\ & & & \\ & & & \\ 1 & & & -1 \\ & 1 & & -1 \end{array} \right. \\
 \\
 \begin{array}{c} 0 \\ 1 \\ \dots \\ n-1 \\ n \end{array} \left| \begin{array}{cccc} 0 & 1 & & \\ & & d-1 & d \\ & & & \\ & & & \\ & & & \\ 1 & 1 & 1 & 1 \\ & & & \end{array} \right. & \sim & \begin{array}{c} 0 \\ 1 \\ \dots \\ n-1 \\ n \end{array} \left| \begin{array}{cccc} 0 & 1 & & \\ & & d-1 & d \\ & & & 1 \\ & & & 1 \\ & & & 1 \\ 1 & 1 & 1 & 1 \\ & & & \end{array} \right. \\
 \\
 \begin{array}{c} 0 \\ 1 \\ \dots \\ n-1 \\ n \end{array} \left| \begin{array}{cccc} 0 & 1 & & \\ & & d-1 & d \\ & & & 1 \\ & & & 1 \\ & & & 1 \\ 1 & 1 & & 1 \\ & & & \end{array} \right. & \dots \sim & \begin{array}{c} 0 \\ 1 \\ \dots \\ n-1 \\ n \end{array} \left| \begin{array}{cccc} 0 & 1 & & \\ & & d-1 & d \\ & & & 1 \\ & & & 1 \\ & & & 1 \\ 1 & 1 & 1 & 1 \\ & & & \end{array} \right.
 \end{array}$$

Thus, $p(z) = g(m_0, \dots, m_{n-1}; z)$ with
 $m_0 = \dots = m_{n-1} = d.$

(1.12) Lemma: Any monotonic diagram A is equivalent to a reduced monotonic diagram B . If A has bounds $m_0 \geq \dots \geq m_s > 0$, then B has bounds $n_0 \geq \dots \geq n_s > 0$, with $n_i \geq m_i$ for each i .

Proof. Assume that A is reduced for all a_{ij} with $i > r$. By repeated addition of diagrams of type (1.9b) to row r , we can reduce row r while keeping A monotonic. This requires only finitely many steps, since each step leaves the sum of the entries in row r fixed. The sums of the entries in rows $< r$ increase during this process, so the bounds m_i can only increase when we reduce A to B . Repeating this process for each row $r-1, \dots, 0$ yields the result. \square

$$\begin{array}{c}
 \begin{array}{c|ccccc}
 & 0 & 1 & 2 & 3 & 4 \\
 \hline
 0 & & 1 & 1 & 1 & 1 \\
 1 & & 1 & 1 & 1 & \\
 & & 1 & 1 & 1 & \\
 r & & 1 & 2 & & \\
 & & 1 & & &
 \end{array}
 & \sim &
 \begin{array}{c|ccccc}
 & 0 & 1 & 2 & 3 & 4 \\
 \hline
 0 & & 1 & 1 & 2 & 1 \\
 1 & & 1 & 1 & 2 & \\
 & & 1 & 1 & 2 & \\
 r & & 1 & 1 & 1 & \\
 & & 1 & & &
 \end{array}
 \end{array}$$

The above illustrates a step in the proof.

(1.13) Lemma: If $m_0 \geq \dots \geq m_r > 0$, and $n_0 \geq \dots \geq n_s > 0$, with $r \leq s$, then

$$g(m_0, \dots, m_r; z) + g(n_0, \dots, n_s; z) = g(p_0, \dots, p_s; z)$$

with $p_0 \geq \dots \geq p_s > 0$, and $p_i \geq \max\{m_i, n_i\}$ for each i .

Proof. Let A, B be the diagrams corresponding to $m_0 \geq \dots \geq m_r > 0$, $n_0 \geq \dots \geq n_s > 0$, by (1.5). Then $A+B$ is monotonic with bounds $p_0 \geq \dots \geq p_s > 0$, where each $p_i = \max\{m_i, n_i\}$. The result follows by (1.12). \square

(1.14) Lemma: If $m_0 \geq \dots \geq m_s > 0$ and $q \geq 0$, then

$$g(m_0, \dots, m_s; z+q) = g(n_0, \dots, n_s; z)$$

for $n_0 \geq \dots \geq n_s > 0$, with $n_i \geq m_i$ for each i .

Proof. It suffices to show the statement for $q = 1$.

Let A be the diagram corresponding to $m_0 \geq \dots \geq m_s > 0$, by (1.5). Since

$$\binom{(z+1)+i-j}{i} = \binom{z+i-(j-1)}{i},$$

$B = \{b_{ij}\}$ is a diagram corresponding to $g(m_0, \dots, m_s; z+1)$ if we define $b_{ij} = a_{i, j+1}$ for each i, j . Adding diagrams of type (1.9b) for each entry in column 0 of B , we obtain a monotonic diagram, which by (1.12) is equivalent to a reduced monotonic diagram with bounds $n_0 \geq \dots \geq n_s > 0$. Since the sum of the entries in each row can only increase throughout this process, we must have $n_i \geq m_i$ for each i . \square

$$\begin{array}{c} \begin{array}{c|ccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 1 & 1 & 1 & \\ 1 & 1 & 1 & 1 & \\ 2 & 1 & 1 & & \end{array} \\ \sim \\ \begin{array}{c|ccc} & 0 & 1 & 2 & 3 \\ \hline 0 & & 4 & 1 & \\ 1 & & 3 & 1 & \\ 2 & & 2 & & \end{array} \end{array}$$

The above illustrates a step in the proof.

Note that $g(d, \dots, d; z-1)$ cannot be written in the desired form, so $q \geq 0$ is a necessary hypothesis.

(1.15) Example: Let $S = k[x_0, \dots, x_n]$, and let $I \subset S$ be the zero ideal $I = (0)$. Then the Hilbert polynomial of S/I is

$$p(z) = \binom{z+n}{n}.$$

Applying (1.9b), we obtain the equivalence of diagrams

$$\begin{array}{c} 0 \quad 1 \quad 2 \\ \left| \begin{array}{ccc} & & \\ & & \\ & & \\ 1 & & \\ & & \\ n & 1 & \end{array} \right. \end{array} \sim \begin{array}{c} 0 \quad 1 \quad 2 \\ \left| \begin{array}{ccc} & & \\ & 1 & \\ & 1 & \\ & 1 & \\ n & 1 & \end{array} \right. \end{array}.$$

Thus, $p(z) = g(m_0, \dots, m_n; z)$ with $m_0 = \dots = m_n = 1$.

(1.16) Example: Let $I \subset S$ be an ideal defining d points in P^n , so the Hilbert polynomial of S/I is $p(z) = d$. Then $p(z) = g(m_0; z)$ with $m_0 = d$.

(1.17) Example: Let $I \subset S$ be an ideal which defines a degree d , genus g curve $X \subset P^n$. Then S/I has Hilbert polynomial $p(z) = dz + (1-g)$. Note that

$$\binom{z+1}{2} - \binom{z+1-m_1}{2} = m_1 z - \binom{m_1}{2};$$

$$\binom{z+0}{1} - \binom{z+0-m_0}{1} = m_0.$$

Thus, following the proof of (1.3), we see that

$$p(z) = g(m_0, m_1; z)$$

with

$$m_0 = \binom{d}{2} + 1 - g, \quad m_1 = d.$$

(1.18) Lemma: Let $p(z) = g(m_0, \dots, m_s; z)$ be a numerical polynomial, following (1.3). Then

$$g(m_0, \dots, m_s; z) - g(m_0, \dots, m_s; z-1) = g(m_1, \dots, m_s; z).$$

Proof. $g(m_0, \dots, m_s; z) - g(m_0, \dots, m_s; z-1)$

$$= \left[\sum_{i=0}^s \binom{z+i}{i+1} - \binom{z+i-m_i}{i+1} \right] - \left[\sum_{i=0}^s \binom{z-1+i}{i+1} - \binom{z-1+i-m_i}{i+1} \right]$$

$$= \sum_{i=1}^s \binom{z-1+i}{i} - \binom{z-1+i-m_i}{i}$$

$$= \sum_{i=0}^{s-1} \binom{z+i}{i+1} - \binom{z+i-m_{i+1}}{i+1}$$

$$= g(m_1, \dots, m_s; z). \quad \square$$

§2 m-Regularity

(2.1) We recall the notion of m -regularity, due to Castelnuovo, which measures the vanishing of coherent sheaf cohomology. A discussion of m -regularity can be found in Mumford [Mum66, lecture 14], where a loose bound is obtained on the vanishing of ideal sheaf cohomology. We follow Mumford in the proofs of (2.2) and (2.3a).

Definition: A coherent sheaf F on P^n is m -regular if $H^i(F(m-i)) = (0)$ for all $i \geq 1$.

(2.2) The following exact sequence is fundamental to the study of m -regularity:

Lemma: Let F be a coherent sheaf on P^n , and let $H \subset P^n$ be a hyperplane not containing any associated primes of F . If F_H denotes the restriction of F to H , then

(a) the sequence

$$0 \longrightarrow F(-1) \longrightarrow F \longrightarrow F_H \longrightarrow 0$$

is exact;

(b) if F is m -regular, then F_H is m -regular.

Proof. (a) We have tensored the exact sequence

$$0 \longrightarrow \mathcal{O}(-1) \longrightarrow \mathcal{O} \longrightarrow \mathcal{O}_H \longrightarrow 0$$

by F , where $\mathcal{O} = \mathcal{O}_P$ is the structure sheaf on P^n . Since by assumption, any local equation for H is a unit at all associated primes of F , the map $F(-1) \longrightarrow F$ is injective,

which is all that we need to check.

(b) From the exactness of (a), we have

$$H^i(F(m-i)) \longrightarrow H^i(F_H(m-i)) \longrightarrow H^{i+1}(F(m-i-1))$$

for each $i \geq 1$. If F is m -regular, then the outside groups are zero, so F_H is m -regular. \square

(2.3) The following result is due to Castelnuovo.

Proposition: If F is an m -regular coherent sheaf on P^n , then

(a) F is j -regular for each $j \geq m$;

(b) $F(m)$ is generated by global sections, as an O_P -module.

Proof. (a) Choose a hyperplane H not containing any associated prime of F , and consider the exact sequence (2.2a). By (2.2b) and induction, we can assume for $j > m$ that F_H is j -regular and F is $(j-1)$ -regular. By the exactness of

$$H^i(F(j-i-1)) \longrightarrow H^i(F(j-i)) \longrightarrow H^i(F_H(j-i)),$$

F is j -regular.

(b) is an immediate consequence of (a) and the following lemma. \square

(2.4) Lemma: Let F be a coherent sheaf on P^n , and let

$$0 \longrightarrow M_n \longrightarrow \dots \xrightarrow{A_1} M_1 \xrightarrow{A_0} M_0 \longrightarrow F \longrightarrow 0$$

be a finite free resolution of F , where each

$$M_i = \bigoplus_j \mathcal{O}_P(-e_{ij}).$$

Let $m = \max_{i,j} \{e_{ij} - i\}$. Then

- (a) F is m -regular;
- (b) for a minimal free resolution, F is not $(m-1)$ -regular.

Proof. Each group $H^i(F(z))$ is dual as a k -vector space to $\text{Ext}^{n-i}(F(z), \omega)$ by Serre duality on P^n , where $\omega \simeq \mathcal{O}_P(-n-1)$. We can use the given projective resolution of F to compute these Ext groups. Write $0 = 0_P$.

$\text{Ext}^{n-i}(F(z), \omega)$ is the kernel mod image of the sequence

$$\text{Hom}(M_{n-i+1}(z), \omega) \xleftarrow{A_{n-i}^*} \text{Hom}(M_{n-i}(z), \omega) \xleftarrow{A_{n-i-1}^*} \text{Hom}(M_{n-i-1}(z), \omega),$$

where

$$\text{Hom}(M_{n-i}(z), \omega) = \bigoplus_j \text{Hom}(\mathcal{O}(z - e_{n-i,j}), \mathcal{O}(-n-1)).$$

- (a) If $m = \max_{i,j} \{e_{ij} - i\}$, then

$$\text{Hom}(M_{n-i}(m-i), \omega) = (0),$$

so necessarily $H^i(F(m-i)) = (0)$, for $i \geq 1$, and F is m -regular.

(b) A minimal free resolution has the property that each map $A_i : M_{i+1} \rightarrow M_i$ is given by a matrix whose entries are either zero, or homogeneous polynomials of degree ≥ 1 . Thus each syzygy $\mathcal{O}(-e_{ij})$ is either preceded in the resolution by an $\mathcal{O}(-e_{i+1,r})$ with $e_{i+1,r} > e_{ij}$,

or the map A_i has a zero j^{th} row corresponding to the summand $\mathcal{O}(-e_{ij})$ of M_i . Thus we can choose a syzygy where the latter is the case, and where $m = e_{ij} - i$.

The dual map A_i^* has as matrix the transpose of the matrix for A_i , so the summand $\text{Hom}(\mathcal{O}(z - e_{ij}), \omega)$ of $\text{Hom}(M_i(z), \omega)$ is contained in the kernel of A_i^* . Let $z = e_{ij} - n - 1$, and consider the sequence

$$\text{Hom}(M_{i+1}(z), \omega) \xleftarrow{A_i^*} \text{Hom}(M_i(z), \omega) \xleftarrow{A_{i-1}^*} \text{Hom}(M_{i-1}(z), \omega).$$

$\text{Hom}(M_i(z), \omega)$ has as summand $\text{Hom}(\mathcal{O}(z - e_{ij}), \omega) = \text{Hom}(\mathcal{O}(-n-1), \mathcal{O}(-n-1)) \simeq k$, contained in the kernel of A_i^* . Furthermore,

$$\begin{aligned} \text{Hom}(M_{i-1}(z), \omega) &= \bigoplus_p \text{Hom}(\mathcal{O}(z - e_{i-1,p}), \omega) \\ &= \bigoplus_p \text{Hom}(\mathcal{O}(e_{ij} - e_{i-1,p} - n - 1), \mathcal{O}(-n-1)) \end{aligned}$$

which is zero since by construction $e_{ij} > e_{i-1,p}$ for each p . Thus $\text{Ext}^1(F(e_{ij} - n - 1), \omega) \neq (0)$, so

$$H^{n-i}(F((e_{ij} - i - 1) - (n - i))) \neq 0$$

Since $e_{ij} - i - 1 = m - 1$, F is not $(m - 1)$ -regular. \square

(2.5) Let F be an m -regular coherent sheaf on P^n , with Hilbert polynomial

$$p(z) = \chi(F(z)).$$

Then since all higher cohomology of F vanishes in degrees $z \geq m - 1$, we have equality between the Hilbert polynomial of F and the Hilbert function of F ,

$$p(z) = h^0(F(z)),$$

for all $z \geq m-1$.

(2.6) The following is a continuation of (2.2). We follow [Got78].

Lemma: Let F be a coherent sheaf on P^n , and let $H \subset P^n$ be a hyperplane not containing any associated primes of F .

(a) If F_H is m -regular, then F satisfies the conditions of m -regular for $i \geq 2$.

(b) Furthermore, if the Hilbert polynomial $\chi(F(m-1))$ agrees with the Hilbert function $h^0(F(m-1))$ of F at degree $m-1$, then F is m -regular.

Proof. (a) From the exactness of (2.2a), we have for $i \geq 2$ the exact sequence

$$H^{i-1}(F_H(z-i+1)) \rightarrow H^i(F(z-i)) \rightarrow H^i(F(z-i+1)) \rightarrow H^i(F_H(z-i+1)).$$

When $z \geq m$, the outside groups are zero, so

$H^i(F(z-i)) \simeq H^i(F(z-i+1))$. Since these groups are zero for all large degrees, we must have that, in fact, $H^i(F(m-i)) = (0)$ for $i \geq 2$.

(b) By (a), we need only show that $H^1(F(m-1)) = (0)$. Also by (a),

$$\chi(F(m-1)) = h^0(F(m-1)) - h^1(F(m-1)).$$

The hypothesis forces $h^1(F(m-1)) = 0$. \square

(2.7) The following is an extended version of a result from [Got78]; David Eisenbud related this generalization to me.

Lemma: Let $I \subset S$ be the ideal defined by

$$(I)_z = h^0(I(z)), \quad z \geq m,$$

$$(I)_z = (0), \quad \text{otherwise,}$$

where I is an m -regular ideal sheaf on P^n . Then I is generated by $(I)_m$. Also, the 1st syzygies are all of degree $m+1$, and more generally, the i^{th} syzygies are all of degree $m+i$, in a minimal free resolution of I .

Proof. We would like to associate I with a truncated ideal sheaf $I_{\geq m}$, assert that this ideal sheaf is still m -regular, and so, by (2.4), claim the above results.

There are two approaches to doing exactly this. One is to employ local cohomology. The second, which we use, is to add a variable to S , and consider $I_{\geq m}$ as an ideal sheaf on P^{n+1} . There, a generic hyperplane section yields the original ideal sheaf I . Furthermore, the minimal free resolution for $I_{\geq m}$ does not involve the new variable, and gives exactly a minimal free resolution for I . We need only to establish that $I_{\geq m}$ is m -regular.

By (2.6), it suffices to check that

$h^1(I_{\geq m}(m-1)) = 0$. Consider the exact sequence

$$0 \longrightarrow I_{\geq m}(z-1) \longrightarrow I_{\geq m}(z) \longrightarrow I(z) \longrightarrow 0$$

given by a hyperplane section, as in (2.2). Since

$h^0(I_{\geq m}(z)) - h^0(I_{\geq m}(z-1)) = h^0(I(z))$ for all $z \geq m$ by construction, we have $h^1(I_{\geq m}(z-1)) = h^1(I_{\geq m}(z))$ for all $z \geq m$. Thus, these groups must all be zero, and the result follows. \square

(2.8) Lemma: Let I be an ideal sheaf on P^n , and let $H \subset P^n$ be a hyperplane not containing any associated primes of I . If the Hilbert polynomial $\chi(\mathcal{O}_P/I)(z)$ is written as $g(m_0, \dots, m_s; z)$ for integers m_0, \dots, m_s , by (1.3), then

$$\chi(\mathcal{O}_H/I_H)(z) = g(m_1, \dots, m_s; z).$$

Proof. It follows from (2.2) that

$$0 \longrightarrow (\mathcal{O}_P/I)(z-1) \longrightarrow (\mathcal{O}_P/I)(z) \longrightarrow (\mathcal{O}_H/I_H)(z) \longrightarrow 0$$

is an exact sequence. Thus, we have the formula

$$\chi(\mathcal{O}_H/I_H)(z) = \chi(\mathcal{O}_P/I)(z) - \chi(\mathcal{O}_P/I)(z-1)$$

for Hilbert polynomials.

The result now follows from (1.18). \square

§3 Borel Ideals

(3.1) Let $SL(n+1)$ denote the group of $(n+1) \times (n+1)$ matrices over k with determinant 1. Let $T(n+1) \subset SL(n+1)$ denote the Borel subgroup of upper triangular matrices, and let $D(n+1) \subset T(n+1)$ denote the subgroup of diagonal matrices.

Let S_1 be the k -vector space of degree 1 polynomials in $S = k[x_0, \dots, x_n]$, and let the above groups act on S_1 , via the basis x_0, \dots, x_n for S_1 . These actions extend to actions on all of S :

$S = \bigoplus_d S_d = \bigoplus_d \text{Sym}^d(S_1)$, and $g \in SL(n+1)$ acts on

$S_d = \text{Sym}^d(S_1)$ via

$$g(x_0^{a_0} \dots x_n^{a_n}) = (gx_0)^{a_0} \dots (gx_n)^{a_n}.$$

An ideal $I \subset S$ is fixed by a group G acting on S if $GI \subset I$, i.e., for every $f \in I$, $g \in G$ we have $gf \in I$.

Definition: An ideal $I \subset S$ is Borel fixed if I is fixed by the Borel subgroup $T(n+1) \subset SL(n+1)$.

(3.2) Lemma: An ideal $I \subset S$ is fixed by $D(n+1)$ if and only if I is a monomial ideal.

Proof. Suppose I is fixed by $D(n+1)$. If $f \in I$, then $gf \in I$ for every $g \in D(n+1)$. Since k is infinite, the span of $\{gf \mid g \in D(n+1)\}$ includes the monomials underlying each term of f . Thus f is a linear combination of

monomials in I , so I is generated by monomials.

Conversely, monomial ideals are clearly fixed by $D(n+1)$. \square

The above argument can be found in [Har66].

(3.3) Since $D(n+1) \subset T(n+1)$, Borel fixed ideals must be monomial ideals.

While a monomial ideal can be considered as a subset of N^{n+1} , independent of the field k , the question of which monomial ideals are Borel fixed turns out to depend on the characteristic of k .

Example: Let $S = k[x, y, z]$, and let $I = (x^p, y^p)$, where p is prime. I defines a point of multiplicity p^2 in P^2 . Let $g \in T(3)$ be the matrix

$$g = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Then $gx = x$, $gy = x+y$, and $gz = z$. Thus $gy^p = (x+y)^p$.

$(x+y)^p$ is an element of I precisely when $\text{char } k = p$, so I is Borel fixed only when $\text{char } k = p$.

(3.4) We will be particularly concerned with monomial ideals $I \subset N^{n+1}$ which correspond to a Borel fixed ideal $I \subset S$ in any characteristic. Such ideals admit a simple combinatorial description, considered as subsets of N^{n+1} . Consequently, certain useful results can be proved for

them. These results will be valid in any characteristic, but by (3.3), their usefulness will be impaired in any characteristic except zero by the fact that they do not apply to all Borel fixed ideals.

The above motivates the following definition. Let N_d^{n+1} denote the monomials of degree d in N^{n+1} , by the usual grading.

Definition: A Borel ideal $I \subset N^{n+1}$ is a set of monomials which correspond to a Borel fixed ideal $I \subset S$, when k is of characteristic zero.

A Borel subset $J \subset N_d^{n+1}$ is a set of monomials which spans a Borel fixed subspace of S_d , in characteristic zero.

(3.5) Let \geq denote the natural partial order on N^{n+1} : if $\vec{a}, \vec{b} \in N^{n+1}$ with $\vec{a} = (a_0, \dots, a_n)$, $\vec{b} = (b_0, \dots, b_n)$, then $\vec{a} \geq \vec{b}$ iff $a_i \geq b_i$ for each i .

A monomial ideal $I \subset S$ can be identified with the subset of N^{n+1} consisting of the monomials it contains; we write $I \subset N^{n+1}$. The subsets $J \subset N^{n+1}$ which correspond to monomial ideals satisfy the following property: if $\vec{a} \in J$, $\vec{b} \in N^{n+1}$, and $\vec{b} \geq \vec{a}$, then $\vec{b} \in J$.

Let $\vec{e}_i \in N^{n+1}$ have zero entries except for a 1 in the i^{th} coordinate. In the above condition, it suffices to check that $\vec{a} + \vec{e}_i \in J$ for each i .

We seek a similar criterion for $J \subset N^{n+1}$ to

correspond to a Borel fixed monomial ideal in characteristic zero.

(3.6) Lemma: Let $S = k[x, y]$, where $\text{char } k = 0$, so S_1 is 2-dimensional with basis x, y . If $J \subset N_d^2$ is a set of degree d monomials, then the following conditions are equivalent;

(a) J is a Borel subset of N_d^2 ;

(b) for some r , J consists of the first $r+1$ monomials of degree d in the lexicographic order, i.e.

$$J = \{x^{d-i}y^i \mid i = 0, \dots, r\}.$$

Proof. (a) \Rightarrow (b): Let $\vec{a}_0, \dots, \vec{a}_r$ be the monomials of J . Suppose that condition (b) does not hold, and let i be the first index so $\vec{a}_i = x^{d-j}y^j$ with $j > i$. Let $g \in T(2)$ be the matrix

$$g = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

so $gx = x$, and $gy = x+y$. Then

$$g\vec{a}_i = x^d + \binom{j}{1}x^{d-1}y + \dots + \binom{j}{j-1}x^{d-j+1}y^{j-1} + x^{d-j}y^j,$$

so in characteristic zero $g\vec{a}_i$ is not a linear combination of a_0, \dots, a_r , and condition (a) does not hold.

(b) \Rightarrow (a); $T(2)$ is generated by $D(2)$ and the matrix g above. Given condition (b), by the above calculation each $g\vec{a}_i$ is a linear combination of a_0, \dots, a_r , so J generates a Borel fixed subspace of S_d in any characteristic. In particular, condition (a) holds. \square

(3.7) Lemma: Let $S = k[x_0, \dots, x_n]$, where $\text{char } k = 0$. If $J \subset N_d^{n+1}$ is a set of degree d monomials, then the following conditions are equivalent:

- (a) J is a Borel subset of N_d^{n+1} ;
 (b) for each $\vec{a} = (a_0, \dots, a_n) \in J$, and for each $i < j$ with $a_j > 0$, $(a_0, \dots, a_{i+1}, \dots, a_{j-1}, \dots, a_n)$ also belongs to J .

Proof. $T(n+1)$ is generated by $D(n+1)$ and matrices g_{ij} , $i < j$, which consist of identity matrices with an extra 1 in position (i, j) . For example, in $T(3)$ we have

$$g_{13} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Let $p: N^{n+1} \rightarrow N^{n-1}$ be the projection which omits the i, j coordinates, i.e.

$$p(a_0, \dots, a_n) = (a_0, \dots, a_{i-1}, a_{i+1}, \dots, a_{j-1}, a_{j+1}, \dots, a_n).$$

For each $\vec{b} \in N^{n-1}$ of degree $\leq d$, let $W_{\vec{b}} \subset S_d$ denote the subspace spanned by the degree d monomials of $p^{-1}(\vec{b})$. Then we have the direct sum decomposition

$$S_d = \bigoplus_{\vec{b}} W_{\vec{b}},$$

and the action of g_{ij} on S_d is the direct sum of its actions on each summand $W_{\vec{b}}$. g_{ij} acts on each $W_{\vec{b}}$ according to the isomorphism

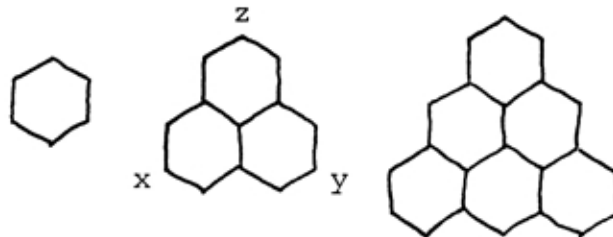
$$W_{\vec{b}} \simeq \text{Symm}^{d-\text{deg}(\vec{b})}(x_i, x_j),$$

so the result follows from lemma (3.6). \square

(3.8) We shall need to draw sets of monomials in N^3 in the following pages. This can be done by representing N_d^3 , the possible monomials of degree d in $k[x,y,z]$, by a triangle whose cells correspond naturally to these monomials. We have

$$\begin{array}{ccccccc}
 & & & & & & z^2 \\
 & & & & & & xz & yz \\
 & & & z & & & x^2 & xy & y^2 \\
 & & x & & y & & & & \\
 1 & & & & & & & &
 \end{array}$$

represented by the diagram

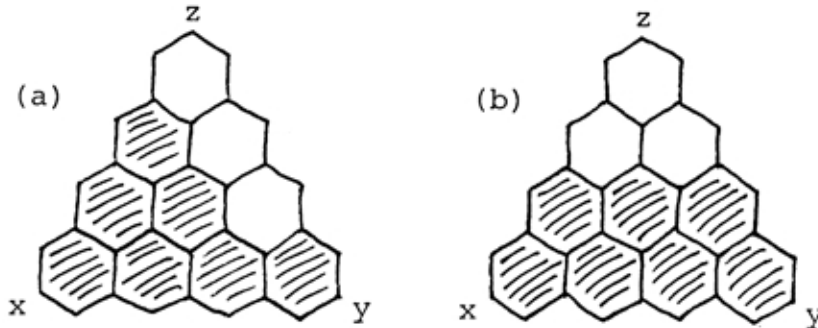


Using this notation, a specific set of monomials can be indicated by shading in the corresponding cells.

If we wish to illustrate N_d^3 for a single degree d , we will use a single triangle. This notation is employed in the following example.

Example: According to (3.7), in characteristic zero, the possible sets of 7 monomials which are Borel subsets of

N_3^3 are these:



Condition (3.7b) can be imagined as follows:

For each $i < j$, when corner i of such a diagram is lowered, and corner j lifted, the monomials $J \in N^{n+1}$ cannot roll further downhill, if one assumes gravity.

(3.9) Definition: The partial sum operator $\sigma : N^{n+1} \rightarrow N^{n+1}$ is defined by

$$\sigma(a_0, \dots, a_n) = (a_0, a_0+a_1, \dots, a_0+\dots+a_n).$$

Note that σ is injective and linear.

(3.10) Let $\vec{e}_i \in N^{n+1}$ be defined as in (3.5), and let $\vec{c}_{ij} = \vec{e}_i - \vec{e}_j$. For example, in N^4 ,

$$\vec{e}_2 = (0, 1, 0, 0); \quad \vec{c}_{24} = (0, 1, 0, -1).$$

Then

$$\sigma(\vec{e}_2) = (0, 1, 1, 1); \quad \sigma(\vec{c}_{24}) = (0, 1, 1, 0).$$

Lemma: Let $\vec{a}, \vec{b} \in N^{n+1}$, and suppose $\sigma(\vec{b}) \geq \sigma(\vec{a})$. Then there exists a sequence $\vec{a} = \vec{a}_0, \dots, \vec{a}_r = \vec{b}$ with each $\vec{a}_s \in N^{n+1}$, so for $s = 0, \dots, r-1$ we have $\vec{a}_{s+1} - \vec{a}_s = \vec{e}_i$ or \vec{c}_{ij} for some i, j .

Proof. Suppose that a partial sequence $\vec{a} = \vec{a}_0, \dots, \vec{a}_s$ has been constructed, with $\sigma(\vec{b}) \geq \sigma(\vec{a}_s)$, and $\vec{a}_s \neq \vec{b}$. Let $\sigma(\vec{a})_i$ denote the i^{th} coordinate of $\sigma(\vec{a})$, and choose an i so $\sigma(\vec{b} - \vec{a}_s)_i > 0$.

There are two cases: first, if each coordinate $j > i$ of \vec{a}_s is zero, then we can define $\vec{a}_{s+1} = \vec{a}_s + \vec{e}_i$, and then $\sigma(\vec{b}) \geq \sigma(\vec{a}_{s+1})$. Otherwise, let $j > i$ be the next nonzero coordinate of \vec{a}_s , and define $\vec{a}_{s+1} = \vec{a}_s + \vec{c}_{ij}$; again, $\sigma(\vec{b}) \geq \sigma(\vec{a}_{s+1})$. In either case, $\sigma(\vec{a}_0), \dots, \sigma(\vec{a}_{s+1})$ forms a strictly increasing sequence in N^{n+1} under the natural partial order \geq , and so must terminate at $\sigma(\vec{b})$ in finitely many steps. \square

(3.11) Proposition: Let $I \subset N^{n+1}$; the following conditions are equivalent:

- (a) I is a Borel ideal;
- (b) for each $\vec{a} \in I$, $\vec{b} \in N^{n+1}$ so $\sigma(\vec{b}) \geq \sigma(\vec{a})$, we have $\vec{b} \in I$.

Proof. (b) \implies (a): For condition (a) to hold, I must first correspond to a monomial ideal. By (3.5), it suffices to check that $\vec{a} + \vec{e}_i \in I$ for each $\vec{a} \in I$, and for each i . Also, for each d , the degree d monomials in

I must form a Borel subset of N_d^{n+1} . By (3.7), it suffices to check that $\vec{a} + \vec{c}_{ij} \in I$ for each $\vec{a} \in I$, and for each $i < j$ with $\vec{a}_j > 0$. Since $\sigma(\vec{a} + \vec{e}_i) \geq \sigma(\vec{a})$ and $\sigma(\vec{a} + \vec{c}_{ij}) \geq \sigma(\vec{a})$, these requirements both follow from condition (b).

(a) \implies (b). Suppose condition (a), and let $\vec{a} \in I$, $\vec{b} \in N^{n+1}$ with $\sigma(\vec{b}) \geq \sigma(\vec{a})$. Construct a sequence $\vec{a} = \vec{a}_0, \dots, \vec{a}_r = \vec{b}$ with the property asserted in lemma (3.10). For each $s = 0, \dots, r-1$, if $\vec{a}_s \in I$, then either $\vec{a}_{s+1} = \vec{a}_s + \vec{e}_i$ and $\vec{a}_{s+1} \in I$ by (3.5), or $\vec{a}_{s+1} = \vec{a}_s + \vec{c}_{ij}$ and $\vec{a}_{s+1} \in I$ by (3.7). Thus $\vec{b} = \vec{a}_r$ belongs to I by induction, so condition (b) holds. \square

§4 Saturated Ideals

(4.1) We recall the notion of a saturated ideal, and study it for the case of Borel ideals.

Definition: A homogeneous ideal $I \subset S$ is saturated if, for any $J \supset I$ so $(J)_z = (I)_z$ for all $z \gg 0$, we have $J = I$.

If I is not saturated, there exists a largest $J \neq I$ with the above property, which is called the saturation of I , denoted I^{sat} .

Consider the subscheme $X \subset P^n$ defined by I ; I is saturated if it is the largest ideal of S which defines X . Equivalently, I is saturated if in the primary decomposition of I , the irrelevant ideal $(x_0, \dots, x_n) \subset S$ (corresponding to the vertex $\vec{0}$ of the affine cone over P^n) does not occur as an associated prime.

I is saturated in degrees $\geq d$ if

$$(I)_j = (I^{\text{sat}})_j \quad \text{for all } j \geq d.$$

(4.2) Lemma: Let the ideal $I \subset S$ define the subscheme $X \subset P^n$, and suppose $y \in S_1$ defines a hyperplane which does not contain any associated primes of X . Then the following are equivalent, for $f \in S$:

- (a) $f \in I^{\text{sat}}$;
- (b) $y^j f \in I$ for some j .

Proof. (a) \implies (b): This follows from the definition

(4.1). (b) \implies (a): Choose a primary decomposition

$I_1 \cap \dots \cap I_q$ of I^{sat} ; by assumption, y is not contained in any associated prime $r(I_i)$. Since $y^j f \in I \subset I^{\text{sat}}$, $y^j f \in I_i$ for each i . Since each I_i is primary, it follows that $f \in I_i$ for each i . Thus $f \in I^{\text{sat}}$. \square

(4.3) Lemma: Let $I \subset S$ be a Borel ideal, defining the subscheme $X \subset P^n$. Then $x_n \in S_1$ defines a hyperplane which does not contain any associated primes of S .

Proof. Since I is Borel fixed, the associated primes of X are themselves defined by Borel fixed monomial ideals. The only possibilities are $I_r = (x_0, \dots, x_r)$ for $r = 0, \dots, n-1$. x_n is contained in no such I_r . \square

Note that the above result in fact holds for any Borel fixed ideal in any characteristic.

(4.4) Lemma: Let $I \subset S$ be a Borel ideal, generated by its degree d part $(I)_d$. If $v \in S_d$ is a monomial so $vx_n^j \in I$ for some j , then $v \in I$.

Proof. Associate I with the subset of N^{n+1} consisting of its monomials, and associate v with the corresponding vector $v \in N^{n+1}$. If $\vec{v} + (0, \dots, 0, j) \in I$, then $\vec{v} + (0, \dots, j) = \vec{w} + \vec{a}$ for some $\vec{w} \in (I)_d$, $\vec{a} \in N^{n+1}$. Moreover, if $\vec{a} = (a_0, \dots, a_n)$, then $\sigma(\vec{a}) = (a_0, \dots, a_0 + \dots + a_{n-1}, j)$.

Thus $\sigma(\vec{v}) = \sigma(\vec{w}) + (a_0, \dots, a_0 + \dots + a_{n-1}, 0)$, so $\sigma(\vec{v}) \geq \sigma(\vec{w})$.

It follows by proposition (3.11) that $\vec{v} \in I$. \square

We recall the discussion from (3.4). The above result is valid in any characteristic, but is about a class of ideals which are primarily of interest in characteristic zero.

(4.5) Corollary: Let J be a Borel subset of S_d . let $I \subset S$ be the ideal generated by J . Then I is a Borel ideal, saturated in degrees $\geq d$.

Proof. I is Borel fixed in any characteristic, since for any $g \in T(n+1)$, gI is generated by gJ , which spans the same subspace of S_d as J , by assumption.

The saturation of I in degrees $\geq d$ now follows from lemmas (4.2), (4.3), (4.4). \square

§5 The Wild Card Partition

(5.1) In this section, we develop a notation for describing Borel ideals, which makes their structure more apparent. These results hold in any characteristic, but are of most interest in characteristic zero (see (3.4)).

Definition: A wild card $a^* = (a_0, \dots, a_r, *, \dots, *) \in N^{n+1}$ is the subset

$$(a_0, \dots, a_r, *, \dots, *) = \{\vec{b} \in N^{n+1} \mid a_i = b_i \text{ for } i=0, \dots, r\}.$$

The wild card a^* consists of all $b \in N^{n+1}$ whose coordinates match those of a^* , where $*$ as a coordinate of a^* matches anything.

A wild card has rank j if $j+1$ of its coordinates are $*$.

The height of a wild card is the sum of its coordinates, excluding occurrences of $*$.

A set of wild cards is disjoint if it consists of disjoint subsets of N^{n+1} .

The partial sum operator σ is defined on wild cards by

$$\sigma(a_0, \dots, a_r, *, \dots, *) = (a_0, a_0 + a_1, \dots, a_0 + \dots + a_r, *, \dots, *).$$

The partial order \geq on N^{n+1} can be extended to wild cards of equal rank:

$(b_0, \dots, b_r, *, \dots, *) \geq (a_0, \dots, a_r, *, \dots, *)$ if $b_i \geq a_i$ for each $i = 0, \dots, r$.

(5.2) Lemma: Let I be a subset of N^{n+1} , and let B be the set of all wild cards contained in the complement of I :

$$B = \{b^* \mid b^* \in N^{n+1} \setminus I\}.$$

The following conditions are equivalent:

- (a) I is a Borel ideal;
- (b) For each $b^* \in B$, if a^* is a wild card of the same rank so $\sigma(b^*) \geq \sigma(a^*)$, then $a^* \in B$.

Proof. If a^*, b^* are two wild cards of the same rank so $\sigma(b^*) \geq \sigma(a^*)$, then each monomial $\vec{a} \in a^*$ is similarly bounded by a corresponding monomial $\vec{b} \in b^*$: if $b^* = (b_0, \dots, b_r, *, \dots, *)$, and $\vec{a} = (a_0, \dots, a_n) \in a^*$, then let $\vec{b} = (b_0, \dots, b_r, a_{r+1}, \dots, a_n)$; we have $\vec{b} \in b^*$, and $\sigma(\vec{b}) \geq \sigma(\vec{a})$.

The equivalence of conditions (a) and (b) is now a direct rewording of proposition (3.11). \square

(5.3) Example: Let $S = k[x, y, z]$, and let $I \subset S$ be the Borel ideal generated by x^3, x^2y, xy^2, x^2z , and xyz :



The complement of I is then the union of the wild cards $(0,*,*)$, $(1,0,*)$, $(1,1,0)$, and $(2,0,0)$. These wild cards are disjoint, and thus form a partition of the complement of I .

Note that the complement of $I^{\text{sat}} = (x^2, xy)$ is partitioned by the wild cards $(0,*,*)$ and $(1,0,*)$; the rank -1 wild cards $(1,1,0)$ and $(2,0,0)$ do not appear.

We seek to show that such a finite wild card partition exists for the complement of any Borel ideal.

(5.4) Definition: Let I be a subset of N^{n+1} . A wild card b^* is c -maximal with respect to I if $b^* \in N^{n+1} \setminus I$, and no $a^* \in N^{n+1} \setminus I$ properly contains b^* .

The complement of any subset $I \subset N^{n+1}$ is clearly the union of c -maximal wild cards, which must be disjoint. The difficulty is to determine when such a partition is finite.

(5.5) Definition: Let I be a subset of N^{n+1} , and let a^* , b^* be c -maximal for I . b^* σ -dominates a^* if for some $c^* \in a^*$, we have $\sigma(b^*) \supseteq \sigma(c^*)$. Equivalently, if $b^* = (b_0, \dots, b_r, *, \dots, *)$ and $a^* = (a_0, \dots, a_s, *, \dots, *)$, then b^* σ -dominates a^* if $r \geq s$, and $b_0 + \dots + b_i \geq a_0 + \dots + a_i$ for $i = 0, \dots, s$.

A wild card b^* is σ -maximal for I if b^* is c -maximal, and no c -maximal a^* distinct from b^* σ -dominates b^* .

Note that if b^* σ -dominates a^* , then the height of b^* bounds the height of a^* .

In example (5.3), $(2,0,0)$ is the only σ -maximal wild card for I . $(1,0,*)$ is the only σ -maximal wild card for I^{sat} .

(5.6) Lemma: Let $I \subset \mathbb{N}^{n+1}$ be a Borel ideal. For each c -maximal wild card a^* associated to I , there exists a σ -maximal b^* associated to I , which σ -dominates a^* .

Proof. Let $a^* = a_0^*, \dots, a_i^*, \dots$ be an infinite sequence of c -maximal wild cards so a_{i+1}^* σ -dominates a_i^* for each i . We show that such a sequence is eventually constant.

Let each $a_i^* = (a_{0i}, \dots, a_{r_i i}, *, \dots, *)$. Assume inductively that for some q and all $i \geq q$, $a_i^* \subset b^* = (b_0, \dots, b_j, *, \dots, *)$. If each $a_i^* \neq b^*$, then by the c -maximality of the a_i^* , $b^* \cap I$ is nonempty. Let $\vec{c} = (c_0, \dots, c_n) \in b^* \cap I$; we claim that for each $i \geq a$, $c_{j+1} + \dots + c_n \geq a_{j+1, i}$. Otherwise, by proposition (3.11), a_i^* would intersect I , contrary to assumption. Now, since for $i \geq q$, $a_{j+1, i}$ is a monotone sequence, it must eventually be constant. Thus we can choose a new q and a new $b^* = (b_0, \dots, b_{j+1}, *, \dots, *)$ so $a_i^* \subset b^*$ for all $i \geq q$.

Thus, there is a limiting b^* so for all $i \gg 0$, $a_i^* = b^*$. From this we conclude that σ -maximal wild cards exist as claimed. \square

(5.7) Lemma: Let $I \subset N^{n+1}$ be a Borel ideal. If $a^* = (a_0, \dots, a_r, *, \dots, *)$ is a σ -maximal wild card for I , then

$$\vec{a} = (a_0, \dots, a_{r-1}, a_r+1, 0, \dots, 0)$$

belongs to the minimal generating set for I .

Proof. \vec{a} belongs to I , since no wild card can contain \vec{a} without σ -dominating a^* .

However, $\vec{a}_r = (a_0, \dots, a_r, 0, \dots, 0) \in a^*$, and so cannot belong to I . Similarly, if

$\vec{a}_i = (a_0, \dots, a_i-1, \dots, a_r+1, 0, \dots, 0)$, then $\sigma(\vec{a}_r) \geq \sigma(\vec{a}_i)$, so by proposition (3.11), \vec{a}_i cannot belong to I .

Thus \vec{a} is a minimal generator for I . \square

(5.8) The following result is a companion for (5.7)

Lemma: Let $I \subset N^{n+1}$ be a Borel ideal. If I has a minimal generator \vec{a} of degree d , then there exists a c -maximal wild card b^* for I , of height $d-1$.

Proof. Let $\vec{a} = (a_0, \dots, a_r, 0, \dots, 0)$, with $a_0 + \dots + a_r = d$, and $a_r > 0$. Then $\vec{b} = (a_0, \dots, a_r-1, 0, \dots, 0)$ cannot belong to I , so \vec{b} belongs to a c -maximal b^* that does not contain \vec{a} . Such a b^* must be contained in the wild card $(a_0, \dots, a_r-1, *, \dots, *)$, and thus has height $a_0 + \dots + a_r - 1 = d-1$. \square

(5.9) Proposition: Let $I \subset N^{n+1}$ be a Borel ideal. Then there exists a unique finite set of disjoint wild

cards whose union is the complement of I .

Proof. Let B consist of the c -maximal wild cards for I . These are disjoint with union $N^{n+1} \setminus I$, as noted in (5.4). By (5.6) each $a^* \in B$ is σ -dominated by, and thus has height bounded by, a σ -maximal $b^* \in B$. This b^* has height bounded by the degree of some minimal generator for I , by (5.7). Since S is noetherian, I has only finitely many minimal generators, so the heights of wild cards in B can be uniformly bounded. Thus B is finite.

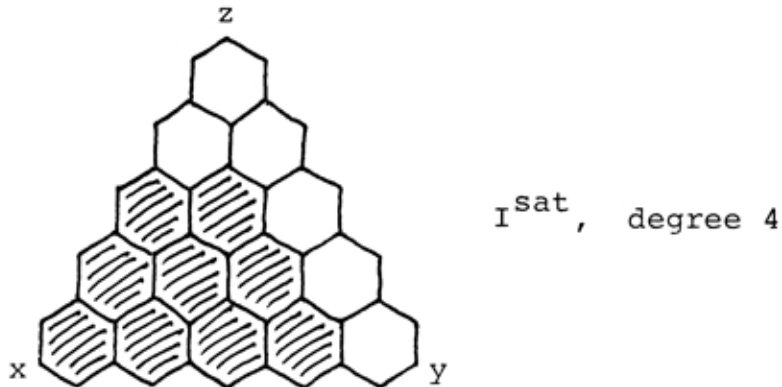
Any finite wild card partition for I must consist of c -maximal elements, since no wild card is the union of finitely many wild cards it properly contains. Thus such a partition is unique. \square

(5.10) Wild card partitions can be used as an aid to understanding the subscheme structure of $X \subset P^n$ defined by a Borel ideal $I \subset S$.

Such an $X \subset P^n$ has each of its components supported on one of the linear subspaces $L_i \subset P^n$, defined by the ideal (x_0, \dots, x_{n-i-1}) , in the flag in P_n fixed by $T(n+1)$. In terms of the wild card partition for I , the component of X supported on L_i (of dimension i) has multiplicity given by the number of wild cards of rank i in the partition. The exact nilpotent structure of this component of X is given by specific knowledge of these wild cards.

The rank -1 wild cards do not occur in the partition of a saturated ideal, as (6.2) will show, and thus play no role in describing X .

X is easily visualized in terms of the degree d monomials not in I , for any sufficiently large d . We reexamine example (5.3), looking at a slice of I^{sat} of degree 4.



$X \subset \mathbb{P}^2$ defined by I^{sat} consists of a line corresponding to the complete row of monomials contained in the wild card $(0, *, *)$ of rank 1, and an embedded point. This point corresponds here to the monomial $xz^3 \in (1, 0, *)$.

Thus, wild cards of rank ≥ 0 describe the appearance of a slice of an ideal, for any large degree, which in turn describes the induced subscheme of \mathbb{P}^n .

One can define wild cards more generally for arbitrary monomial ideals. They do not then form a partition, and otherwise behave less nicely, but in an analogous way describe the induced subscheme structure, and provide a useful proof technique. We do not develop

this theory here.

§6 m-Regularity of Borel Ideals

(6.1) In this section we make a number of applications of wild card partitions.

Lemma: Let $I \subset N^{n+1}$ be a Borel ideal, and let B be the wild card partition of I given by proposition (5.9). If $c^* \in B$ is σ -maximal, then $I \cup c^*$ is also a Borel ideal, with wild card partition $B - \{c^*\}$.

Proof. This result follows directly from (5.2), since by the σ -maximality of c^* , no $a^* \subset c^*$ can become involved in a test of condition (b) on $I \cup c^*$. \square

(6.2) Lemma: Let $I \subset N^{n+1}$ be a Borel ideal, and let B be the wild card partition for I . The following are equivalent:

- (a) I is saturated;
- (b) B contains no rank -1 wild cards.

Proof. (b) \implies (a); Let \vec{b} be a monomial not in I . \vec{b} must be contained in a wild card $b^* \in B$ of rank ≥ 0 , but then $\vec{b} + (0, \dots, 0, j) \in b^*$ for each $j \geq 0$. By (4.2) and (4.3), \vec{b} does not belong to I^{sat} . Thus $I = I^{\text{sat}}$.

(a) \implies (b): If B contains a rank -1 wild card $b^* = \{\vec{b}\}$, where $\vec{b} = (b_0, \dots, b_n)$, then by the c -maximality of b^* , $(b_0, \dots, b_{n-1}, *) \cap I$ is nonempty. Thus by (4.2) and (4.3), since $\vec{b} + (0, \dots, 0, j) \in I$ for some j , $\vec{b} \in I^{\text{sat}}$, and $I \neq I^{\text{sat}}$.

Alternatively, b^* is σ -dominated by a σ -maximal wild card c^* of rank -1 , by (5.6). $I \cup c^*$ is an ideal, by (6.1), and $(I)_z = (I \cup c^*)_z$ for all large degrees z , since c^* consists of a single monomial. Thus $I \subset I \cup c^* \subset I^{\text{sat}}$, and $I \neq I^{\text{sat}}$. \square

(6.3) Lemma: If b^* is a wild card of rank $i \geq 0$ and height j , then b^* contains $\binom{z+i-j}{i}$ monomials of degree z , for each $z \geq j-i$. When $z < j-i$, b^* contains no monomials of degree z , but the above expression is negative.

Proof. The second statement is immediate. b^* in fact contains no monomials of degree $z < j$, but this agrees with the expression for $j-i \leq z < j$. Let

$b^* = (b_0, \dots, b_{n-i-1}, *, \dots, *)$, where $b_0 + \dots + b_{n-i-1} = j$.

If $z \geq j$, then the degree z monomials of b^* are in 1:1 correspondence with the set of all degree $z-j$ monomials in $i+1$ variables. These are $\binom{z+i-j}{i}$ in number. \square

(6.4) Lemma: Let $I \subset N^{n+1}$ be a Borel ideal, and let B be the wild card partition for I . If $b^* \in B$ has rank i and height $j > 0$, then some $a^* \in B$ has rank $\geq i$ and height $j-1$.

Proof. Let $b^* = (b_0, \dots, b_s, 0, \dots, 0, *, \dots, *)$, with $b_s > 0$, and $b_0 + \dots + b_s = j$. Then

$\vec{b} = (b_0, \dots, b_{s-1}, 0, \dots, 0)$ is contained in some wild card $a^* \in B$, by proposition (3.11). By the c -maximality of b^* , a^* must be contained in $(b_0, \dots, b_{s-1}, *, \dots, *)$, and thus has height $j-1$. a^* must also have rank at least that of b^* , since b^* σ -dominates a^* , by (5.2). \square

(6.5) Proposition: Let $I \subset N^{n+1}$ be a saturated Borel ideal, and let B be the wild card partition of I . Let $X \subset P^n$ be the subscheme defined by I . Let $p(z) = g(m_0, \dots, m_s; z)$ be the Hilbert polynomial of \mathcal{O}_X , of equivalently of S/I , in the notation of (1.3). Let d be the maximum of the heights of elements of B . Then

- (a) $m_0 \geq \dots \geq m_s > 0$;
- (b) $m_0 \geq d+1$;
- (c) $p(z) = \dim(S/I)_z$ for all $z \geq d$.

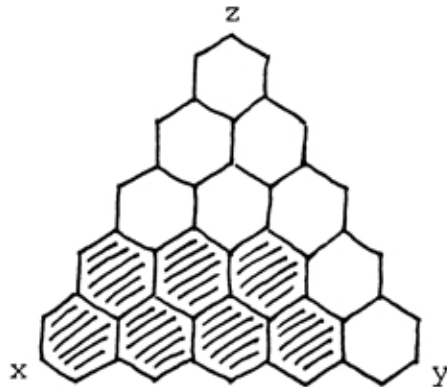
Proof. For all degrees $z \gg 0$, $p(z)$ is the number of degree z monomials in $N^{n+1} \setminus I$. This set is partitioned by the wild cards in B , so $p(z)$ is the sum of contributions from each $b^* \in B$.

By (6.3), $p(z) = g(A, z)$ for a diagram $A = \{a_{ij}\}$ in the notation of (1.4), where a_{ij} is the number of rank i , height j wild cards in B . By (6.4), A can be brought into monotonic form by a single application of (1.10b) to each term corresponding to an element of B . A now has bounds $m_0 \geq \dots \geq m_s \geq 0$, with $m_0 \geq d+1$. By lemmas (1.13), (1.14), A is equivalent to a reduced monotonic diagram, with bounds at least as large as

$m_0 \geq \dots \geq m_s > 0$. This proves (a), (b).

(c) follows from (6.3), which asserts that for $z \geq d$, the above count is correct. \square

(6.6) We follow the argument of (6.5) for an example. Let $I \subset S = k[x, y, z]$ be defined by the wild card partition $(0, *, *)$, $(1, 0, *)$, $(1, 1, *)$, $(2, 0, *)$. The degree 4 part of I is then



We compute the Hilbert polynomial $p(z)$ of S/I :

$$\begin{array}{c}
 \begin{array}{c|cccc}
 & 0 & 1 & 2 & 3 & 4 \\
 0 & & 1 & 2 & & \\
 1 & 1 & & & &
 \end{array}
 \quad \sim \quad
 \begin{array}{c|cccc}
 & 0 & 1 & 2 & 3 & 4 \\
 0 & & 1 & 1 & 2 & \\
 1 & 1 & & & &
 \end{array} \\
 \\
 \sim \quad
 \begin{array}{c|cccc}
 & 0 & 1 & 2 & 3 & 4 \\
 0 & & 1 & 1 & 1 & 1 \\
 1 & 1 & & & &
 \end{array}
 \end{array}$$

Thus, $p(z) = g(m_0, m_1; z)$ with $m_0 = 4$, $m_1 = 1$.

(6.7) Let $I \subset S$ be an ideal, and let $I \subset \mathcal{O}_P$ be the corresponding ideal sheaf. If $\mathcal{O}_X = \mathcal{O}_P/I$, then $\dim(S/I)_z$ and $h^0(\mathcal{O}_X(z))$ are not necessarily equal, for all values of z . However, they do share a common Hilbert polynomial $p(z)$, so

$$\dim(S/I)_z = h^0(\mathcal{O}_X(z)) = p(z)$$

for all large z .

For all z , we have

$$\dim(s)_z = h^0(\mathcal{O}_P(z)) = \binom{z+n}{n};$$

Thus if we define $q(z) = \binom{z+n}{n} - p(z)$, then

$$\dim(I)_z = h^0(I(z)) = q(z)$$

for all large z . Here, since I is a sheaf of ideals, $\dim(I)_z$ and $h^0(I(z))$ are equal for all values of z : in fact, $(I)_z = H^0(I(z))$.

(6.8) Lemma: Let $I \subset S$ be an ideal, and let $I \subset \mathcal{O}_P$ be the corresponding ideal sheaf. Suppose I is generated by elements of degree $\leq d$, and let $H = \{h = 0\}$ be a hyperplane in P^n . If I_H is the restriction of I to H as in (2.2), and I_H^{sat} is the corresponding saturated ideal in $S_H = S/hS$, then I_H^{sat} is generated by elements of degree $\leq d$.

Proof. Let $I = (f_1, \dots, f_s)$, and let \bar{f}_i denote the image of f_i in S_H . Then I_H^{sat} is the saturation of $(\bar{f}_1, \dots, \bar{f}_s) \subset S_H$, and so is generated by elements of degree $\leq d$. \square

(6.9) Proposition: Let $I \subset N^{n+1}$ be a saturated Borel ideal. If d is the largest degree of a minimal generator for I , then the corresponding sheaf of ideals $I \subset \mathcal{O}_P$ is d -regular.

Proof. We proceed by induction on n . If $n = 1$, then I is principal, so $I = (x_0^d)$, by (3.6). Thus, $I \simeq \mathcal{O}(-d)$, which is d -regular.

In general, consider the exact sequence

$$0 \longrightarrow I(-1) \longrightarrow I \longrightarrow I_H \longrightarrow 0$$

of (2.2). By (4.3), we can choose H to be the hyperplane defined by $x_n = 0$. Then by (6.8), the minimal generators of the corresponding ideal I_H^{sat} are all of degree $\leq d$, so I_H is d -regular by induction.

Now, by (2.6b) and (6.7), I is d -regular if $h^0(I(d-1)) = \binom{n+d-1}{n} - g(m_0, \dots, m_s; d-1)$, where m_0, \dots, m_s give the Hilbert polynomial of S/I . By (5.7), the wild card partition for I consists of elements of height $\leq d-1$. Thus, the desired identity follows from (6.5c). \square

(6.10) Corollary: Let I be as in (6.9). If S/I has Hilbert polynomial $p(z)$, then $\dim(I)_z = \binom{z+n}{n} - p(z)$ for all $z \geq d-1$.

Proof. By (6.9), the corresponding ideal sheaf I is d -regular. Thus, $h^0(I(z))$ is equal to $\chi(I(z))$ for

$z \geq d-1$, by (2.5). By (6.7),

$$\dim(I)_z = \chi(I(z)) = \binom{z+n}{n} - p(z),$$

yielding the result. \square

(6.11) Proposition: Let $I \subset \mathcal{O}_p$ correspond to a Borel ideal $I \subset S$. If S/I has Hilbert polynomial $g(m_0, \dots, m_s; z)$, then I is m_0 -regular.

Proof. Let d be the largest height of the elements of the wild card partition for I . Then by (5.8), I is generated by elements of degree $\leq d+1$. Thus, by (6.9), I is $(d+1)$ -regular. By (6.5b), $m_0 \geq d+1$. Thus, I is m_0 -regular, by (2.3a). \square

§7 The Lexicographic Ideal

(7.1) We establish some further notational conventions, before defining a lexicographic ideal.

Let $N^n \subset N^{n+1}$ denote the inclusion of N^n onto the subset of N^{n+1} consisting of elements with last coordinate zero. Similarly, let $N_d^n \subset N_d^{n+1}$ denote the degree d part of the previous inclusion, for the usual grading.

If $I \subset S$ is an ideal, and H is a hyperplane in P^n defined by $h = 0$, then let I_H denote the ideal $\bar{I} \subset S/hS$. Note that I_H can fail to be saturated when I is saturated. We shall write explicitly I_H^{sat} when the saturation is meant.

Definition: $J \subset N_d^{n+1}$ is a lexicographic subset of N_d^{n+1} if J consists of the r greatest monomials of N_d^{n+1} in the lexicographic order $>_{\text{lex}}$, for some r .

$L \subset N^{n+1}$ is a lexicographic ideal if L is an ideal, and $(L)_d$ is a lexicographic subset of N_d^{n+1} for each d .

Let H denote the hyperplane $x_n = 0$. If $J \subset N_d^{n+1}$ is lexicographic, then clearly $J_H = J \cap N_d^n$ is lexicographic. Similarly, if $L \subset N^{n+1}$ is a lexicographic ideal, then $L_H = L \cap N^n$ is a lexicographic ideal in N^n .

(7.2) Lemma: A lexicographic subset $J \subset N_d^{n+1}$ is a Borel subset; a lexicographic ideal $L \subset N^{n+1}$ is a Borel

ideal.

Proof. Suppose that $\vec{a} = (a_0, \dots, a_n) \in J$, and $\vec{b} = (b_0, \dots, b_n) \in N_d^{n+1}$, so $\sigma(\vec{b}) \geq \sigma(\vec{a})$. If $\vec{b} \neq \vec{a}$, let i be the first coordinate so $\sigma(\vec{b})_i > \sigma(\vec{a})_i$. Then $b_0 = a_0, \dots, b_{i-1} = a_{i-1}$, and $b_i > a_i$. Thus, $\vec{b} >_{\text{lex}} \vec{a}$, so $\vec{b} \in L$.

The ideal generated by J will be a Borel ideal iff J is a Borel subset. Thus, by (3.11), J is Borel. It follows immediately that L is a Borel ideal. \square

(7.3) We seek to describe the wild card partition of a saturated lexicographic ideal; the following lemma is preparatory.

Let H denote the hyperplane $x_n = 0$, and write $N^n \subset N^{n+1}$ as in (6.1). For each wild card $b^* \in N^{n+1}$ of rank ≥ 0 , let $b_H^* \in N^n$ denote the wild card $b^* \cap N^n$ obtained by deleting the last coordinate of b^* . For example, $(1, *, *)_H = (1, *)$.

For each wild card $c^* \in N^n$, let $(c^*, *)$ denote adjoining $*$ as an n^{th} coordinate to c^* . For example, $((1, 0), *) = (1, 0, *)$.

Lemma: Let I be a saturated Borel ideal in N^{n+1} , and let H be the hyperplane $x_n = 0$. If B is the wild card partition for I , then I_H has the wild card partition

$$B_H = \{b_H^* \mid b^* \in B\}.$$

Proof. We have $I_H = I \cap N^n$. Thus, if $b^* \in B$, then $b_H^* \cap I_H$ is empty. In the other direction, if $c^* \cap I_H$ is empty for a wild card $c^* \in N^n$, then $(c^*, *) \cap I$ can be shown to be empty. Suppose on the contrary that $\vec{c} = (c_0, \dots, c_n) \in (c^*, *) \cap I$. Since I is saturated, $(c_0, \dots, c_{n-1}, 0)$ belongs to I by (4.2) and (4.3), and so to $c^* \cap I_H$. This is contrary to assumption, so $(c^*, *) \cap I$ must in fact be empty.

By (5.9), the wild card partitions for I , I_H consist of the c -maximal wild cards for I , I_H , respectively. By the above argument, the result follows. \square

(7.4) Lemma: Let J be a Borel subset of N_d^{n+1} , and let $I \subset S$ be the saturation of the ideal generated by J . Then the wild card partition B for I can be computed as follows.

First, compute inductively B_H for I_H^{sat} , and adjoin to B each $(c^*, *)$ for $c^* \in B_H$.

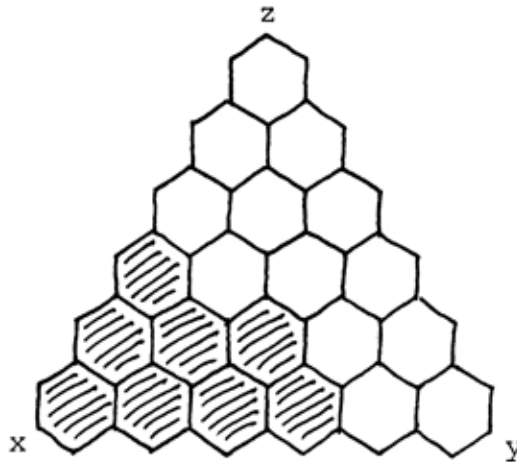
Second, for each $\vec{b} = (b_0, \dots, b_n) \in N_d^{n+1}$ contained in neither J nor B , adjoin to B the wild card $b^* = (b_0, \dots, b_{n-1}, *)$.

Proof. First, each wild card $(c^*, *)$ is c -maximal for I , by the proof of (7.3). Second, if $\vec{b} \in J$, then $b^* \cap I$ is empty, by (4.2) and (4.3), because I is saturated. If $\vec{b} \notin (c^*, *)$ for each $c^* \in B_H$, then b^* must also be c -maximal for I , again by the proof of (7.3).

Since I is saturated, all c -maximal wild cards for I have rank ≥ 0 , and are accounted for in one of the above two cases. Thus by (5.9), we have computed B . \square

(7.5) Example: Let J be the lexicographic subset of N_5^3 consisting of the monomials

$$\{x^5, x^4y, x^4z, x^3y^2, x^3yz, x^3z^2, x^2y^3, x^2y^2z\}:$$



If I , I_H^{sat} are defined as in (7.4), then the wild card partition for I_H^{sat} is seen from the hyperplane section

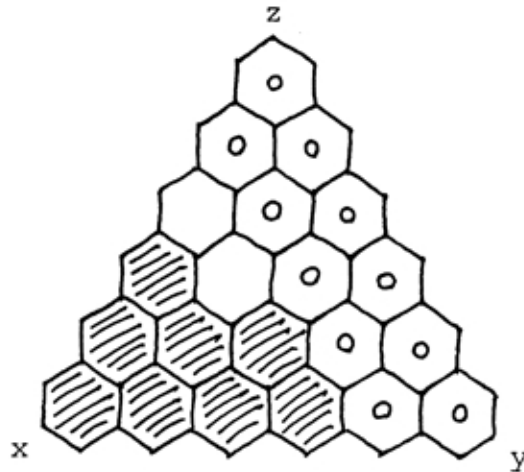


to consist of $(0,*)$ and $(1,*)$. These account for the

two complete rows of cells marked



below:



Thus, by (7.4), the wild card partition for I consists of

$$(0, *, *) , (1, *, *) , (2, 0, *) , (2, 1, *) .$$

Following the discussion (5.10), the subscheme defined by I in P^2 is therefore a line of multiplicity 2, with an embedded point of multiplicity 2.

We compute the Hilbert polynomial of S/I , by the method of (6.5):

$$\begin{array}{c}
 0 \\
 1
 \end{array}
 \begin{array}{c}
 \hline
 0 \quad 1 \quad 2 \quad 3 \quad 4 \\
 \hline
 \quad 1 \quad 1 \\
 1 \quad 1 \quad 1
 \end{array}
 \sim
 \begin{array}{c}
 0 \\
 1
 \end{array}
 \begin{array}{c}
 \hline
 0 \quad 1 \quad 2 \quad 3 \quad 4 \\
 \hline
 \quad 1 \quad 1 \quad 1 \quad 1 \\
 1 \quad 1 \quad 1
 \end{array}
 .$$

Thus, $p(z) = g(m_0, m_1; z)$ with $m_0 = 4$, $m_1 = 2$.

(7.6) The following is a continuation of (7.4).

If $J \subset N_d^{n+1}$ is a Borel subset, and $b^* \in N^{n+1}$ is

a wild card, then define b^* to be c -maximal for J if b^* has height $< d$, $b^* \cap J$ is empty, and no wild card disjoint from J properly contains b^* . This extends the definition made in (5.4).

Lemma: Let $J \subset N_d^{n+1}$ be a Borel subset, and let I be the saturation of the ideal generated by J . Then the wild card partition for I consists of the c -maximal wild cards for J .

Proof. One can prove this inductively, following (7.4). Alternatively, all elements of the wild card partition for I have height $< d$, by (5.7), since I is generated by monomials of degree $\leq d$. Since I is saturated, all elements of the wild card partition for I have rank ≥ 0 , by (6.2). Rank ≥ 0 , height $< d$ wild cards have a nonempty intersection with N_d^{n+1} , and the inclusion relationships among them are preserved by their intersections with N_d^{n+1} . Thus, a wild card is c -maximal for J iff it is c -maximal for I , so the result follows by the proof of (5.9). \square

(7.7) Lemma: Let $J \subset N_d^{n+1}$ be a Borel subset, and let $I \subset N^{n+1}$ be the saturation of the ideal generated by J . Then the following are equivalent:

- (a) J is a lexicographic subset of N_d^{n+1} ;
- (b) For nonnegative integers a_0, \dots, a_{n-1} so $a_0 + \dots + a_{n-1} \leq d$, the wild card partition B for I is

given by

$$B = \{(a_0, \dots, a_{i-1}, b, *, \dots, *) \mid i = 0, \dots, n-1 \text{ and } 0 \leq b < a_i\}.$$

Proof. (a) \implies (b): Let $\vec{a} = (a_0, \dots, a_n)$ be the least element of J in the lexicographic order; a_0, \dots, a_{n-1} are the desired integers. The union of the elements of B is disjoint from J , and includes every monomial in $N_d^{n+1} \setminus J$. B consists of c -maximal wild cards for J , so by the preceding remark, B consists of every c -maximal wild card for J . By (7.6), B is the wild card partition for I .

(b) \implies (a): If we define $a_n = d - a_0 - \dots - a_{n-1}$, then $J = N_d^{n+1} \setminus \cup B$ consists precisely of the monomials in N_d^{n+1} which are $\geq_{\text{lex}} (a_0, \dots, a_n)$, so J is a lexicographic subset. \square

(7.8) Lemma: Let $L \subset N_d^{n+1}$ be an ideal generated by a lexicographic subset of N_d^{n+1} . Then L is a lexicographic ideal.

Proof. We need to show that $(L)_j$ is a lexicographic subset of N_j^{n+1} for each $j \geq d$. By (7.2), L is generated by a Borel subset of N_d^{n+1} , so L is a Borel ideal. By (4.5), L is saturated in degrees $\geq d$, so for $j \geq d$, $(L)_j$ is described by the wild card partition for L^{sat} . The result now follows by the reasoning of (7.7). \square

(7.9) Proposition: There exists a unique saturated

lexicographic ideal $L \subset N^{n+1}$ for each sequence $m_0 \geq \dots \geq m_s > 0$, with $s \leq n-1$, so S/L has Hilbert polynomial $g(m_0, \dots, m_s; z)$. The highest degree of a minimal generator for L is m_0 .

Proof. The form of the wild card partition B for any such L is given by (7.7b). Given such integers a_0, \dots, a_{n-1} , we can compute m_0, \dots, m_s . B consists of one wild card of each height h for $0 \leq j < a_0 + \dots + a_{n-1}$. In this order, the ranks of these wild cards form a nonincreasing sequence, with a_{n-1-i} wild cards of each rank i . Following the computation of m_0, \dots, m_s in (6.5), one sees that $m_i = a_i + \dots + a_{n-1}$ for each i , so by adept choice of the integers a_0, \dots, a_{n-1} , any sequence $m_0 \geq \dots \geq m_s > 0$ is obtainable.

Since the maximum height of a wild card for L is m_0-1 , it follows from (5.7) and (5.8) that the highest degree of a minimal generator for L is m_0 . \square

It is helpful to follow this proof on example (7.5). This result is due to Macaulay [Mac27].

§8 The Extreme Behavior of the Lexicographic Ideal

(8.1) Lemma: Let J be a Borel subset of N_d^{n+1} , and let L be a lexicographic subset with at most the same number of elements: $\#(L) \leq \#(J)$. Let H be the hyperplane $x_n = 0$, so $J_H = J \cap N_d^n$, and $L_H = L \cap N_d^n$. Then $\#(L_H) \leq \#(J_H)$.

Proof. Express N_d^{n+1} as the union, $N_d^n \cup x_n N_d^{n+1}$, of its elements with zero and nonzero last coordinate, respectively. We construct J, L by removing elements from N_d^{n+1} until we are left with the desired sets. In this framework, the lemma asserts that the number of elements removed from N_d^n in the construction of L bounds the number removed in the construction of J .

A wild card $a^* \in N^{n+1}$ will be said to complement J (or L) if a^* is disjoint from J (or L), and a^* intersects N_d^{n+1} , i.e. has height $\leq d$. We specifically include nonmaximal wild cards, with respect to inclusion, in the following argument.

The number of elements removed from N_d^n in the construction of J is then given by the number of rank 1 wild cards which complement J , and similarly for L . Denote these quantities by $r_1(J), r_1(L)$. More generally, let $r_i(J), r_i(L)$ denote the number of rank i wild cards which complement J, L .

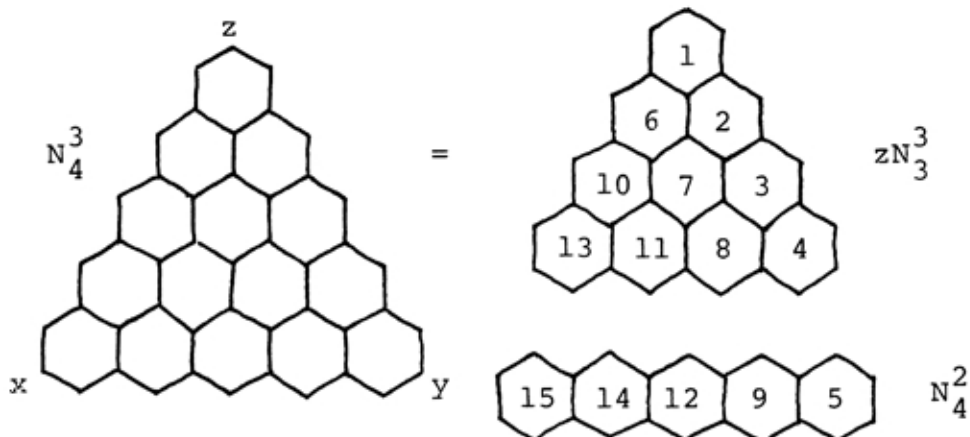
Our inductive hypothesis is then that $r_i(L) \geq r_i(J)$ for each $i = 1, \dots, n$. This claim is clear

if $J, L \subset N_d^1$ or N_0^{n+1} ; we prove it for

$N_d^{n+1} = N_d^n \cup x_n N_{d-1}^{n+1}$, assuming the claim on these two pieces.

It is helpful to imagine the process of carving N_d^{n+1} down to J or L as a game, where after removing each element, one must leave a Borel subset, and the object is to remove as many elements as possible from N_d^n . There is no harm in imposing the additional requirement that a Borel subset is left after each step, since the partial order constructed from σ and \geq in (3.11) can be refined to a total order in such a way that J (or L) is a section of the order. Then this order specifies a sequence of monomials to remove from N_d^{n+1} , so each intermediate step is a Borel subset. This additional requirement makes the following argument easier to visualize.

We describe the lexicographic strategy for this game, using N_4^3 as an example:

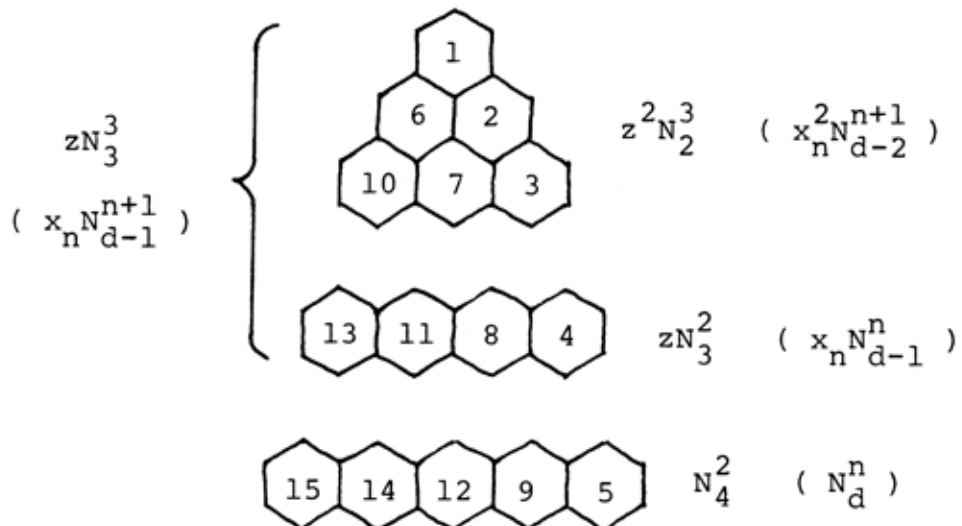


The cells on the right are numbered in increasing lexicographic order, the order in which they are removed

under this strategy. We take away elements of $(0,*,*)$ until scoring a removal in N_4^2 , then we work along $(1,*,*)$, etc.. When $(3,*,*)$ is removed, the sole element of $(4,*,*)$, in N_4^2 , can be removed without further preparation in zN_3^3 . This completes the removal of the rank 2 wild card $(*,*,*)$.

Note that by the requirement that we leave a Borel subset, the element $(a_1, \dots, a_s, 0, \dots, 0)$ of the wild card $(a_1, \dots, a_{s-1}, *, \dots, *)$ must under any circumstances be removed last.

We now refine our analysis of this game, to clarify the induction. Further divide $x_n N_{d-1}^{n+1}$ into parts $x_n^2 N_{d-2}^{n+1}$ and $x_n N_{d-1}^n$:



Once we have removed an element from $x_n N_{d-1}^n$, completing a rank 1 wild card in $x_n N_{d-1}^{n+1}$, it becomes permissible to remove the corresponding element of N_d^n , completing that same wild card in N_d^{n+1} , as long as this leaves a Borel

subset of N_d^n . The lexicographic strategy does so at the next turn. Furthermore, if we have completed a rank 2 or higher wild card in $x_n N_{d-1}^{n+1}$, it also becomes possible to remove elements, without further preparation, from N_d^n , completing these same wild cards in N_d^{n+1} . The lexicographic strategy does so before playing back in $x_n N_{d-1}^{n+1}$: the removal of $(a_0, \dots, a_s, 0, \dots, 0, 1)$ is followed by the removal of $(a_0, \dots, a_s, 0, \dots, 0, 1, 0), \dots, (a_0, \dots, a_{s+1}, 0, \dots, 0), (a_0, \dots, a_{s-1}, *, \dots, *)$.

Thus, to receive maximum scoring potential from a given allocation of moves within $x_n N_{d-1}^{n+1}$, one wants to maximize the number of wild cards of any rank ≥ 1 completed within $x_n N_{d-1}^{n+1}$. This sum is precisely the number of moves then playable within the scoring zone N_d^n . By induction, there is no better allocation of moves within $x_n N_{d-1}^{n+1}$ than that given by the lexicographic order.

Since the lexicographic strategy plays within N_d^n as soon as permissible, there can be no way to allocate fewer moves to $x_n N_{d-1}^{n+1}$ than the lexicographic strategy does, and then to be able to play any extra moves as scoring moves within N_d^n . Thus $r_1(L) \geq r_1(J)$.

The rest of the inductive assertion follows from two observations. First, L_H is a lexicographic subset of N_d^n , so we can assume our results there. Second, the rank i wild cards which complement L_H, J_H correspond exactly to rank $i+1$ wild cards complementing L, J .

Thus, by applying the induction assertion to L_H, J_H , we find that $r_i(L) \geq r_i(J)$ for $i = 1, \dots, n$.

This completes the proof. \square

(8.2) Proposition: Let $I \subset S$ be a Borel ideal, generated by elements of degree $\leq d$. Let $L \subset S$ be a lexicographic ideal, also generated by elements of degree $\leq d$.

(a) If $\dim(I)_z \geq \dim(L)_z$ holds for $z = d$, then this holds for all $z \geq d$.

(b) If $\dim(I)_z > \dim(L)_z$ holds for $z = d$, then this holds for all $z \geq d$.

(c) If $\dim(I)_z = \dim(L)_z$ holds for $z = d$ and $z = d+1$, then this holds for all $z \geq d$.

Proof. Let H be the hyperplane $x_n = 0$, and let I, L be the sheafifications of I, L on P^n . By (2.2), (4.3) we have exact sequences

$$0 \rightarrow I(-1) \rightarrow I \rightarrow I_H \rightarrow 0,$$

$$0 \rightarrow L(-1) \rightarrow L \rightarrow L_H \rightarrow 0.$$

We have $h^0(I(z)) = \dim(I)_z$ for $z \geq d$, since by (4.5) I is saturated in degrees $\geq d$. Thus $\dim(I)_{z+1} - \dim(I)_z = \dim(I_H)_{z+1}$ for $z \geq d$, and similarly for L, L_H .

To prove (a), it suffices to show that $\dim(I)_{d+1} \geq \dim(L)_{d+1}$; higher degrees then follow by induction, since $(L)_{d+1}$ is a lexicographic subset by (6.9). By the above, we need only to show that

$\dim(I_H)_{d+1} \geq \dim(L_H)_{d+1}$. It follows from (6.8) that $\dim(I_H)_d \geq \dim(L_H)_d$. The result, trivial when $n = 1$, now follows by induction.

To prove (b), note that if $\dim(I)_d > \dim(L)_d$, then L can be enlarged in degree d , while preserving the applicability of (a). Since L was already saturated in degrees $\geq d$, these additional generators will increase the dimension of L in every higher degree. This gives a strict inequality for every $z \geq d$.

To prove (c), note that the hypothesis implies that $\dim(I_H)_{d+1} = \dim(L_H)_{d+1}$. Since by (6.8), $\dim(I_H)_d \geq \dim(L_H)_d$, it follows from (b) that in fact, $\dim(I_H)_d = \dim(L_H)_d$. The result, trivial when $n = 1$, now follows by induction. \square

(8.3) The reader may find the two dimensions of $k[x,y,z]$, P^2 inadequate for visualizing the proofs of this section, or may wish to consider P^3 for other reasons, such as the desire to study space curves. By a fortunate accident, Borel subsets of N_d^4 are easily modeled.

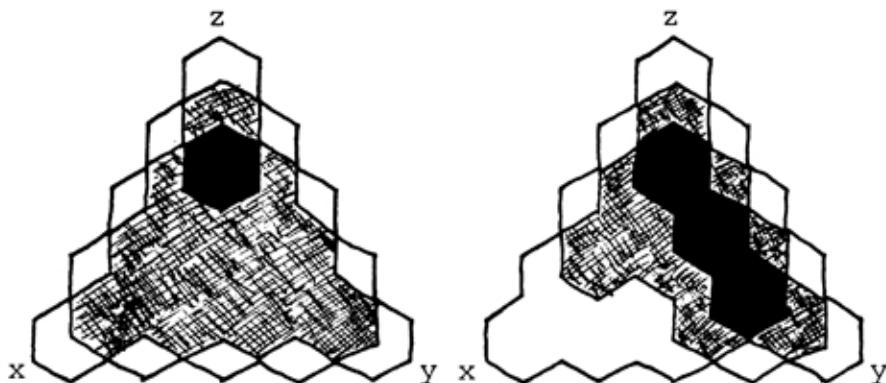
Arrange the degree d monomials of $k[w,x,y,z]$ in a pyramid with peak w^d , and base corners x^d, y^d, z^d , generalizing the discussion in (3.8). Consider the complement of a Borel subset $J \subset N_d^4$, in terms of the requirement given by (3.7). Each layer described by a constant power w^i of w must look like the complement of

a Borel subset of N_{d-i}^3 ; this can be imagined as described in (3.8). Furthermore, if $(q,r,s,t) \notin J$, with $q > 0$, then none of

$$(q-1,r+1,s,t), (q-1,r,s+1,t), (q-1,r,s,t+1)$$

can belong to J . This gives (q,r,s,t) a complete base of monomials to rest on, in the layer for w^{q-1} , if one assumes gravity.

The gist of this is that one can build a model for the complement of any Borel subset of N_d^4 , by stacking hex nuts from a hardware store, and the resulting structure will be stable. Alternatively, one can draw overlapping silhouettes for each layer, and make sense of the resulting diagram. We draw the complements of two Borel subsets of N_4^4 , where the peak w , rising out of the page, is not labeled. One describes a lexicographic subset, and the other a different Borel subset; the complements of each consist of 26 monomials:



§9 Characteristic Zero Results

(9.1) Throughout this section, we let $S = k[x_0, \dots, x_n]$, where k is restricted to be an algebraically closed field of characteristic zero.

The following lemma strengthens the argument made in (3.6)

Lemma: Let $S = k[x, y]$, and let V be a subspace of S_d . Let $\text{char } k = 0$. Let $g^c \in T(2)$ be the matrix

$$g^c = \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} .$$

In terms of the coordinate system on S_d given by the basis consisting of monomials, represent V by an $r \times (d+1)$ matrix whose r rows are a basis for V . Then for all but finitely many values of c , $g^c V$ has a matrix representation whose $r \times r$ minor consisting of the first r columns is nonzero.

Proof. The $r \times r$ minors of $g^c V$, which projectively give the Plücker coordinates of $g^c V$, can be computed by applying a matrix derived from g^c to the $r \times r$ minors of V . We study this matrix.

g^c acts on S_d via the matrix

$$\begin{bmatrix} 1 & c & c^2 & c^3 & \dots \\ 0 & 1 & \binom{2}{1}c & \binom{3}{1}c^2 & \\ 0 & 0 & 1 & \binom{3}{2}c & \\ 0 & 0 & 0 & 1 & \\ \vdots & & & & \end{bmatrix}$$

The matrix which acts on the $r \times r$ minors of V is given by the $r \times r$ minors of this matrix. We are only interested in the minors obtained by choosing rows $1, \dots, r$, and columns i_1, \dots, i_r . These minors have the form

$$\left| \begin{bmatrix} \binom{i_1}{0^1} & \binom{i_2}{0^2} & \dots \\ \binom{i_1}{1^1} & \binom{i_2}{1^2} & \\ \vdots & & \end{bmatrix} \right| c^j,$$

where $j = i_1 + \dots + i_r - 1 - \dots - r$. By elementary row operations, the determinant shown can be reduced to the Vandermonde determinant

$$\begin{vmatrix} \begin{bmatrix} 1 & 1 & 1 & \dots \\ i_1 & i_2 & i_3 \\ i_1^2 & i_2^2 & i_3^2 \\ \vdots \end{bmatrix} \end{vmatrix} .$$

This determinant is known to be nonzero for distinct integers i_1, \dots, i_r . Thus, given the $r \times r$ minors of V , the first $r \times r$ minor of $g^c V$ can be computed as a polynomial in c .

It remains to be seen that this polynomial is not identically zero; we do not want like powers of c to cancel. However, among the minors of V , there is a unique nonzero minor so $i_1 + \dots + i_r$ is minimal: choose i_1, \dots, i_r to be the columns containing lead ones when the matrix for V is in row reduced form. Thus, the corresponding power of c has a nonzero coefficient.

Therefore, for any choice of c not a root of this polynomial, the first $r \times r$ minor of $g^c V$ is nonzero. \square

(9.2) Lemma: Let I be a homogeneous ideal. Let $\text{char } k = 0$. There exists a change of coordinates $g \in T(n+1)$, and a multiplicative order $>$ on N^{n+1} , so $\text{in}(gI)$ is a Borel ideal.

Proof. Consider the subspace $(I)_d$ of S_d . Let $>_{\text{lex}}$ be the lexicographic order on N_d^{n+1} . $>_{\text{lex}}$ can be induced on N_d^{n+1} by the grading $q = ((d+1)^n, \dots, d+1, 1)$, by (I,1.9). $\text{in}(I)_d$ is spanned by the monomials associated with the lead terms of a basis for $(I)_d$, if such a basis is chosen so no two basis elements begin with the same lead term. Define the weight of $\text{in}(I)_d$ to be the sum of the degrees of its monomial basis, with respect to the above grading q . Note that this weight is bounded.

Suppose that $\text{in}(I)$ is not a Borel subset of N_d^{n+1} . Choose i, j so condition (3.7b) fails, and define $g_{ij}^c \in T(n+1)$ to be an identity matrix except for an (i, j) entry of c . Consider the decomposition $S_d = \bigoplus_b W_b$ induced by g_{ij}^c , analogous to the decomposition studied in the proof of (3.7).

The monomials of $\text{in}(I)_d$ are partitioned according to which summand W_b contains them. Consider the effect of g_{ij}^c on the above basis for $(I)_d$ yielding these monomials; the occupancy numbers of the above partition are seen to be the same for $\text{in}(g_{ij}^c I)_d$. Within each summand W_b by (7.1) all but finitely many choices for c will yield the lexicographically greatest monomials as the elements of $\text{in}(g_{ij}^c I)_d$. Choose a c which does this for each summand W_b ; since $\text{in}(I)_d$ failed condition (3.7b) on i, j , the weight of $\text{in}(g_{ij}^c I)_d$ must be greater than the weight of $\text{in}(I)_d$. Since this weight is bounded, if

we were only concerned with $(I)_d$, we could realize the g claimed in the lemma as the composition of finitely many such g_{ij}^c .

The above argument extends to $I \in S$ in all degrees, by repeated use of the noetherian property of S . \square

(9.3) Consider I as a point on the appropriate Hilbert scheme. The orbit of I under $T(n+1)$ has points in its closure which are fixed by $T(n+1)$. In characteristic zero, these points correspond to Borel ideals. One expects, according to general principles, to be able to realize such a point as a point in the closure of the orbit of I by a one parameter subgroup of $T(n+1)$ (see [Mum65, chapter 2]). Such a one parameter subgroup, once diagonalized by a suitable change of coordinates, can be thought of as inducing a multiplicative order, based on the weights it induces on monomials. While we have proved (9.2) directly, its truth was first inferred by the above reasoning. See chapter V for an elaboration of this line of reasoning.

(9.4) Proposition: Let I be an ideal sheaf on P^n , with $\text{char } k = 0$. Suppose that $\chi(O/I)(z) = g(m_0, \dots, m_s; z)$. Then

- (a) $m_0 \geq \dots \geq m_s > 0$;
- (b) I is m_0 -regular.

Proof. Following (9.2), we make a change of coordinates, and choose a multiplicative order \succ so if $I = \bigoplus H^0(I(z))$, then $\text{in}(I)$ is a Borel ideal. Since I and $\text{in}(I)$ have the same Hilbert function, by (I,1.5), (a) follows from (6.5a).

If $\text{in}(I)$ denotes the ideal sheaf for $\text{in}(I)$, then $\text{in}(I)$ is m_0 -regular by (6.11). Using the flat family constructed in (I,2.12), $\text{in}(I)$ can be taken to be the special fiber of a flat family of coherent sheaves with general fibers all isomorphic to I . It follows from the upper semicontinuity of cohomology groups on flat families that $h^i(\text{in}(I)(z)) \geq h^i(I(z))$ for every i, z . (See [Har77, III12.8]). Thus, I is m_0 -regular, proving (b). \square

The history of this result will be discussed in (10.3).

(9.5) Proposition: Let $I \subset S$ be an ideal, generated by elements of degree $\leq d$. Let $\text{char } k = 0$. Let $L \subset S$ be a lexicographic ideal, also generated by elements of degree $\leq d$.

(a) If $\dim(I)_z \geq \dim(L)_z$ holds for $z = d$, then this holds for all $z \geq d$.

(b) If $\dim(I)_z > \dim(L)_z$ holds for $z = d$, then this holds for all $z \geq d$.

(c) If $\dim(I)_z = \dim(L)_z$ holds for $z = d$ and $z = d+1$, then this holds for all $z \geq d$.

Proof. As in (9.2), we make a change of coordinates, and choose a multiplicative order $>$ so $\text{in}(I)$ is a Borel ideal. I and $\text{in}(I)$ have the same Hilbert function, by (I,1.5). Let J be the ideal generated by $\text{in}(I)_d$. Then $\dim(I)_z \geq \dim(J)_z$ for each $z \geq d$. (a) and (b) follow from this inequality, and (8.2).

For (c), we have $\dim(J)_z = \dim(L)_z$ for all $z \geq d$, by (8.2c). The ideal sheaf associated with J is d -regular, by (6.9). Since J itself is generated entirely by monomials of degree d , it follows from (2.7) that a minimal set of 1^{st} syzygies among these monomials are all of degree $d+1$.

We assert that a k -basis for $(I)_d$, whose lead terms generate J , is in fact a standard basis for I . Let m_1, \dots, m_q be such a k -basis. It suffices by (I,2.9) to check that

$$(m_i \text{ S } m_j) \text{ R } m_1, \dots, m_q = 0$$

for all pairs i, j corresponding to the above degree $d+1$ syzygies. Since $(I)_{d+1}$ has as small dimension as possible, by part (a), there is no room for the above test (I,2.9) to fail. In other words, $\dim(I)_{d+1} = \dim(J)_{d+1}$, so every element of $(I)_{d+1}$ will have remainder zero with respect to m_1, \dots, m_q , including the elements $m_i \text{ S } m_j$ under consideration.

Thus, $\text{in}(I)_z = (J)_z$ for $z \geq d$. Since the result holds for J , by (8.2c), and I and $\text{in}(I)$ have the same

Hilbert function, by (I,1.5), the result follows. \square

The history of this result will be discussed in (10.3).

§10 Characteristic Free Results

(10.1) We allow k to be an algebraically closed field of any characteristic.

Proposition: Let $M = \bigoplus_i \mathcal{O}_P(e_i)$, $e_i \geq 0$, be a free sheaf on P^n , generated by global sections as an \mathcal{O}_P -module.

Let F be a coherent sheaf, generated by global sections. F can be considered as a quotient of M above, for suitable choices of the e_i .

Alternatively, fix M , and let I be a submodule of M .

In either case, we obtain the exact sequence

$$0 \longrightarrow I \longrightarrow M \longrightarrow F \longrightarrow 0.$$

Let $p(z) = \chi(F(z))$ be the Hilbert polynomial of F . Then

- (a) $p(z) = g(m_0, \dots, m_s; z)$ for integers $m_0 \geq \dots \geq m_s > 0$;
- (b) I is m_0 -regular;
- (c) F is (m_0-1) -regular.

Proof. Let M be the S -module associated to M , and let I be the saturated submodule of M associated to I . Choose a multiplicative order (I,1.1) on M , and form $\text{in}(I)$. Let $\text{in}(I)$ be the associated coherent sheaf, which is a submodule of M . $M/\text{in}(I)$ has the same Hilbert polynomial $p(z)$ as F , by (I,1.5). $M/\text{in}(I)$ is a direct sum of nonnegatively twisted structure sheaves defined by monomial ideals. Each such structure sheaf satisfies (a)

by (8.2a), since the Hilbert function of the quotient of a monomial ideal is independent of the characteristic of k , being a combinatorial phenomenon inside N^{n+1} . By (1.14), each structure sheaf still satisfies (a) after twisting by $e_i \geq 0$. Thus, the direct sum $M/\text{in}(I)$ satisfies (a), since by (1.13), the sum of polynomials of the form (a) is again of the form (a). This proves (a).

Assume inductively that (b) holds on P^{n-1} . We prove (b) first for monomial ideal sheaves I on P^n . If $\chi(O/I)(z) = g(m_0, \dots, m_s; z)$, then for a hyperplane H not containing any associated primes of I ,

$$\chi(O_H/I_H)(z) = g(m_1, \dots, m_s; z) \text{ by (2.8).}$$

Since $m_0 \geq m_1$, I_H is m_0 -regular, by (2.3a) and the inductive hypothesis. To show that I is m_0 -regular, it suffices by (2.6b) to show that

$$h^0(O/I)(m_0-1) = g(m_0, \dots, m_s; m_0-1).$$

The corresponding ideal sheaf in characteristic zero is m_0 -regular, by (9.4b), so the above equality holds in characteristic zero, by (2.5). As remarked above, Hilbert functions of monomial ideals are independent of the characteristic, so the above equality always holds. Thus, monomial ideals I are m_0 -regular.

Now, if I is an arbitrary submodule of M , by (I,2.12) there exists a flat family of coherent sheaves with general fibers all isomorphic to I , and central fiber $\text{in}(I)$. $\text{in}(I)$ is a direct sum of twisted monomial ideals,

as remarked above. By the m_0 -regularity of monomial ideal sheaves, the twisting and addition formulas (1.13), (1.14), and the property (2.3a) of m -regularity, it follows that $\text{in}(I)$ is m_0 -regular.

We now argue as in (9.4b). On flat families, the ranks of cohomology groups vary upper semicontinuously. See [Har77, III12.8]. In particular, the vanishing of certain cohomology groups for $\text{in}(I)$ forces the corresponding vanishing for I . Thus, I is m_0 -regular, proving (b).

(c) is an immediate consequence of (b), using the given exact sequence. \square

The history of this result will be discussed in (10.3).

Note that the above argument in fact shows that $H^i(I(z-i)) = (0)$ for $i \geq 1$, $z \geq m_{i-1}$. This gives an interpretation of each integer m_i .

(10.2) The following result extends (9.5) to any characteristic.

Proposition: Let $I \subset S$ be an ideal, generated by elements of degree $\leq d$. Let $L \subset S$ be a lexicographic ideal, also generated by elements of degree $\leq d$.

(a) If $\dim(I)_z \geq \dim(L)_z$ holds for $z = d$, then this holds for all $z \geq d$.

(b) If $\dim(I)_z > \dim(L)_z$ holds for $z = d$, then

this holds for all $z \geq d$.

(c) If $\dim(I)_z = \dim(L)_z$ holds for $z = d$ and $z = d+1$, then this holds for all $z \geq d$.

Proof. As in the proof of (10.1), note that the Hilbert function of a monomial ideal is characteristic free. Thus, (a), (b), (c) hold in any characteristic for monomial ideals.

We argue exactly as in (9.5), replacing the use of Borel ideals by monomial ideals, and skipping the preliminary change of coordinates.

Let J be generated by $\text{in}(I)_d$; $\dim(I)_z \geq \dim(J)_z$ for each z . The monomial ideal J satisfies (a), (b), (c) by the above argument. This proves (a), (b).

In the case of (c), it follows that J and L have the same Hilbert polynomial. Let this polynomial be $g(m_0, \dots, m_s; z)$. By (7.9), $m_0 \leq d$, since L is generated in degrees $\leq d$. By (10.1) and (2.3a), the ideal sheaf J associated to J is d -regular. Thus, (2.7) applies to J , so a minimal set of 1^{st} syzygies among the generators of J are all of degree $d+1$. As in (9.5), it follows from (I, 2.9) and the minimum growth of J that $\text{in}(I)_z = (J)_z$ for $z \geq d$, proving (c). \square

(10.3) We discuss the history of (10.1), (10.2). Note that (10.1) generalizes (9.4), and (10.2) generalizes (9.5).

(10.2a), (10.2b) were proved by Macaulay [Mac27].

He used (I,1.5) to reduce to a monomial ideal, and then proceeds with a direct combinatorial argument, which he prefaced with the amusing disclaimer,

"Note.- This proof of the theorem which has been assumed earlier is given only to place it on record. It is too long and complicated to provide any but the most tedious reading."

A number of simpler proofs followed; see [Sta78] for a good bibliography. The proof offered here, by reduction to Borel ideals in characteristic zero, is more geometric than preceding arguments. The combinatorics lacking a geometric interpretation is confined to (8.1). It seems that such an obvious statement as (8.1) should admit a shorter proof, but this author has discarded many false arguments for (8.1) without finding one.

(10.1a) was proved by Macaulay [Mac27] for the case of an ideal, in the same manner that he proved (10.2a,b). Hartshorne [Har66] gives an independent proof for the case of an ideal, by considering special subschemes of P^n called fans. The notation $g(m_0, \dots, m_s; z)$ is from his treatment; the present author has found it more workable (see §1) than the alternatives in the literature.

(10.1b) was proved in the case where I is an ideal sheaf, by Gotzmann [Got78]. He combines (10.2a,b) with (2.6) to obtain an extremely short proof by induction.

The deformation argument as given here for the general case has been adapted to take advantage of the ideas in his proof, which does not generalize without the tools developed here.

(10.2c) was proved by Gotzmann [Got78]. We have simplified his argument by the use of (I,2.9), as described in the proof of (9.5c).

(10.4) The following result is essential to analyzing the complexity of the division algorithm (I,§2). See chapter III for further discussion.

Proposition: Let M be a free S -module, generated by elements of degree ≤ 0 , and let I be a saturated submodule of M , so M/I has Hilbert polynomial $p(z) = g(m_0, \dots, m_s; z)$. Then $\text{in}(I)$ is generated by elements of degree $\leq m_0$.

Proof. Let $I \subset M$ be the coherent sheaves associated to $I \subset M$. Note that by (10.1), $m_0 \geq \dots \geq m_s > 0$, and I is m_0 -regular.

First, consider the case where $I \subset S$ is a saturated ideal. $\text{in}(I)$ need not be saturated; see example (I,1.4). However, I and $\text{in}(I)$ have the same Hilbert function, by (I,1.5). Let L be the saturated lexicographic ideal with the same Hilbert polynomial, as in (7.9). By (7.9), L is generated in degrees $\leq m_0$. By (2.5), the Hilbert functions for I , $\text{in}(I)$, L all agree in

degrees $\geq m_0 - 1$. Let J be the ideal generated by $\text{in}(I)_{m_0}$. Applying (10.2a), $\dim(J)_z \geq \dim(L)_z$ for each $z \geq m_0$. Since $J \subset \text{in}(I)$, in fact J and $\text{in}(I)$ agree as ideals for all degrees $\geq m_0$. Thus, $\text{in}(I)$ is generated by elements of degree $\leq m_0$.

In short, because $\text{in}(I)$ is growing in dimension at the slowest possible rate, given by (10.2), in degrees $\geq m_0$, there is no room for $\text{in}(I)$ to have a generator of degree $> m_0$.

Now, consider the general case where I is a submodule of M . The above argument carries over intact, with the help of (1.13), (1.14). $\text{in}(I)$ is a direct sum of nonnegatively twisted monomial ideals. Each such twisted ideal must be growing in dimension at the slowest possible rate in degrees $\geq m_0$. By the addition and twisting formulas (1.13), (1.14), any deviation from this rate would show up as a discrepancy between the Hilbert function and the Hilbert polynomial of $\text{in}(I)$. By (2.5), this cannot happen, since I is m_0 -regular. Thus, there is no room for $\text{in}(I)$ to have a generator of degree $> m_0$. \square

(10.5) The m -regularity bound given by (10.1) is precise. By (7.9), the saturated lexicographic ideal with quotient Hilbert polynomial $g(m_0, \dots, m_s; z)$ has a generator of degree m_0 . By (2.3b), the associated ideal sheaf cannot be better than m_0 -regular.

Lexicographic ideals generally define nonreduced

subschemes of P^n , with multiple embedded components. If one puts additional assumptions on the subscheme X defined by an ideal I , one finds that the cohomology of I vanishes in considerably lower degrees. For example, if X is a 1-dimensional subscheme of P^n , of degree d with arithmetic genus g , then by (1.17),

$$m_0 = \binom{d}{2} + 1 - g.$$

On the other hand, if X is a reduced, irreducible curve of codimension r in the smallest linear space containing it, then I is m -regular for

$$m = d + 1 - r.$$

This has been proved by Rob Lazarsfeld. It is suspected by various people that this formula can be extended to higher dimensional X .

Thus, multiple and embedded components tend to increase the least m for which I is m -regular.

A lexicographic ideal L can easily occur as $\text{in}(I)$ for an arbitrary ideal I , since L is Borel fixed. From the proof of (9.2), one sees that $\text{in}(I)$ will be Borel fixed in characteristic zero for a generic coordinate system. Thus, (10.4) not only gives a sharp bound, but gives a good indication of usual behavior; by the preceding discussion, Borel fixed ideals are likely to be m -regular only for m relatively close to m_0 .

Chapter III

On the Complexity of the Division Algorithm

§1 Problems Arising from Algebraic Geometry

(1.1) Within algebraic geometry, there are two related categories for which the division algorithm is well-suited. These are the category of subschemes of a fixed projective space P^n , and the category of coherent sheaves defined on a fixed projective space P^n . Both of these situations can be studied via exact sequences

$$0 \longrightarrow I \longrightarrow M \longrightarrow F \longrightarrow 0$$

of the type considered in (II,10.1), where I is a subsheaf of the free \mathcal{O}_P -module M . The division algorithm can be used to study this sequence, by considering the corresponding saturated submodule I of the graded free S -module M .

Two aspects of the typical situation turn out to be crucial in determining the complexity of constructing a standard basis for I . First, the n of P^n is often fixed. Second, one often knows the Hilbert polynomial $\chi(F(z))$, or at least anticipates what it might be, so m_0 can be considered known.

It is precisely for fixed P^n , and for saturated submodules $I \subset M$, that (II,10.4) can be applied to bound the complexity of constructing a standard basis for I , in terms of m_0 . If $\text{in}(I)$ is constructed degree by degree, one enumerates a minimal generating set for $\text{in}(I)$, as a standard basis for I is built. (II, 10.4) bounds this generating set for $\text{in}(I)$: its elements are all of degree

$\leq m_0$.

The affine case $I \subset M$, where M is a nongraded A -module, as in the notation of chapter I, can be understood in terms of this result. First, one can add a homogenizing variable, to retreat to the graded case. There is not a 1:1 correspondence between standard bases in the two cases, as more simplifications become possible in the affine setting where the distinction between powers of the homogenizing variable is blurred, but a standard basis for the graded case does dehomogenize into a standard basis for the affine case. Second, by adding one more variable and ignoring it completely, any graded submodule of the original free module becomes a saturated submodule of the new free module. Geometrically, this is because any embedded components supported at the vertex of the affine cone over the original projective object become legitimate components, visible in the new projective space. Thus, with suitable preparation, the cohomological interpretation of the division algorithm given by (II,10.4) applies to the general case.

There are two motivations for the organization of this chapter into the two groupings of algebraic geometry and complexity theory. First, the number of variables arising in problems from complexity theory is seldom fixed, in contrast to problems from algebraic geometry; the cohomological interpretation (II,10.4) is insufficient to yield interesting bounds on the behavior of the division

algorithm when the number of variables is not fixed. Second, while it is reasonable to group inputs to the division algorithm according to m_0 in the case of algebraic geometry, the relation of m_0 to the size of inputs arising from complexity theory is certainly erratic, and not understood.

In the above algebraic geometry setting, the division algorithm appears to be a tractable approach to tackling natural problems, as (1.2), (1.3) reveal. Experience is bearing this out.

(1.2) Proposition: Let I be a saturated submodule of the free S -module M , so M/I has Hilbert polynomial $p(z) = g(m_0, \dots, m_s; z)$. Then the construction of the reduced standard basis for I requires a number of field operations which is a polynomial in m_0 .

Proof. We show that the number of terms collectively of all members of the reduced standard basis for I is a polynomial in m_0 . It is apparent, but we do not justify rigorously, that the number of field operations involved in the construction of this basis is a polynomial in the above quantity.

The number of monomials in M of degree $\leq m_0$ is a polynomial in m_0 . The reduced standard basis for I is in 1:1 correspondence with a minimal set of generators for $\text{in}(I)$. By (II,10.4), each element of this basis is of degree $\leq m_0$. Thus, the number of possible elements, and

the number of terms of each element, are each bounded by a polynomial in m_0 . The product of these polynomials bounds the total number of possible terms in this basis. \square

The above argument relies on a careful analysis of the degrees of standard basis elements, and a very loose analysis of the number of terms arising in the computation. One does much better than the above analysis indicates, in terms of the cardinality of $\text{in}(I)$. For example, the first generator of $\text{in}(I)$ itself generates a principal submodule of M , immediately reducing the degree of the polynomial giving the number of remaining generators possible within that summand of M . Our naive analysis simply subtracts 1 from the count. How much better one does, however, is not understood.

Over a finite field, the cost of each field operation can be considered constant, as we are not making field extensions; the above result asserts in this case that the complexity of constructing a standard basis is polynomial time. In characteristic zero, one sees already in use of the euclidean algorithm a possible explosion in the size of integer coefficients. We make no attempt to analyze this effect. It is nice to be able to work in characteristic zero, but one should be prepared to jump ship when necessary. Characteristic p is for many reasons computationally more attractive.

(1.3) Corollary: Let I be a saturated ideal in S , defining a degree d , genus g curve $X \subset \mathbb{P}^n$. Then the number of field operations required to construct a standard basis for I is a polynomial in d .

Proof. By (II,1.17),

$$m_0 = \binom{d}{2} + 1 - g.$$

The result now follows from (1.2). \square

Without further improvements, the study of curves in \mathbb{P}^3 may be by far the most reasonable application for the division algorithm within algebraic geometry. Our estimate, as it stands, is exponential in the n of \mathbb{P}^n .

(1.4) Buchberger, in [Buc79], bounds the degrees of a standard basis for I , when I is an ideal in $k[x,y]$. He does not assume that I is saturated.

(1.5) There is a practical point to studying the complexity of algorithms: one cannot look for bargains until one knows the going price of something. Here, the cohomology interpretation (II,10.4) of the complexity of the division algorithm indicates that substantial savings in computation can be achieved in certain situations where it is not actually necessary to compute the entire standard basis.

Suppose I defines an irreducible, reduced curve $X \subset \mathbb{P}^n$, and for example, we wish to either

- (a) compute the 1st syzygies of I , or

(b) compute the equations of the projection of X to a subspace of P^n .

A minimal set of syzygies for (a), or a minimal set of equations for (b), will consist of elements of degrees bounded by roughly the actual m -regularity of I , rather than the theoretical upper bound m_0 given by (II,10.1). See (II,2.2a), (II,2.4) to establish these bounds. As discussed in (II,10.5), the actual m -regularity of I grows like d , whereas the bound m_0 grows like d^2 , if X is of degree d .

When X is reduced, irreducible of higher dimension, the gulf widens considerably between the actual m -regularity of I , and m_0 . As suggested in (1.3), the very feasibility of using the division algorithm at all for higher dimensional X may depend on exploiting this gulf.

One takes advantage of the above situation by computing the standard basis for I degree by degree, and bailing out when the necessary information has been obtained. This is only possible when the m -regularity of I is known in advance. It is conceivable that a method exists for deducing when enough of the standard basis has been computed to yield whatever information is desired, for an alien I , but it seems unlikely to this author. The reader is encouraged to dispute this point.

§2 Problems Arising from Complexity Theory

(2.1) Much of this section is speculative in nature; its purpose is to indicate a number of questions that the author has been unable to answer satisfactorily.

The problem of determining if a system of polynomial equations has a common solution over an algebraically closed field is NP-hard. The problem of determining if a given polynomial belongs to a given ideal is exponential space hard [MaM81]. The division algorithm can be used to solve either of these problems.

This would seem at first to suggest that the division algorithm is an inappropriate method for the first problem. However, the behavior of the division algorithm is extremely variable; it takes very little time to construct a standard basis for certain ideals involving an arbitrary number of variables. Furthermore, the first problem may itself be exponential space hard. In this case, the systems of polynomials arising as images of NP-complete problems would be of a simpler character than those arising from exponential space complete problems.

What is the complexity of the division algorithm when applied to NP-complete problems? Its ability to handle harder problems is not necessarily an indication of its behavior here, given the variability of the size of standard bases. This question should be considered separately from any attempt to identify circumstances when the division algorithm could be of practical use; the

information obtained about the structure of NP-complete problems would be of interest in any case.

Separately, can one delineate circumstances when the division algorithm is of practical use? The spirit of the method by which NP-complete problems are translated into this setting can be used to guide other applications.

Finally, what can be said about the systems of polynomials arising from NP-complete problems, using methods of algebraic geometry? We suggest some specific directions to explore.

(2.2) We describe how to translate two different NP-complete problems into systems of polynomial equations.

For background, see [HoU79], [GaJ79]. This NP-hardness result was first observed in [FrY77].

Example: A boolean expression in 3-conjunctive normal form is defined as follows:

Let x_1, x_2, \dots be logical variables, and let \wedge, \vee, \sim denote logical *and, or, not*. Let a literal a_{ij} denote either $x_{t_{ij}}$ or $\sim x_{t_{ij}}$, and let a clause be the \vee of three literals. Then a 3-CNF boolean expression is the \wedge of arbitrarily many clauses involving arbitrarily many variables. Specifically, it is of the form

$$\bigwedge_{i=1}^p (a_{i1} \vee a_{i2} \vee a_{i3}).$$

A 3-CNF boolean expression is satisfiable if there exist

values for x_1, x_2, \dots making the expression *true*. Determining if 3-CNF boolean expressions are satisfiable is NP-complete.

To translate a 3-CNF expression into a system of polynomial equations, let the involved variables x_1, \dots, x_n generate the polynomial ring $k[x_1, \dots, x_n]$ over an arbitrary field k .

Choose two field values $T, F \in k$ to represent *true*, *false*. Create an equation for each clause by replacing each literal $a_{ij} = x_{t_{ij}}$ by $(x_{t_{ij}} - T)$, and $a_{ij} = \sim x_{t_{ij}}$ by $(x_{t_{ij}} - F)$. Replace \vee by multiplication, and set the resulting expression equal to zero. For example,

$$(x_1 \vee \sim x_2 \vee x_3) \text{ becomes } (x_1 - T)(x_2 - F)(x_3 - T) = 0.$$

Then the system of equations obtained has a solution over the algebraic closure of k if and only if the original 3-CNF expression is satisfiable, so the division algorithm is applicable.

(2.3) Example: Let G be an undirected graph on n vertices. G is 3-colorable if its vertices can be labeled from a palette of three colors, so no edge connects two vertices of the same color. Determining if a graph G is 3-colorable is an NP-complete problem.

To translate this problem into a system of polynomial equations, choose a field k containing three cube roots of unity, and use these values as colors. Represent

each vertex i of G by the variable x_i , subject to the equation

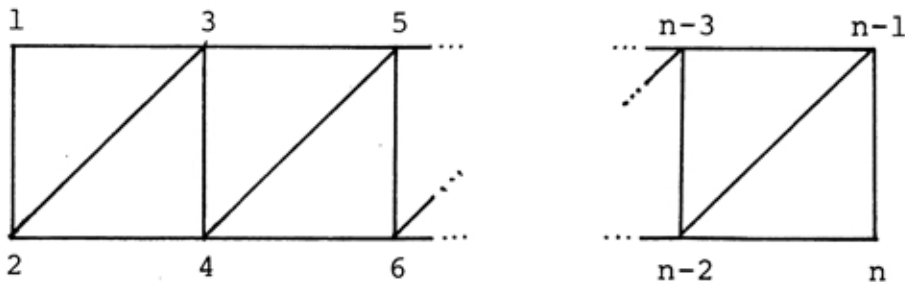
$$x_i^3 - 1 = 0.$$

Represent each edge (i,j) of G by the equation

$$x_i^2 + x_i x_j + x_j^2 = 0,$$

which enforces the requirement that adjacent vertices assume distinct colors. Then the system of equations obtained has a solution over the algebraic closure of k if and only if G is 3-colorable, so the division algorithm is applicable.

Consider the graph G shown, on n vertices $1, \dots, n$.



G is 3-colorable, as is seen if we color each vertex by its residue mod 3. We study the behavior of the division algorithm on this specific input.

Let k be the algebraic closure of $\mathbb{Z}/2\mathbb{Z}$, chosen for ease of computation. Assign variables x_i to each vertex i of G . As described above, the input equations to the division algorithm are:

$$x_i^3 + 1 = 0, \quad \text{for } i = 1 \text{ to } n;$$

$$x_i^2 + x_i x_j + x_j^2 = 0, \quad \text{for } j = i+1 \text{ or } i+2.$$

The reduced standard basis with respect to the lexicographic order is found to be

$$\begin{aligned} x_i + x_n &= 0, & 1 \leq i \leq n-2 & \text{ and } n-i \equiv 0 \pmod{3}; \\ x_i + x_{n-1} &= 0, & 1 \leq i \leq n-2 & \text{ and } n-i \equiv 1 \pmod{3}; \\ x_i + x_{n-1} + x_n &= 0, & 1 \leq i \leq n-2 & \text{ and } n-i \equiv 2 \pmod{3}; \\ x_{n-1}^2 + x_{n-1} x_n + x_n^2 &= 0; \\ x_n^3 + 1 &= 0. \end{aligned}$$

Thus, G is found to be 3-colorable, by (I,3.4). The possible 3-colorings can be obtained by (I,3.6).

If a standard basis is constructed inductively for the equations which only involve x_1, \dots, x_j , given a standard basis for the equations involving x_1, \dots, x_{j-1} , a fixed number of new equations are produced, independent of j . In this sense, the computation of the above standard basis is of length linear in n .

Suppose that $1 \equiv n \pmod{3}$, and adjoin an extra edge connecting vertex 1 to vertex n . Then G is not 3-colorable, but every proper subgraph of G is 3-colorable. The computation of the standard basis for this G yields a machine verifiable proof that G is not 3-colorable, in the form of a computation showing 1 to belong to the ideal we associate with G . By the preceding discussion, the length

of this proof is linear in n . Any proof needs to refer to each vertex of G , so this length is optimal.

How special is this sequence of examples?

(2.4) It is shown in [MaM81] that the problem of determining if a given polynomial $f \in Q[x_1, \dots, x_n]$ belongs to the ideal generated by given elements f_1, \dots, f_j is exponential space hard. Here, as in the preceding examples, n is not fixed. Within a given length input, one may name as many variables as space permits.

They translate into this setting the word problem for commutative semigroups, which they previously prove is exponential space hard. A monomial $x^a \in Q[x_1, \dots, x_n]$ can be thought of as a word in the commuting letters x_1, \dots, x_n . To ask if $x^a \sim x^b$, given $x^c \sim x^d$, $x^e \sim x^f$, ..., is the same as to ask if $x^a - x^b$ belongs to the ideal generated by $x^c - x^d$, $x^e - x^f$,

The division algorithm can determine ideal membership, by (II, 2.6): the remainder of f with respect to a standard basis constructed from f_1, \dots, f_j will be zero iff $f \in (f_1, \dots, f_j)$. So we see that the size of a standard basis can grow exponentially in the size of the input set of polynomials to the division algorithm, if the number of variables is not fixed. This does not always happen, as (2.3) shows.

(2.5) Let $f_1, \dots, f_s \in A = k[x_1, \dots, x_n]$. Let $\deg(f_i)$ denote the maximum of the degrees of terms of f_i , which need not be homogeneous. If f belongs to the ideal generated by f_1, \dots, f_s , then

$$f = \sum_{i=1}^s g_i f_i \quad \text{for } g_i \in A.$$

It is shown in [Her26], [MaM81] that these g_i can be chosen so

$$\deg(g_i) \leq \deg(f) + (sd)^{2^n},$$

where $d = \max_i \{\deg(f_i)\}$.

Note that if f_1, \dots, f_s is a standard basis, then by (I,2.2), we get the corresponding bound

$$\deg(g_i) \leq \deg(f).$$

(2.6) Let G be a graph which is not 3-colorable. If we homogenize the equations of (2.3), via a homogenizing variable x_0 , then G can be associated with the homogeneous ideal $I \subset S = k[x_0, \dots, x_n]$ generated by a polynomial

$$x_i^3 - x_0^3$$

for each vertex i , and a polynomial

$$x_i^2 + x_i x_j + x_j^2$$

for each edge (i,j) . A proof that G is not 3-colorable is provided by a computation showing that $x_0^r \in I$ for some

r. This is because for any graph, the associated ideal I defines a finite set of points in P^n , away from the hyperplane $x_0 = 0$, which correspond to the possible 3-colorings of the graph.

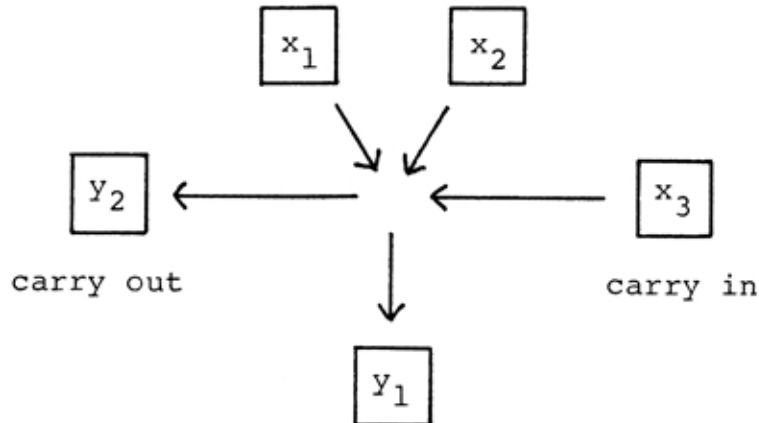
Since G is not 3-colorable, S/I is a finite dimensional k -algebra. Its dimension is clearly related to upper bounds on the complexity of determining the non-3-colorability of G . Does this dimension have a combinatorial interpretation, in terms of the graph G ? What rates of growth can be achieved for this dimension, in terms of the size of G , in sequences of examples?

This question could be posed in an analogous manner for other NP-complete problems.

In a related vein, can the study of lengths of proofs showing non-3-colorability, or the equivalent for other NP-complete problems, be put on a rigorous footing within the category of polynomial rings? In terms of the discussion here, would a lower bound on the length of any computation showing $x_0^r \in I$ translate into a lower bound on the number of steps needed by a nondeterministic Turing machine to infer that G is not 3-colorable? Such a bridge could prove useful.

(2.7) One could apply the division algorithm to the problem of integer factorization, by modeling a nondeterministic digital circuit for integer multiplication by a system of polynomial equations. For example, a subcircuit

which handles one bit addition with carry is represented as follows.



If each bit x_1, x_2, x_3, y_1, y_2 is interpreted as a variable over $\mathbb{Z}/2\mathbb{Z}$, then the above adder is represented by the equations

$$x_i^2 + x_i = 0, \quad i = 1, 2, 3;$$

$$y_i^2 + y_i = 0, \quad i = 1, 2;$$

$$y_1 = x_1 + x_2 + x_3;$$

$$y_2 = x_1x_2 + x_1x_3 + x_2x_3.$$

Now, to attempt to factor a given binary integer, solve for the inputs to a multiplication circuit with the integer to be factored as output. This should be attempted separately for each possible position of lead ones for the binary factors. No attempt should be made to eliminate intermediate variables in the circuit before the output is known, as this would cause an explosion in the size of the system of equations.

We do not know the complexity of the above suggested algorithm, but have found it to be surprisingly fast at small hand examples. We single out this application for reasons entirely independent of an immediate desire to find a fast factorization routine: the division algorithm needs to be better understood as a practical tool. Integer factorization would make an excellent opponent in an effort to shake down an actual implementation of the division algorithm, because it is presumed that the complexity of factoring products of large primes is a fairly uniform function of the size of the product. Thus, empirical results would be easier to understand in this context than in the study of an NP-complete problem, where the complexity of specific instances is seen to vary wildly. On the other hand, (1.2) indicates that the fewer solutions there are for a system of equations, the easier it is to find them. This favors integers with few factors.

Chapter IV

An Algorithm for Coherent Sheaf Cohomology

§1 Computing the Saturation of a Submodule.

(1.1) This chapter describes work in progress, and is necessarily sketchy. We seek to realize an efficient algorithm for the machine computation of the ranks of coherent sheaf cohomology groups. This goal has been a prime motivation for much of the preceding theory. At present, a reasonable algorithm exists, but vast improvements are possible. This project is being continued in collaboration with Michael Stillman, and is in the process of being implemented.

It will be assumed that the input to the algorithm is a finitely presented coherent sheaf F , i.e. an exact sequence

$$M_1 \xrightarrow{A_0} M_0 \longrightarrow F \longrightarrow 0,$$

where M_0, M_1 are free \mathcal{O}_P -modules, and the map A_0 is given. This sequence is represented by the corresponding exact sequence of S -modules

$$M_1 \xrightarrow{A_0} M_0 \longrightarrow F \longrightarrow 0,$$

where $S = k[x_0, \dots, x_n]$.

Here, we encounter the first practical difficulty. If $I \subset M_0$ is the image of M_1 via the map A_0 , then I may fail to be a saturated submodule of M_0 , in actual situations where we still wish to study the associated coherent sheaf F . For example, it is easier to obtain equations defining space curves if one need not worry about saturation. This author anticipates that the machinery for

the computer study of equations describing interesting objects in algebraic geometry may soon get ahead of the machinery for producing such equations. For example, a recent unpublished result of Harris and Mumford reveals intrinsic limitations to one's ability to write down the general curve of a sufficiently high genus. Thus, our algorithms should make as few assumptions as possible about the equations they accept, to improve their applicability.

With this motivation, we first describe how to compute the saturation of a submodule I of the free S -module M . See (II, §4) for preliminaries.

(1.2) Let M be a finitely generated free S -module, and let $I \subset M$ be a homogeneous submodule. The saturation of I is defined as in (II, 4.1). (II, 4.2) extends to this setting: if $y = 0$ defines a hyperplane $H \subset P^n$ not containing any associated primes of I , then $f \in I^{\text{sat}}$ iff $y^j f \in I$ for some j . We use this fact to saturate I .

First, we want to find such a hyperplane H . Since the set of associated primes of I is a finite subset of the scheme P^n , a Zariski open subset of the candidates for H will do, so we can choose H at random, repeating until a successful choice is made. Here is a slight quandry: what should random mean in this setting? What does it even mean to pick a random integer? Before getting

too lost in this question, try 1. One should be warned, however, that in characteristic p , a Zariski open set can turn out to have surprisingly few rational points over a given finite field.

A candidate for H can be tested by comparing the Hilbert polynomials of M/I , M_H/I_H . If M/I has Hilbert polynomial $p(z)$, then M_H/I_H will have Hilbert polynomial $p(z)-p(z-1)$ iff H contains no associated primes of I . This extends (II, 2.8). Hilbert polynomials can be determined by use of the division algorithm; this will be discussed in §2.

Once H has been found, make a change of coordinates so H is defined by $x_n = 0$.

The geometric idea behind our method for saturating I is as follows. If we restrict I to the affine piece of P^n given by the complement of H , find a sufficiently canonical description of I there, and then recompute a projective object from this description, we should get I^{sat} back. This is because nothing gets thrown out with H . (If, on the other hand, we want to throw away the contents of a hypersurface, perhaps in an effort to break something into primary components, then a generalization of the following method is applicable.)

To follow the above program, the correct notion of "sufficiently canonical" is a standard basis with respect to a multiplicative order that orders first by total

degree. Such a basis, when homogenized, will always yield a saturated submodule. This is not quite what we do, but it motivates the actual algorithm.

Choose a multiplicative order $>$ on M that orders first by the total degree of monomials, and then backwards by the degree if x_n is ignored. $>$ can now be refined to a total order in any way one likes; breaking ties lexicographically is one choice. The idea behind this order is closely related to the idea of (I,3.5): for $m \in M$, we want $\text{in}(m)$ to have a certain property iff m has the same property. Here, $\text{in}(m)$ is divisible by x_n iff m is divisible by x_n , for homogeneous m , since least powers of x_n are greatest for $>$ within a given total degree.

To compute the saturation of I , compute a standard basis from I , with respect to the above order $>$. Each time a basis element is found that is divisible by x_n , replace it by its quotient. Such an element belongs to I^{sat} , by the generalization of (II,4.2) discussed earlier. Moreover, if $x_n^j f \in I$ for some j , then in terms of the modified standard basis m_1, \dots, m_p obtained,

$$x_n^j f = g_1 m_1 + \dots + g_p m_p$$

by division. Since no m_i is divisible by x_n , it follows from (II,2.2) that each g_i is divisible by x_n^j . Thus, f belongs to the submodule generated by m_1, \dots, m_p . This submodule is therefore I^{sat} .

§2 Computing the Hilbert Function of a Module

(2.1) There are at least two approaches to obtaining the Hilbert function of M/I , given an exact sequence

$$0 \longrightarrow I \longrightarrow M \longrightarrow M/I \longrightarrow 0$$

in terms of a generating set for I . One is to compute a free resolution for M/I , and read the Hilbert function off the degrees of the free generators for each M_i , where $M = M_0$. Another is to replace I by $\text{in}(I)$, which is a direct sum of twisted monomial ideals, susceptible to combinatorial methods. The Hilbert functions for I , $\text{in}(I)$ are the same, by (I,1.5).

Recall from (III,1.5) that one wants to avoid, if at all possible, computing an entire standard basis when the actual m -regularity of I is known. If this is the case, then computing Hilbert functions via free resolutions can be significantly faster than via $\text{in}(I)$: by (II,2.4), the i^{th} syzygies of the saturated submodule I are of degree $\leq m+i$, if I is m -regular, so the standard bases arising in their construction need only be computed up through these degrees.

On the other hand, if the actual m -regularity of I is not known, then the entire standard basis for I needs to be computed in either case. From here, $\text{in}(I)$ and I are both available, and $\text{in}(I)$ is a simpler object, so one might as well switch over to it. This setting favors a combinatorial approach.

(2.2) We actually seek the generating function for the Hilbert function of M/I , as described in [AtM69]. If

$$a_j = \dim(M/I)_j$$

for each j , then the generating function for this sequence can be written as

$$\sum_j a_j t^j = \frac{g(t)}{(1-t)^{n+1}},$$

where $g(t)$ is a polynomial in $\mathbb{Z}[t]$. This polynomial is easily understood, if one remembers that $t^d/(1-t)^{n+1}$ is the generating function for a free S -module generated by a single element of degree d .

For example, the twisted cubic curve $X \subset \mathbb{P}^3$ is cut out by three polynomials of degree 2, and has two 1st syzygies of degree 3. This is seen in the generating function associated with \mathcal{O}_X :

$$\sum_j h^0(\mathcal{O}_X(j)) t^j = \frac{1-3t^2+2t^3}{(1-t)^4}.$$

From the generating function for a Hilbert function, the corresponding Hilbert polynomial is easily computed. Make the substitution $u = (1-t)$, and expand the generating function into a Laurent series

$$\frac{b_{-s}}{u^s} + \dots + \frac{b_{-1}}{u} + b_0 + b_1 u + \dots + b_q u^q.$$

The polar part then yields the Hilbert polynomial

$$p(z) = b_{-s} \binom{z+s-1}{s-1} + \dots + b_{-1} \binom{z+0}{0},$$

since $1/u^j = 1/(1-t)^j$ is the generating function for $\binom{z+j-1}{j-1}$.

After substituting back $t = (1-u)$, the nonpolar part describes the discrepancy between the Hilbert polynomial and the Hilbert function.

(2.3) To compute Hilbert functions via free resolutions, one first calculates a minimal free resolution for M/I , by the method of (I,2.11). Following the discussion in (2.1), we only calculate a standard basis for each stage in the resolution, up through the highest degree in which a minimal syzygy is expected. Each syzygy among standard basis elements of the submodule under consideration needs to be rewritten into a syzygy among the chosen minimal generators for this submodule, and then this set needs to be trimmed into a minimal set of syzygies before we can proceed with the next stage of the resolution.

Once a free resolution

$$0 \longrightarrow M_r \longrightarrow \dots \longrightarrow M_0 \longrightarrow M/I \longrightarrow 0$$

is obtained, the desired generating function is easy to write down. Denote the degrees of the free basis for each M_i as an S -module by d_{i1}, \dots, d_{ip} . Then the generating function for the Hilbert function of M/I is given by

$$\frac{\sum_{i,j} (-1)^i t^{d_{ij}}}{(1-t)^{n+1}} .$$

(2.4) The capacity to compute Hilbert functions via $\text{in}(I)$ relies on a capacity to determine the Hilbert function of a monomial ideal $I \subset N^{n+1}$.

Let $j : N^{n+1} \rightarrow \{0,1\}$ be the characteristic function of I , so $j(v) = 1$ if $v \in I$, and $j(v) = 0$ otherwise. By Möbius inversion on N^{n+1} , we can compute a second function $q : N^{n+1} \rightarrow \mathbb{Z}$, so with respect to the natural partial order on N^{n+1} ,

$$\sum_{u \leq v} q(u) = j(v).$$

q is nonzero for only finitely many monomials in N^{n+1} , which are each the join of at most $n+1$ generators of I . Thus, q can be computed in a number of operations which is polynomial in the number of generators of I , and exponential in n . See [Aig79] for a detailed exposition on Möbius inversion.

Naive inclusion-exclusion counting yields instead an algorithm exponential in the number of generators of I .

Once q has been computed, the desired generating function is easy to write down. The generating function for the Hilbert function of the monomial ideal I is given by

$$\frac{\sum_u q(u) t^{\deg(u)}}{(1-t)^{n+1}} .$$

From this formula, we can obtain a formula for $M/\text{in}(I)$.

§3 Computing Coherent Sheaf Cohomology

(3.1) Given an exact sequence

$$M_1 \xrightarrow{A_0} M_0 \longrightarrow F \longrightarrow 0$$

of graded S -modules, where M_0, M_1 are finitely generated free S -modules, and the map A_0 is given, we want to compute the ranks of the cohomology groups of the coherent sheaf F on P^n associated to F .

First, let $I \subset M_0$ be the image of A_0 . Using the method of §1, modify M_1, A_0 so I becomes saturated.

Now, compute a minimal free resolution

$$0 \longrightarrow M_n \xrightarrow{A_{n-1}} \dots \longrightarrow M_1 \xrightarrow{A_0} M_0 \longrightarrow F \longrightarrow 0$$

for F as an S -module. This sequence corresponds naturally to a minimal resolution of F by free \mathcal{O}_P -modules,

$$0 \longrightarrow M_n \longrightarrow \dots \longrightarrow M_1 \longrightarrow M_0 \longrightarrow F \longrightarrow 0.$$

Such a resolution can be computed as described in (2.3), using the division algorithm.

Each cohomology group $H^i(F(z))$ on P^n is k -dual to $\text{Ext}^{n-i}(F(z), \omega)$, where $\omega \simeq \mathcal{O}(-n-1)$ is the dualizing sheaf on P^n , so to obtain the ranks we seek, it suffices to compute the ranks of these Ext groups. ω only serves to introduce a grading shift, so we concentrate on computing the ranks of $\text{Ext}^i(F(z), \mathcal{O})$ for each i, z .

Ext is the derived functor for Hom , so $\text{Ext}^i(F(z), \mathcal{O}) \simeq \text{Ext}^i(F(z), S)$ is the kernel mod image of

the dualized sequence

$$\text{Hom}(M_{i+1}(z), S) \xleftarrow{A_i^*} \text{Hom}(M_i(z), S) \xleftarrow{A_{i-1}^*} \text{Hom}(M_{i-1}(z), S)$$

obtained from the previous free resolution for F . Here, $\text{Hom}(M, S)$ is the finite dimensional vector space of degree preserving S -module homomorphisms from M to S . More generally, define M^* to be the dual S -module

$$M^* = \bigoplus_z \text{Hom}(M(-z), S).$$

Note the reversal of the grading. Then if Ext_*^i is the S -module defined by

$$\text{Ext}_*^i(F, S) = \bigoplus_z \text{Ext}^i(F(-z), S),$$

we can compute Ext_*^i as the kernel mod image of the sequence

$$M_{i+1}^* \xleftarrow{A_i^*} M_i^* \xleftarrow{A_{i-1}^*} M_{i-1}^*$$

obtained from the resolution for F .

This approach has the advantage of obtaining infinitely many ranks at once: what we seek is the Hilbert function of each $\text{Ext}_*^i(F, S)$.

The actual module $\text{Ext}_*^i(F, S)$ can be isolated at this point. Each M_i^* is a free S -module: if

$$M_i = \bigoplus_j S(-e_{ij})$$

for integers e_{ij} , then

$$M_i^* = \bigoplus_j S(e_{ij}).$$

Moreover, each matrix A_i^* is just the transpose of A_i .

A set of generators for the kernel of A_i^* can be found by computing the syzygies among the columns of A_i^* , using the division algorithm. To finitely present $\text{Ext}_*^i(F,S)$, we use these generators as a basis for the free S -module L_0 , in the exact sequence

$$L_1 \longrightarrow L_0 \longrightarrow \text{Ext}_*^i(F,S) \longrightarrow 0.$$

L_1 is constructed both from the syzygies among the generators of the kernel of A_i^* , and from the columns of A_{i-1}^* .

The Hilbert function of $\text{Ext}_*^i(F,S)$ can now be computed, as described in §2.

(3.2) If the m -regularity of F is known, then a minimal free resolution for F can be computed without ever constructing an entire standard basis, as described in (III,1.5). One should be able to infer bounds on the m -regularity of each $\text{Ext}_*^i(F,S)$ considered in (3.1), in order to quickly compute their Hilbert functions via free resolutions. We do not know how to do this at this time, so we are forced to compute their Hilbert functions by the much more laborious process of constructing an entire standard basis. This is a reasonable option for curves, but the computer study of the cohomology of higher dimensional varieties awaits a resolution of this question.

Chapter V

Orbits of Hilbert Points

§1 The Structure of Maximal Torus Orbits

(1.1) In this chapter, we briefly describe a geometric interpretation of the division algorithm, in terms of the Hilbert scheme. The point of view expressed here was arrived at in collaboration with Ian Morrison, in seeking to better understand the stability of Hilbert points, in the sense of geometric invariant theory [Mum65], [Mum77], [Kem78]. This point of view has since provided the motivation for much of this thesis.

(1.2) Fix a coordinate system on P^n , and let $D(n+1) \subset SL(n+1)$ denote the maximal torus of diagonal matrices. $D(n+1)$ acts on the coordinate ring $S = k[x_0, \dots, x_n]$ for P^n , as described in (II, 3.1).

Given a saturated ideal $I \subset S$ corresponding to a subscheme $X \subset P^n$, so S/I has Hilbert polynomial $p(z) = g(m_0, \dots, m_s; z)$ in the notation of (II, 1.2), consider the degree d part I_d of I , where $d \geq m_0$. Since the associated ideal sheaf I is m_0 -regular, by (II, 10.1), I is generated in degrees $\leq m_0$, so I can be reconstructed from I_d .

In general, I can be associated abstractly with a point on the Hilbert scheme for $p(z)$ on P^n . The subspace $I_d \subset S_d$, considered as a point in the appropriate Grassmanian, gives a point on this Hilbert scheme, as embedded in this Grassmanian by uniformly representing all such I by $I_d \subset S_d$. This is called the degree d

Hilbert point for I .

Questions about group orbits of points of the Hilbert scheme become much more tangible, if considered for Hilbert points of a given degree. We seek to describe the structure of the orbit of the Hilbert point $I_d \subset S_d$, under the action of the maximal torus $D(n+1)$.

(1.3) Using the coordinate system on S_d consisting of the monomials N_d^{n+1} , represent $I_d \subset S_d$ by a matrix whose rows give a basis for I_d . The action of $D(n+1)$ on S induces an action on the minors of I_d . Specifically, if I_d has dimension q , then $D(n+1)$ acts on the point $\wedge^q I_d \in \wedge^q S_d$. Let $g \in D(n+1)$ be the matrix with diagonal entries $\vec{a} = (a_0, \dots, a_n)$; the minor of I_d obtained by choosing columns corresponding to the monomials $x^{\vec{b}_1}, \dots, x^{\vec{b}_q}$ is multiplied by $\vec{a}^{(\vec{b}_1 + \dots + \vec{b}_q)}$ in gI_d . Thus, we can associate the weight $\vec{b}_1 + \dots + \vec{b}_q$ with this minor.

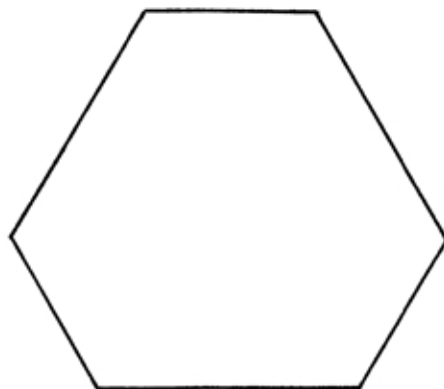
For each nonzero minor of I_d , plot a point at position $\vec{b}_1 + \dots + \vec{b}_q$ in Z^{n+1} . This corresponds formally to considering the weight decomposition of I_d with respect to the characters of the action of $D(n+1)$. Since

$$\deg(\vec{b}_1 + \dots + \vec{b}_q) = qd,$$

this drawing actually lies in an n -dimensional hyperplane of Z^{n+1} .

Consider the convex hull of the points plotted

above. If I defines two points in P^2 , this hull can look like



Choose a multiplicative order $>$ on S . By (I,1.8), choose a grading $r = (r_0, \dots, r_n) \in N_+^{n+1}$ which induces the same order as $>$ on the monomials of S_d . r can be visualized as inducing a linear map $Z^{n+1} \rightarrow Z$ on the above diagram. Now, consider the 1-parameter subgroup $\lambda \in D(n+1)$ whose diagonal entries are $(t^{-r_0}, \dots, t^{-r_n})$, with parameter t . The limit $\lim_{t \rightarrow 0} \lambda I_d$, as a point in the Grassmanian, is precisely $\text{in}(I)_d$, where $\text{in}(I)$ is the monomial ideal of initial forms of I , for the order $>$.

This follows because the monomials generating $\text{in}(I)_d$ give a minor of I_d on which the map $r: Z^{n+1} \rightarrow Z$ achieves a unique maximum. To see this, consider a row reduced matrix representing I_d , where the columns are ordered according to the weight given them by

r . The positions of lead ones in this matrix give the desired minor. So, r is the link between λ and \succ .

In terms of the above weight diagram, $\text{in}(I)_d$ corresponds to a vertex of the convex hull, specifically the vertex on which the map r is maximal. In general, monomial ideals yield one point weight diagrams, since I_d for a monomial ideal has only one nonzero minor, given by the monomials in I_d .

(I,1.8) guarantees that every multiplicative order \succ on S can be so represented. Conversely, given a 1-parameter subgroup λ with monomial ideal limit for I_d , the associated grading r can be extended to a multiplicative order \succ on S . There will be monomials of equal grade for r in higher degrees, but we can refine this grading to a total order by breaking ties lexicographically, for example.

Thus, the possible monomial ideals $\text{in}(I)$ that can be obtained from I , as \succ ranges through all possible multiplicative orders, are described by the vertices of the convex hull of the above weight diagram for I_d .

(1.4) Consider the point on the Hilbert scheme given by I_d . The orbit of this point under the action of $D(n+1)$ can be described in the above framework. The monomial ideals given by vertices of the above convex hull correspond to fixed points of this action, in the closure of the orbit of I_d . More generally, the faces of this

convex hull correspond to components of the boundary of this orbit. Their dimensions, and incidence relationships, are exactly as described by this diagram.

(1.5) In questions such as arise in geometric invariant theory, one sometimes wants to understand the behavior of the sequence of weight diagrams obtained from I_d as $d \rightarrow \infty$. The discussion in (1.3) yields a method for obtaining information about this sequence.

The convex hulls considered here are completely described by knowledge of the set of $\text{in}(I)$ achievable from I . This set can be described intrinsically, independent of a choice of degree d . If J is a monomial ideal from this set, then the sequence of unique weights of the one point diagrams associated with each J_d is a polynomial in d , computable in terms of the function q obtained by Möbius inversion as described in (IV,2.4). Thus, the entire sequence of convex hulls for each I_d can be described as varying in a polynomial manner in d .

The division algorithm provides a computer tool for seeking the above description, in examples.

This is a situation where many standard bases have to be computed in their entirety. Following the discussion in (III,1.5), this procedure is likely to only be reasonable for curves.

Chapter VI

The Hilbert Scheme

§1 Equations for the Hilbert Scheme

(1.1) This chapter describes work in progress, and is necessarily sketchy. A goal is to ferret out information about the component structure (number of components, their dimensions, how they meet) of the Hilbert scheme, in examples as needed. This goal remains out of reach, at this time. We describe a possible attack, which applies many of the ideas in chapter II.

We give explicit equations for an embedding of the Hilbert scheme into projective space, with one possible qualification: the image will be correct, set-theoretically, but we do not prove that the scheme structure is correct. (The Hilbert scheme is known to have nonreduced components; see [Mum62], where a space curve of degree 14, genus 24 is studied.) The equations, however, are obtained in a natural manner; we conjecture that they give the right scheme structure.

From here, there are at least two possible directions to explore. As is, the equations we obtain involve a number of variables beyond any conceivable computer's reach, but they have a strong combinatorial pattern. Hodge was able to find the Hilbert polynomials of Grassmanians in their Plücker embedding, by considering combinatorial patterns to their equations. This approach has been generalized considerably in [DEP82]. The Hilbert scheme is a generalization of the Grassmanian; it might be feasible to seek the Hilbert polynomials of the embeddings

given here, by such methods.

Alternatively, the equations defining the tangent cone of our equations around a point corresponding to a monomial ideal, appear to be easily obtainable. (In general, computing tangent cones is a difficult process, analogous to constructing a standard basis (see [Mor81]), but in certain well-behaved situations one simply reads the tangent cone off the original equations. There is some evidence to suggest that the Hilbert scheme is such a situation, but this needs justification.) In characteristic zero, every component of the Hilbert scheme must pass through a point corresponding to a Borel ideal, as defined in chapter II. See (I,2.12), (II,9.2) to establish this. Borel ideals were studied extensively in chapter II, are much better behaved than arbitrary monomial ideals, and themselves have a strong combinatorial pattern that may mesh well with the pattern underlying our equations. Therefore, a concerted study of the tangent cone of the Hilbert scheme around Borel ideals could yield useful local data. One approach to combining such local data might be to consider the fans employed by Hartshorne [Har66] to prove the connectedness of the Hilbert scheme.

We describe here the equations we have found. We have adopted a visual notation precisely because algebraic notation rapidly becomes convoluted and opaque in this setting. The author has only been able to appreciate the combinatorial pattern in these equations by considering

them visually.

(1.2) Let k be an algebraically closed field, and let $S = k[x_0, \dots, x_n]$ be the graded ring associated with P^n ; $S = \bigoplus_d S_d$, where S_d is the degree d part of S .

Fix a Hilbert polynomial $p(z) = g(m_0, \dots, m_s; z)$. Let $I \subset S$ be a saturated ideal, so S/I has Hilbert polynomial $p(z)$. Then the associated ideal sheaf I is m_0 -regular by (II, 10.1), so $(I)_{m_0}$ has codimension $p(m_0)$ in S_{m_0} , by (II, 2.5). Also, I is the saturation of the ideal generated by $(I)_{m_0}$, by (II, 2.3b). Thus, I can be associated with a point in the Grassmanian $G(\langle m_0 \rangle - p(m_0), \langle m_0 \rangle)$, where $\langle d \rangle = \dim S_d = \binom{n+d}{n}$.

Which points in this Grassmanian correspond to ideals $I \subset S$, so S/I has Hilbert polynomial $p(z)$? By (II, 10.2), if the corresponding ideal I satisfies

$$\dim(I)_{m_0+1} \leq \langle m_0+1 \rangle - p(m_0+1),$$

then in fact, equality holds, and S/I has Hilbert polynomial $p(z)$. Thus, equations on the Grassmanian representing the above condition will cut out a subscheme whose closed points correspond naturally to the closed points of the Hilbert scheme for $p(z)$ on P^n . This is the approach we shall take.

(1.3) Let $I_d \subset S_d$ be a subspace of dimension r_1 ; I_d can be considered as a point in the Grassmanian $G(r_1, \langle d \rangle)$.

Let I be the ideal generated by I_d , and let I_{d+1} be the degree $d+1$ part of this ideal. We seek equations in the Plücker coordinates of the Grassmanian $G(r_1, \langle d \rangle)$ that determine which I_d satisfy $\dim I_{d+1} \leq r_2$.

We have the commutative diagram

$$\begin{array}{ccc}
 S_1 \times S_d & \longrightarrow & S_{d+1} \\
 \uparrow & & \uparrow \\
 S_1 \times I_d & \longrightarrow & I_{d+1}
 \end{array}$$

where the horizontal maps are given by multiplication, and I_{d+1} is the subspace generated by the image of $S_1 \times I_d$.

The multiplication maps factor through tensor products over k , yielding the diagram

$$\begin{array}{ccccc}
 S_1 \times S_d & \longrightarrow & & \longrightarrow & S_{d+1} \\
 \uparrow & \searrow & & \nearrow & \uparrow \\
 S_1 \times I_d & \longrightarrow & & \longrightarrow & I_{d+1} \\
 & \searrow & & \nearrow & \\
 & & S_1 \otimes S_d & & \\
 K & \nearrow & \uparrow & \searrow & \\
 & & J & &
 \end{array}$$

where $J = S_1 \otimes I_d$, and K is the kernel of the map $S_1 \otimes S_d \rightarrow S_{d+1}$.

J has dimension $\leq r_1$, and maps onto I_{d+1} .

Thus,

$$\dim I_{d+1} \leq r_2$$

precisely when

$$\dim(J \cap K) \geq \langle l \rangle r_1 - r_2.$$

The problem now divides into two parts. We describe which J sufficiently intersect K by equations on the Grassmanian $G(\langle l \rangle r_1, \langle l \rangle \langle d \rangle)$, which parametrizes possible subspaces $J \subset S_1 \otimes S_d$, and we compute the map

$$G(r_1, \langle d \rangle) \longrightarrow G(\langle l \rangle r_1, \langle l \rangle \langle d \rangle)$$

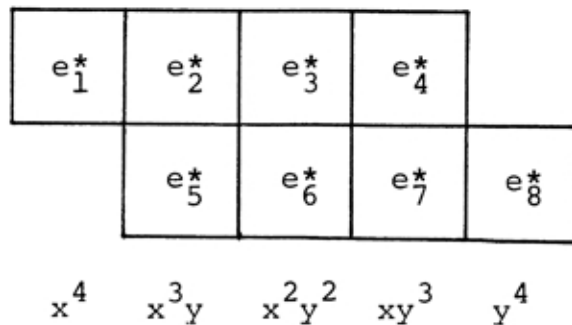
which takes I_d to J .

(1.4) Consider as an example $S = k[x, y]$, $d = 3$.

$S_1 \otimes S_3$ is 8-dimensional. Represent the k -basis for $S_1 \otimes S_3$,

$$\begin{array}{cccc} x \otimes x^3 & x \otimes x^2 y & x \otimes x y^2 & x \otimes y^3 \\ & y \otimes x^3 & y \otimes x^2 y & y \otimes x y^2 & y \otimes y^3 \end{array}$$

by cells as shown:



We have arranged the cells in columns according to their image via the map

$$S_1 \otimes S_3 \longrightarrow S_4,$$

as labeled below the diagram. Denote this k -basis by

e_1, \dots, e_8 , listed in the product lexicographic order on the monomial pairs of $S_1 \otimes S_3$. To e_1, \dots, e_8 we can associate the dual basis e_1^*, \dots, e_8^* , as shown in the above diagram.

Let $L \subset S_1 \otimes S_3$ be a 2-dimensional subspace, and associate L with a matrix whose rows form a basis for this subspace. Then



$$e_3^* \wedge e_5^* \otimes L$$

denotes the (3,5)-minor of L , in the above coordinates. Suppose we want to expand a more complicated expression

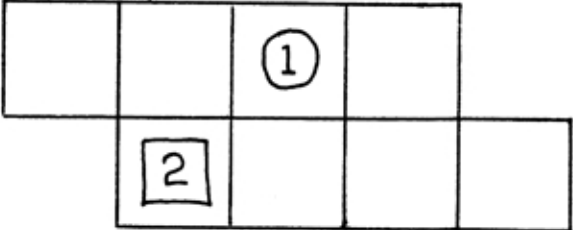
$$(e_3^* + e_6^*) \wedge e_5^* \otimes L$$

to

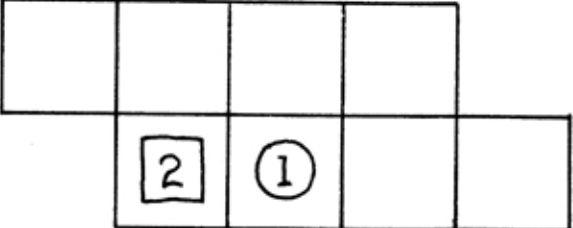
$$(e_3^* \wedge e_5^* - e_5^* \wedge e_6^*) \otimes L.$$

This can be done using the preceding diagram. Represent $(e_3^* + e_6^*)$ by a round marker  which moves freely to either cell e_3^* or e_6^* , and represent e_5^* by a square marker  which stays put in cell e_5^* . Each marker then represents a term in the original equation. Number the markers in the order they occur in the original equation.

Under this identification, each term of the expanded expression corresponds to a set of possible positions for the markers on the diagram, where at most one marker can occupy each cell. The sign of each term is the sign of the permutation obtained from the order of the markers, if cells are scanned in the product lexicographic order. In the above example,



$$= e_3^* \wedge e_5^*;$$

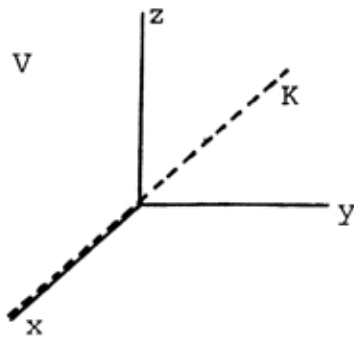


$$= -e_5^* \wedge e_6^*.$$

This notation for minors of a subspace of $S_1 \otimes S_d$ will be used from now on. For $S = k[x_0, \dots, x_n]$, one uses the corresponding diagram whose cells are arranged by staggering n -pyramids in $2n$ dimensions.

(1.5) Let e_1, \dots, e_j be a basis for a vector space V , with corresponding dual basis e_1^*, \dots, e_j^* . Let the subspace $K \subset V$ be the span of e_1, \dots, e_i . If $J \subset V$ is an arbitrary subspace of V , then $J \cap K$ has dimension $\geq r$ precisely when every minor of J involving fewer than r terms from e_1^*, \dots, e_i^* vanishes.

For example, if $V = k^3$, and K is the x -axis



then a 2-dimensional $J \subset V$ contains K precisely when the (y,z) -minor of J vanishes.

(1.6) Which J sufficiently intersect K ? We describe the exact sequence

$$0 \longrightarrow K \longrightarrow S_1 \otimes S_d \xrightarrow{\pi} S_{d+1} \longrightarrow 0.$$

Take as a k -basis for S_j the monomials of degree j . If $a, b \in N^{n+1}$ are monomials in S_1, S_d respectively, then the projection π takes $a \otimes b$ to $c \in S_{d+1}$, where $c = a + b$ as elements of N^{n+1} . Fix c , and let e_1, \dots, e_j denote in the product lexicographic order all $a \otimes b$ mapping to c . Then the elements

$$e_i - e_1, \quad i = 2, \dots, j.$$

form a basis for K , as c ranges over all monomials in S_{d+1} . This basis extends to a basis for $S_1 \otimes S_d$, if we adjoin the e_1 corresponding to each c .

This choice of basis for $S_1 \otimes S_d$ yields the dual basis

$$(e_1^{*+} \dots + e_j^*), e_2^*, \dots, e_j^*,$$

again as c ranges over all possibilities.

Consider this dual basis in terms of the visual notation of (1.4). Each term $(e_1^{*+} \dots + e_j^*)$ can be represented by a round marker \bigcirc , free to range over an entire column corresponding to a choice of c . Each term e_i^* , $i \geq 2$, can be represented by a square marker \square , stuck in the specific cell e_i^* , not at the top of its column.

In terms of this new basis for $S_1 \otimes S_d$ which also describes K , we follow (1.5). An arbitrary $J \subset S_1 \otimes S_d$ intersects K with dimension $\geq \langle l \rangle r_1 - r_2$ precisely when each minor of J involving fewer than $\langle l \rangle r_1 - r_2$ terms of the form e_i^* , i.e. involving fewer than $\langle l \rangle r_1 - r_2$ square markers, vanishes.

(1.7) We continue the example studied in (1.4). Let $S = k[x, y]$, $d = 3$, $r_1 = 3$, $r_2 = 4$. Then $\langle l \rangle r_1 - r_2 = 2$. $J \subset S_1 \otimes S_3$ is 6-dimensional. At most one round marker can occupy a column, so to achieve $\dim(J \cap K) = 2$, we consider equations on the minors of J obtained by arrangements of one square and five round markers on the diagram from (1.4). There are three equations, obtained from the three possible positions of the square marker. We consider one such equation:

②	③	④	⑤	
		①		⑥

= e_{123468}^*

②		④	⑤	
	③	①		⑥

= e_{134568}^*

②	③	④		
		①	⑤	⑥

= $- e_{123678}^*$

②		④		
	③	①	⑤	⑥

= e_{135678}^*

yields

$$(e_{123468}^* + e_{134568}^* + e_{123678}^* + e_{135678}^*) \otimes J = 0,$$

where e_{123468}^* is shorthand for

$$e_1^* \wedge e_2^* \wedge e_3^* \wedge e_4^* \wedge e_6^* \wedge e_8^*.$$

(1.8) What is the map between Grassmanians

$$G(r_1, \langle d \rangle) \longrightarrow G(\langle 1 \rangle r_1, \langle 1 \rangle \langle d \rangle)$$

which takes I_d to J ? This map in fact extends to a map between the projective spaces of their Plücker embeddings, which in turn factors into a $\langle l \rangle$ -uple embedding followed by a linear inclusion.

This is seen by taking a basis for I_d consisting of r_1 vectors in the coordinate system given by the monomials of S_d . Tensoring by S_1 yields a basis of $\langle l \rangle r_1$ vectors for J , which can be written in the coordinate system given by monomial pairs in $S_1 \otimes S_d$, in the product lexicographic order. Following example (1.7), we have $I_d \mapsto J$ represented by the matrices

$$\begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \end{bmatrix} \mapsto \begin{bmatrix} a & b & c & d & & & & \\ e & f & g & h & & 0 & & & \\ i & j & k & l & & & & & \\ & & & & a & b & c & d & \\ & & 0 & & e & f & g & h & \\ & & & & i & j & k & l & \end{bmatrix} .$$

The only minors of J that do not vanish are those which involve exactly r_1 columns from every block of $\langle d \rangle$ columns corresponding to a monomial in S_1 , or a row in the diagrams we have been using. These minors are easily identified as degree $\langle l \rangle$ monomials in the minors of I_d : take the product of the minors from I_d associated with each block of $\langle d \rangle$ columns in J .

(1.9) Using (1.8), we can pull back equations from

$G(\langle 1 \rangle r_1, \langle 1 \rangle \langle d \rangle)$ to $G(r_1, \langle d \rangle)$. In terms of the diagrams of (1.7), the only terms that pull back to nonzero terms are those where the same number of markers occupy each row. These terms pull back to the product of the minors represented by each row, retaining their original sign.

We continue example (1.7). Let $c_{123}, c_{124}, c_{134}, c_{234}$ denote the $\binom{4}{3}$ possible minors of $I_3 \subset S_3$. The terms of the equation considered in (1.7) pull back to terms

$$\begin{array}{|c|c|c|c|} \hline \textcircled{2} & & \textcircled{4} & \textcircled{5} \\ \hline & \textcircled{3} & \boxed{1} & & \textcircled{6} \\ \hline \end{array} = c_{134} c_{124}'$$

$$\begin{array}{|c|c|c|c|} \hline \textcircled{2} & \textcircled{3} & \textcircled{4} & \\ \hline & & \boxed{1} & \textcircled{5} & \textcircled{6} \\ \hline \end{array} = - c_{123} c_{234}'$$

so we obtain the equation

$$c_{123} c_{124} - c_{123} c_{234} = 0$$

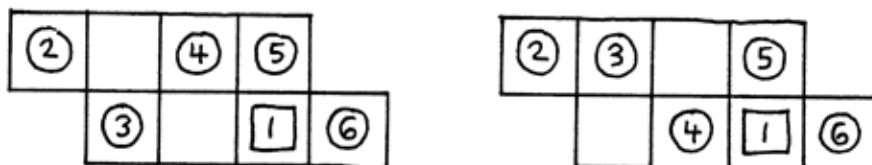
on the minors of $I_3 \subset S_3$. Similarly, from

$$\begin{array}{|c|c|c|c|} \hline \textcircled{2} & \textcircled{3} & & \textcircled{5} \\ \hline & \boxed{1} & \textcircled{4} & & \textcircled{6} \\ \hline \end{array} \qquad \begin{array}{|c|c|c|c|} \hline \textcircled{2} & \textcircled{3} & \textcircled{4} & \\ \hline & \boxed{1} & & \textcircled{5} & \textcircled{6} \\ \hline \end{array}$$

we obtain

$$c_{124}^2 - c_{123}c_{134} = 0,$$

and from



we obtain

$$c_{134}^2 - c_{124}c_{234} = 0.$$

These equations are recognized as cutting out a twisted cubic curve in P^3 .

The interpretation of this example is as follows.

If $I_3 \subset S_3$ satisfies

$$\dim I_4 \leq 4,$$

then I is an ideal so S/I has Hilbert polynomial $p(z) = 1$. The Hilbert scheme parametrizing such ideals is isomorphic to P^1 ; we have realized this Hilbert scheme as a 3-uple embedding of P^1 .

(1.10) In (1.6), instead of requiring fewer than $\langle l \rangle r_1 - r_2$ square markers, we can equivalently require exactly $\langle l \rangle r_1 - r_2 - 1$ square markers, and permit them to occupy any cell. This creates redundant equations, but yields a more symmetric set of equations.

In general, the Grassmanian $G(r_1, \langle d \rangle)$ is properly contained in the projective space of its Plücker embedding,

so to realize a projective embedding of the Hilbert scheme, we must also consider the equations cutting out the Grassmanian. These are well known.

The tangent space to the Grassmanian is particularly easy to describe around points corresponding to monomial ideals: it is flush with the monomial coordinate system, consisting of the span of certain basis vectors. In local questions around monomial ideals, the Grassmanian equations serve simply to eliminate most of the variables, and are not a hindrance.

We have chosen an example from P^1 for simplicity. Once one adjusts to some planar representation of the diagrams needed for P^n , $n > 1$, the discussion in this chapter carries over intact.

Bibliography

- [Aig79] Aigner, M., Combinatorial Theory, Springer-Verlag, Berlin, 1979.
- [AtM69] Atiyah, M. F., MacDonalD, I. G., Introduction to Commutative Algebra, Addison-Wesley Publ. Co., Reading, Mass., 1969.
- [Bri73] Briancon, J., Weierstrass préparé à la Hironaka, Astérisque n° 7,8 (1973), 67-73.
- [Buc70] Buchberger, B., Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems, *Aequationes mathematicae* 4 (1970), 374-383.
- [Buc79] Buchberger, B., A criterion for detecting unnecessary reductions in the construction of Gröbner-bases, Symbolic and Algebraic Computation, Lecture Notes in Computer Science 72, Springer-Verlag, Berlin (1979), 3-21.
- [DEP82] De Concini, C., Eisenbud, D., Procesi, C., Hodge algebras, unpublished manuscript, 1982.
- [FrY77] Fraenkel, A. S., Yesha, Y., Complexity of problems in games, graphs, and algebraic equations, unpublished manuscript, 1977.
- [Gal79] Galligo, A., Théoreme de division et stabilité en géométrie analytique locale, *Ann. Inst. Fourier*, Grenoble 29 (1979), 107-184.
- [GaJ79] Garey, M. R., Johnson, D. S., Computers and Intractability: A Guide to the Theory of NP-Completeness, W. H. Freeman and Company, San Francisco, 1979.

- [Got78] Gotzmann, G., Eine Bedingung für die Flachheit und das Hilbertpolynom eines graduierten Ringes, Math. Z. 158 (1978), 61-70.
- [Har66] Hartshorne, R., Connectedness of the Hilbert scheme, Inst. haut. Etud. sci. Publ. math. 29 (1966), 261-309.
- [Har77] Hartshorne, R., Algebraic Geometry, Graduate Texts in Mathematics 52, Springer-Verlag, Berlin 1977.
- [Her26] Hermann, G., Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, Math Ann. 95 (1926), 736-788.
- [Hir64] Hironaka, H., Resolution of singularities of an algebraic variety over a field of characteristic zero: I, II, Annals of Math. 79 (1964), 109-326.
- [HoU79] Hopcroft, J. E., Ullman, J. D., Introduction to Automata Theory, Languages, and Computation, Addison-Wesley Pub. Co., Reading, Mass. 1979.
- [Kem78] Kempf, G., Instability in Invariant theory, Annals of Math. 108 (1978), 299-316.
- [LLL82] Lenstra, A. K., Lenstra, H. W. Jr., Lovász, L., Factoring polynomials with rational coefficients, unpublished manuscript, 1982.
- [Mac27] Macaulay, F. S., Some properties of enumeration in the theory of modular systems, Proc. London Math. Soc. 26 (1927), 531-555.
- [MaM81] Mayr, E. W., Meyer, A. R., The complexity of the word problems for commutative semigroups and polynomial ideals, M.I.T. Lab. for Comp. Sci. preprint TM-199.

- [Mor81] Mora, F., An algorithm to compute standard bases, rapporti scientifici dell' Istituto di Matematica n.146 (1981), Università di Genova.
- [Mum62] Mumford, D., Further pathologies in algebraic geometry, Am. Journal of Math. 84 (1962), 642-648.
- [Mum65] Mumford, D., Geometric Invariant Theory, Springer-Verlag, Berlin, 1965.
- [Mum66] Mumford, D., Lectures on Curves on an Algebraic Surface, Princeton University Press, Princeton, New Jersey, 1966.
- [Mum77] Mumford, D., Stability of projective varieties, Ens. Math. 23 (1977), 39-110.
- [PoY81] Pohst, M. E., Yun, D. Y. Y., On solving systems of algebraic equations via ideal bases and elimination theory, Proceedings of the 1981 ACM Symposium on Symbolic and Algebraic Computation, 206-211.
- [Rab80] Rabin, M. O., Probabilistic algorithms in finite fields, Siam J. Comput. 9 (1980), 273-280.
- [Sch80] Schreyer, F.-O., Diplomarbeit am Fachbereich Mathematik der Universität Hamburg, 1980.
- [Spe77] Spear, D. A., A constructive approach to commutative ring theory, Proceedings of the 1977 MACSYMA Users' Conference, NASA CP-2012 (1977), 369-376.
- [Sta78] Stanley, R. P., Hilbert functions of graded algebras, Advances in Math. 28 (1978), 57-83.

- [Tri78] Trinks, W., Über B. Buchbergers Verfahren,
Systeme algebraischer Gleichungen zu lösen,
Journal of Number Theory 10 (1978), 475-488.
- [vdW50] van der Waerden, B. L., Modern Algebra, Frederick
Ungar Publ. Co., New York, 1950. More recent
editions do not have a section on elimination
theory.
- [Zac78] Zacharias, G., Bachelor's thesis, Mass. Inst. of
Technology, 1978.