TERM ORDERS ON THE POLYNOMIAL RING AND THE GRÖBNER FAN OF AN IDEAL

by

DENNIS WAYNE TARRANT, JR.

(Under the Direction of Robert Varley, Jr.)

ABSTRACT

Robbiano classified term orders by using ordered systems of vectors. Unfortunately his classification gives little information as to the intuitive “shape” of these spaces. We seek to understand the structure of the spaces of term orders by introducing a topology on them.

We first consider the space of term orders in the bivariate case. We convert weight vectors into slopes and determine that rational slopes require the selection of a “tiebreaking” term order while irrational slopes represent term orders by themselves. By placing an order topology on this space of bivariate term orders, we show that this space has several topological properties. All of these topological properties imply that the space of bivariate term orders is homeomorphic to the Cantor set.

We then consider the spaces of term orders in the general case. We set up a description of the space of term orders in $n \geq 2$ variables as a subspace of a function space. When we consider the topological properties of this view of the term order space on $n \geq 2$ variables, we find that it is homeomorphic to a compact subset of the Cantor set.

These topological descriptions yield important facts about the spaces of term orders that are otherwise very difficult to see or prove. In particular the fact that the Gröbner fan of an ideal has finitely many cones is implied by the compactness of the space of term orders. This was shown previously, but the proof here is much simpler once the topological description of the spaces of term orders is determined.

Finally some facts about the associated geometry are given. The realization of the term order spaces as compact subspaces of Cantor sets leads one to believe certain things about the Gröbner fan. We show the relations between the Gröbner fan and the Netwon polytopes of elements of the reduced Gröbner bases.

INDEX WORDS: Term order, Computer algebra, Polyhedral geometry

TERM ORDERS ON THE POLYNOMIAL RING AND THE GRÖBNER FAN OF AN IDEAL

by

DENNIS WAYNE TARRANT, JR.
B.S., Wake Forest University, 1996
M.A., Indiana University, 1998

A Dissertation Submitted to the Graduate Faculty of The University of Georgia in Partial Fulfillment of the Requirements for the Degree

DOCTOR OF PHILOSOPHY

ATHENS, GEORGIA
2002

TERM ORDERS ON THE POLYNOMIAL RING AND THE GRÖBNER FAN OF AN IDEAL

by

DENNIS WAYNE TARRANT, JR.

Approved:	
Major Professor:	Robert Varley, Jr.
Committee:	Rod Canfield Will Kazez Mitch Rothstein Robert Rumely

Electronic Version Approved:

Gordhan L. Patel
Dean of the Graduate School
The University of Georgia
August 2002

ACKNOWLEDGMENTS

I would like to thank the National Science Foundation VIGRE, National Physical Sciences Consortium, and National Defense Science and Engineering Graduate fellowships for their awards. Their financial support made the attainment of my degree much easier, and for that I am grateful.

I would like to thank my family for their support. In particular my parents and grandparents have always encouraged me and believed in me. It is their dedication to education in general and to me specifically that laid the foundations for my eventual success.

Don Slater and Debbie Poss invested a great amount of time in my life. They saw enthusiasm for mathematics and a small amount of talent, and they nurtured it. Many thanks to these teachers, colleagues, and friends.

Robert Varley has shown amazing dedication to the completion of this degree. His tireless efforts, constant encouragement, and herculean work ethic have been a great model for me. I have said to many others that we need more professors, and more people, like him. My deepest appreciation goes to Robert.

Several people made suggestions and helpful comments along the way. In particular I want to thank Clint McCrory, Will Kazez, Robert Rumely, and Rod Canfield for questions, direction, and interest in my problems. A very special thanks to Mitch Rothstein who took great interest in one of the questions and helped lead me down a road that proved fruitful.

Finally, I want to thank my wife Julia for putting up with so much. It has been a long journey to get here, and she has been supportive and understanding. In lieu of a great number of words, I offer her simple thanks and a shared hope for our future.

TABLE OF CONTENTS

SECTION 1

INTRODUCTION

There are many reasons why one might like to construct a Gröbner basis. If one wants to describe an ideal with a finite set of generators, determine if a polynomial lies in a particular ideal, answer certain questions about radicals of ideals, give a set of generators for a quotient ring that are amenable to computation, or just solve a system of polynomial equations, a Gröbner basis will do the trick. But most ideals have the potential to have several Gröbner bases. So, which one should we pick?

The choice of Gröbner basis is determined by a term order. Term orders are multiplicative total orders which well order the monomials of polynomial rings. In this dissertation we will give a better understanding of the spaces of these term orders. We would like to choose which term order to use depending on what we deem most important in our calculations.

Once we have chosen a term order, we can apply Buchberger's algorithm to get a Gröbner basis in that term order. This Gröbner basis is a set of generators which have certain properties with respect to the term order we have chosen. Since we decided to value one property in our ideal, this Gröbner basis is in some sense the "best" set of generators with respect to that property. We can use this Gröbner basis for whichever calculations we have wanted to perform.

A Gröbner fan is a geometric object which gives information about all of the different Gröbner bases for a given ideal. (see [BS],[MR],[St]) Term orders that are in some sense "close" to one another will yield the same Gröbner basis. When we put together all the term orders that give the same Gröbner basis, we get a polyhedral cone of term orders. The collection of all these cones of term orders is an algebraic fan which is called the Gröbner fan.

The Gröbner fan of an ideal has some interesting properties. For instance the definition gives that the positive orthant must be contained in the support of the Gröbner fan. A study of the Newton polytopes of polynomials and Minkowski sums of these objects has shown a dualistic nature between polyhedral geometry of polynomials and Gröbner fans.

A look at Gröbner fans has caused us to study term orders more closely. In particular we show that the space of term orders in $n \geq 2$ variables is homeomorphic to a compact subset of the Cantor set with the space of bivariate term orders actually being homeomorphic to the Cantor set itself. We use this result to show that the Gröbner fan of an ideal has finitely many cones. Our classification also gives a heuristic answer to the $n = 2$ case of one of the oldest questions in this area: "Is Lex the worst possible term order?" While there had been computational evidence supporting this, we give heuristic reasons why this question should be answered affirmatively when $n = 2$.

Through the use of our classification of term orders, we give an algorithm for determining the Gröbner fan of an ideal. We give reasons why computing adjacent Gröbner bases in the Gröbner fan should be simpler than just wildly computing Gröbner bases for random term orders. This demonstrates why the so-called Gröbner walk method may be preferable to the FGLM method. We discuss the notion of a universal Gröbner basis and how our Gröbner fan algorithm relates to that idea. We also raise several questions about Gröbner bases.

Although the computation of a Gröbner basis answers many ideal-theoretic questions, perhaps the most notable question this computation answers is the determination of solutions to a polynomial system. Since polynomial systems occur in most of mathematics, physics, and computer science, as well as in areas of biology, chemistry, and engineering, the applications of this area of study are virtually limitless. Further investigation may show relevance of Gröbner bases to yet more areas of study.

SECTION 2
HISTORY

The history of these problems goes back to at least 1927. In [Mac] Macaulay introduced the concept of multiplicative total orders for homogeneous ideals and proved that the initial ideal of a homogeneous ideal is indeed an ideal.

In the 1940's Wolfgang Gröbner studied what Hironaka called "standard bases" in the mid 1960's. Gröbner's student Bruno Buchberger investigated these notions in much more depth starting in the late 1960's. Buchberger [B1] gave an equivalent condition for a set of generators to be a standard basis. His definition of S-polynomials gave an algorithm for computing standard bases. Buchberger also renamed the standard bases in honor of his advisor, calling them Gröbner bases. Buchberger [B2] noted properties of Gröbner bases and gave a treatment of the computational complexity of his algorithm for computing them [B5].

In 1978 Kollreider [Ko] showed the importance of the choice of term order in the reduction process and thus in the complexity of the Buchberger algorithm. In 1982 Mayr and Meyer [MaMe] wrote about the complexity of the word problem, a problem closely related to the computation of Gröbner bases.

In 1983 Lazard [L] looked at the problem of computing a Gröbner basis in a different light. Lazard noted the link between constructing Gröbner bases and the process of Gaussian elimination.

Möller and Mora [MoMo] determined some upper and lower bounds on the degrees of elements of Gröbner bases and published their work in 1984. Lorenzo Robbiano [R] gave a classification of term orders in 1985. 1986 saw two important papers. Huynh [Hu] gave superexponential lower bounds for computing Gröbner bases, showing just how computationally complex the Buchberger algorithm is likely to be. And, Bayer and Morrison [BM] injected some polyhedral geometry into this area by introducing the state polytope.

Bayer and Stillman [BS] wrote of refining division orders by using the reverse lexicographic term order, an order which much evidence seemed to show was the "best" for computation. In that same year of 1987 Weipsfenning [W] introduced the idea of a universal Gröbner basis. The next year brought more polyhedral geometry as Mora and Robbiano [MR] defined the Gröbner fan of an ideal.

It was five years before the next big result was published. Faugère, Gianni, Lazard, and Mora [FGLM] showed how one could compute Gröbner bases in any term order if one has a Gröbner basis in some term order. Their process is polynomial in time and only works for zero-dimensional ideals $I \subset k[x_1, \ldots, x_n]$. (By zero-dimensional ideals we mean ideals which have a finite number of solutions $(a_1, \ldots, a_n)$ such that $a_1, \ldots, a_n \in \bar{k}^n$. Geometrically, this means that the variety of I consists of a finite number of points over the algebraic closure of the field k.)

Recently the idea of the "Gröbner walk" has been most studied. Collart, Kalkbrener, and Mall [CKM] wrote of converting Gröbner bases from one term order to another using the Gröbner walk in 1997. Kalkbrener [Ka] wrote another paper in 1999, showing that the complexity of converting Gröbner bases from one term order to another is highly dependent on a distance between those term orders in the Gröbner fan. In 2000 Tran [T] wrote a fast algorithm for Gröbner basis conversion using the Gröbner walk.

SECTION 3

TERM ORDERS

Reduction algorithms are used in many different mathematical applications, most notably in division or Euclidean algorithms. One of the most important concepts for these reduction algorithms is a concept of what constitutes smaller or larger elements. In the case of integers, it is the familiar absolute value. With univariate polynomials the comparison is in the degree of the polynomial. In multivariate polynomials the situation is more complicated. So we must decide how to define a “size” of a polynomial. This will lead us to our definition of a term order.

We note that people from many different areas of mathematics and computer science study Gröbner basis problems. This leads to different terminologies and methods of proof being used on these types of questions. We mostly follow the conventions of Cox, Little, and O'Shea. [CLO1], [CLO2] We will note where we depart from their conventions or methods.

Definition: Let k be a field, and consider the polynomial ring in n variables, $k[x_1, \ldots, x_n]$. Then a *monomial* is an element of $k[x_1, \ldots, x_n]$ of the form ${x_1}^{\alpha_1}{x_2}^{\alpha_2}\cdots{x_n}^{\alpha_n}$, where $\alpha_i \geq 0\ \forall i$. A *term* is an element of the form $c{x_1}^{\alpha_1}{x_2}^{\alpha_2}\cdots{x_n}^{\alpha_n}$, for $c \in k$ and $\alpha_i \geq 0\ \forall i$.

Definition: A *term (or monomial) order* $\succ$ is a relation on the monomials of $k[x_1, \ldots, x_n]$ satisfying the following properties:

1. $\succ$ is a total order on the monomials, i.e. $\succ$ satisfies
   (a) exactly one of $m \succ n, m \prec n$, or $m = n$ holds for all monomials m, n
   (b) $m \succ n$ and $n \succ p \Rightarrow m \succ p$
2. $1 \prec m$ for all monomials m
3. if $m_1 \prec m_2$, then $nm_1 \prec nm_2$ for all monomials n

Proposition: These conditions imply that $\succ$ is a well order.

proof: Suppose not. Then there exist monomials m_i such that $m_1 \succ m_2 \succ m_3 \succ \dots$ (*). This defines a chain of ideals $(m_1) \subset (m_1, m_2) \subset \dots$ (**). But, $(m_1, \dots, m_n) \neq (m_1, \dots, m_{n+1})$, or else $m_{n+1} = \sum_{j=1}^{n} u_j m_j$, with $u_j \in k[x_1, \dots, x_n]$. When we expand the u_j as a linear combination of monomials, then each term in $u_j m_j$ is divisible by some m_j. Then every $u_j m_j$ on the right hand side of the equation is divisible by some m_j for $1 \leq j \leq n$. But m_{n+1} must appear as the monomial of a $u_j m_j$ on the right hand side of the equation. Hence m_{n+1} is divisible by some $m_j, 1 \leq j \leq n$. Thus $m_{n+1} \succeq m_j$ for some $j, 1 \leq j \leq n$. This contradicts (*). So we return to the chain of ideals (**) to see this is a strictly increasing chain of ideals in $k[x_1, \dots, x_n]$. This contradicts Hilbert Basis Theorem. $\square$

Some examples of term orders:

Definition: The *lexicographic order (Lex) with $x_1 \succ x_2 \succ \dots \succ x_n$* on the monomials of $k[x_1, \dots, x_n]$ is defined as follows: For $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\beta = (\beta_1, \dots, \beta_n)$, we define $x^\alpha \prec x^\beta$ iff the first coordinates α_i and β_i in α and β from the left, which are different, satisfy $\alpha_i < \beta_i$.

Definition: The *degree lexicographic order (DegLex) with $x_1 \succ x_2 \succ \dots \succ x_n$* is as follows: $x^\alpha \prec x^\beta$ iff $\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i$ -OR- $\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i$ and $x^\alpha \prec x^\beta$ with respect to LEX with $x_1 \succ x_2 \succ \dots \succ x_n$.

Definition: The *degree reverse lexicographic order (DegRevLex) with $x_1 \succ x_2 \succ \dots \succ x_n$* is as follows: $x^\alpha \prec x^\beta$ iff $\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i$ -OR- $\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i$ and the first coordinates α_i and β_i from the right, which are different, satisfy $\alpha_i > \beta_i$.

Examples:

In Lex with $x \succ y \succ z$, $xy^2 \succ y^3 z^4$, $xy^2 z^3 \prec x^3 y^2$, and $xyz \succ z^3$

In DegRevLex with $x \succ y \succ z$, $xy^2 \prec y^3 z^4$, $xy^2 z^3 \succ x^3 y^2$, and $xyz \succ z^3$

Definition: Let ${x_1}^{\alpha_1}\cdots{x_n}^{\alpha_n} = x^\alpha$. Choose a monomial order $\succ$ on $k[x_1,\ldots,x_n]$. For all $f \neq 0$, we write $f = a_\alpha x^\alpha + a_\beta x^\beta + \ldots + a_\kappa x^\kappa$, with $0 \neq a_\alpha \in k$, and with $x^\alpha \succ x^\beta \succ \ldots \succ x^\kappa$. We define:

$lm(f) = x^\alpha$, the *leading monomial* of f

$lc(f) = a_\alpha$, the *leading coefficient* of f

$lt(f) = a_\alpha x^\alpha = lc(f)lm(f)$, the *leading term* of f.

Also, $lm(0) = lc(0) = lt(0) = 0$.

Example:

Using Lex with $x \succ y$, let $f(x,y) = 3x^2y^3 - 8xy^4 + 2x$. Then $lm(f) = x^2y^3$, $lc(f) = 3$, and $lt(f) = 3x^2y^3$.

Sturmfels discusses another method for classifying term orders in [St]. To describe term orders in $k[x_1,x_2,\ldots,x_n]$, we can use a vector in $\mathbb{R}^n$. But we must make a definition before we may view the term orders via these weight vectors.

Definition: The *exponent vector* of a monomial $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$, where $\alpha_i \geq 0\ \forall i$, is the nonnegative integer vector $ev(x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}) = (\alpha_1,\alpha_2,\ldots,\alpha_n)$.

Definition: Now, take a nonzero vector with real entries (called a *weight vector*), $\omega = (\omega_1,\omega_2,\ldots,\omega_n)$ and an arbitrary term order $\succ$ on $k[x_1,x_2,\ldots,x_n]$. We define the *term order* $\succ_\omega$ on $k[x_1,x_2,\ldots,x_n]$ for nonzero $\omega \geq 0$ by $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n} = x^\alpha \succ_\omega x^\beta = x_1^{\beta_1}x_2^{\beta_2}\cdots x_n^{\beta_n}$ if $\alpha\cdot\omega > \beta\cdot\omega$ or if $\alpha\cdot\omega = \beta\cdot\omega$ and $x^\alpha \succ x^\beta$.

For the arbitrary case we must have that ω is nonnegative, i.e. it must be that $\omega_i \geq 0\ \forall i$. For, take $\omega = (1,-1)$ and consider y^2+1. Then $(0,0)\cdot\omega = 0$ while $(0,2)\cdot\omega = -2$, which would give that $1 \succ y^2$. This violates the second condition for a term order. Choosing some distinctive set of polynomials, it may be the case that weight vectors can have negative entries and still represent orders, (as we see below) but we disallow it in general. Sturmfels actually allows a definition of this larger class of orders that may not meet our definition of a term order for certain collections of monomials.

Proposition : For a nonzero $\omega \geq 0$ and an arbitrary term order $\succ$, $\succ_\omega$ satisfies the conditions of a term order.

proof: We will show that each of the three conditions hold.

1. Take two monomials $m \neq n$. Then either $ev(m)\cdot\omega > ev(n)\cdot\omega$, $ev(m)\cdot\omega < ev(n)\cdot\omega$, or $ev(m)\cdot\omega = ev(n)\cdot\omega$. In the first two cases, we have that $m{\succ_\omega}n$ and $m{\prec_\omega}n$ respectively. In the third case, the arbitrary term order $\succ$ implies that either $m \succ n$ or $m \prec n$. In the former case, $m{\succ_\omega}n$ and in the latter $m{\prec_\omega}n$.

2. Since nonnegative $\omega \geq 0$, a monomial $m \neq 1$ is such that $ev(m) \in (\mathbb{Z}_{\geq 0})^n$, so that $ev(m)\cdot\omega \geq 0$. If $ev(m)\cdot\omega > 0$, then $m{\succ_\omega}0$. If $ev(m)\cdot\omega = 0$, then the fact that $\succ$ is a term order gives that $m{\succ_\omega}1$.

3. Suppose that $m_1{\succ_\omega}m_2$ for two monomials m_1, m_2. Then either $ev(m_1)\cdot\omega > ev(m_2)\cdot\omega$ or $ev(m_1)\cdot\omega = ev(m_2)\cdot\omega$ and $m_1 \succ m_2$. Suppose that $ev(m_1)\cdot\omega > ev(m_2)\cdot\omega$. Then $(ev(nm_1))\cdot\omega = (ev(n)ev(m_1))\cdot\omega) = ev(n)\cdot\omega + ev(m_1)\cdot\omega > ev(n)\cdot\omega + ev(m_2)\cdot\omega = (ev(n)ev(m_2))\cdot\omega = (ev(nm_2))\cdot\omega$ for all monomials n and thus $nm_1{\succ_\omega}nm_2$. Now suppose that $ev(m_1)\cdot\omega = ev(m_2)\cdot\omega$. Then we have that $m_1 \succ m_2$ in the term order $\succ$. Since $\succ$ is a term order, $nm_1 \succ nm_2$ and thus $nm_1{\succ_\omega}nm_2$. □

We mention that orders $\succ_\omega$ correspond to the previously mentioned examples of term orders. Taking the vector $\omega = (1,0)$ and any term order $\succ$ on $k[x,y]$ gives that $\succ_\omega$ is identical to Lex order with $x \succ y$. Now let $\alpha = (1,1)$. If we let $\succ$ be Lex with $x \succ y$, then $\succ_\alpha$ is DegLex with $x \succ y$. If, however, we let $\succ$ be Lex with $y \succ x$, then $\succ_\alpha$ is DegLex with $y \succ x$.

Definition: Consider the same weight vector $\omega = (\omega_1, \omega_2, \ldots, \omega_n)$ and a polynomial $f = c_1x^{a_1} + c_2x^{a_2} + \ldots + c_nx^{a_n}$, where $c_i \neq 0$. Then the *initial form of f with respect to ω, $in_\omega(f)$* is the sum of the $c_ix^{a_i}$ such that $\omega \cdot a_i$ is maximal. When the initial form $in_\omega(f)$ is monomial, we may write $lt_\omega(f)$ for $in_\omega(f)$ as we did earlier in this section.

Examples: Let $\omega = (1,1)$. Then $in_\omega(x^2y + xy^2 + x + y + 1) = x^2y + xy^2$ and $in_\omega(x^3y + xy^2 + xy + 1) = x^3y$. Now let $\alpha = (2,1)$. $in_\alpha(x + y^2) = x + y^2$. Letting $\beta = (3, -1)$ gives $in_\beta(x^3y^2 + x^2y + x^2 + x) = lt_\beta(x^3y^2 + x^2y + x^2 + x) = x^3y^2$.

SECTION 4

GRÖBNER BASES FOR AN IDEAL

We have finally gotten to the point of being able to define our main object of study, the Gröbner basis. After giving a definition of Gröbner basis, we will give another set of conditions on an ideal that will be equivalent to this definition, show that Gröbner bases exist for any ideal, and give properties of Gröbner bases. We then define the more useful concept of the reduced Gröbner basis and give a process which will yield such a reduced Gröbner basis. Here we follow the texts of Cox, Little, and O'Shea [CLO1], [CLO2] and Sturmfels [St].

Definition: Given a term order $\succ$ on $k[x_1, \dots, x_n]$, a set of nonzero polynomials $G = \{g_1, \dots, g_t\}$ contained in a nonzero ideal I is called a *Gröbner basis for* I *with respect to* $\succ$ iff $\forall f \in I$ such that $f \neq 0$, there exists $i \in \{1, \dots, t\}$ such that $lm(g_i) \mid lm(f)$.

Examples: $G_1 = \{x^2 + 5xy - 3y^3, xy + 7y^3, y^3\}$ is a Gröbner basis for $I_1 = \langle x^2, xy, y^3 \rangle$ in Lex with $x \succ y$ order. Now let $\succ$ be Lex with $x \succ y$ and let $g_1 = x^4 - x^3y$ and $g_2 = x^2y^2 - y^4$. $G_2 = \{g_1, g_2\}$ is not a Gröbner basis for $I = \langle g_1, g_2 \rangle$. Notice that $f = xy^5 - y^6 = y^2g_1 - (x^2 + xy - y^2)g_2 \in I$. $lm(g_1) = x^4$, $lm(g_2) = x^2y^2$, and $lm(f) = xy^5$, and thus $lm(g_1) \nmid lm(f)$ and $lm(g_2) \nmid lm(f)$. Since $\exists f \in I$ with no $lm(g_i) \mid lm(f)$, $\{g_1, g_2\}$ is not a Gröbner basis for I.

Definition: In order to give an equivalent and sometimes more useful characterization of a Gröbner basis, we need the following definition: for a given term order $\succ$ on $k[x_1, \dots, x_n]$ and a subset S of $k[x_1, \dots, x_n]$, the *leading monomial ideal* of S is the ideal $LM(S) = \langle lm(s) : s \in S \rangle$. We also define the following: for an ideal I, the *initial ideal* is the ideal generated by all initial forms

$$in_\omega(I) = \langle in_\omega(f) : f \in I \rangle$$

These are not necessarily monomial ideals, but we can add extra hypotheses to assure that they are.

Also, Sturmfels shows two results important for our purposes.

Proposition : If $\omega \geq 0$ and $in_\omega(I)$ is a monomial ideal, then $in_\omega(I) = in_{\succ_\omega}(I)$.

proof: Since the definition of $\succ_\omega$ involves first testing dot products with ω, if $in_\omega(I)$ is already monomial, the additional "tiebreaker" of $\succ$ is irrelevant.

Proposition : For any term order $\succ$ and any ideal $I \subset k[x_1, \ldots, x_n]$, there exists a nonnegative integer vector $\omega \in R^n$ such that $in_\omega(I) = in_\succ(I)$.

We will postpone this proof until after we have defined the concept of a reduced Gröbner basis. The proposition is proved at the end of this section.

Definition: If ω is any real vector such that $in_\omega(I) = in_\succ(I)$, then we call ω a term order for I or we say that ω represents $\succ$ for I.

It is important to note that only certain weight vectors will define term orders for all ideals I. In particular, only weight vectors with nonnegative entries can possibly define term orders for all ideals. It should be noted that certain weight vectors having negative components will represent term orders for some ideals and certain nonnegative weight vectors do not give total orders. These are reasons why we must select the arbitrary term order and define $\succ_\omega$ (as seen in the previous section).

Example: We begin by returning to a previous example. Let I be the principal ideal $I = \langle x^3y^2 + x^2y + x^2 + x \rangle$. Then $\beta = (3, -1)$ is a term order for I. But, β would not be a term order for $J = \langle y^2 + y \rangle$, because $(0, 1) \cdot \beta = -1$, while $(0, 2) \cdot \beta = -2$. This means that $LM(J) = y$, yet $y \mid y^2$, so that (because of the definition of term order) $y^2 \succ y$ and y cannot be the leading term of our polynomial.

Proposition : Assume a term order $\succ$ on $k[x_1, \ldots, x_n]$ is specified. For $G = \{g_1, \ldots, g_t\}$ and $I = \langle g_1, \ldots, g_t \rangle$, G is a Gröbner basis for I iff $LM(G) = LM(I)$. (We will call this equivalent condition the second characterization of a Gröbner basis.)

proof: Suppose the definition of Gröbner basis is satisfied. Then, clearly, $LM(G) \subseteq LM(I)$. To show the reverse inclusion, it suffices to show that $lm(f) \in LM(G)\ \forall f \in I$, since the $lm(f)$'s generate $LM(I)$. But $\forall f \in I$ such that $f \neq 0$, there exists $i \in \{1, \ldots, t\}$ such that $lm(g_i) \mid lm(f)$. Thus $LM(G) = LM(I)$.

Conversely, suppose G is such that $LM(G) = LM(I)$. Now let $f \in I$. Then $lm(f) \in LM(G)$, so $lm(f) = \sum_{i=1}^{t} h_i lm(g_i)$ for some $h_i \in k[x_1, \ldots, x_n]$. Expanding the right hand side, every term is divisible by some $lm(g_i)$. So $lm(f)$ is also divisible by some $lm(g_i)$. □

Examples: Here are some examples where it is fairly easy to check both characterizations of Gröbner basis. First, consider G_1 and I_1 from the above example. In fact, it is simple to show that any set of monomial generators for a monomial ideal is a Gröbner basis in any term order. Second, note that principal ideals $\langle f \rangle$ have $\{f\}$ as a Gröbner basis in any term order. A more ad hoc example is $G_2 = \{x - z^3, y - z^2\}$ is a Gröbner basis in Lex with $x \succ y \succ z$ for $I_2 = \langle x - z^3, y - z^2 \rangle$. Now let $\succ$ be Lex with $x \succ y$ and let $f = x^4 - x^3 y$ and $g = x^2 y^2 - y^4$. $G_3 = \{f, g\}$ is not a Gröbner basis for $I = \langle f, g \rangle$. Notice that $lm(f) = x^4$ and $lm(g) = x^2 y^2$. But $h = xy^5 - y^6 = y^2 f - (x^2 + xy - y^2) g \in I$ and neither of $lm(f)$ and $lm(g)$ divide $lm(h) = xy^5$, so that $LM(I) \neq \langle x^4, x^2 y^2 \rangle$.

Proposition : If $\{g_1, \ldots, g_t\}$ is a Gröbner basis for I, then $\langle g_1, \ldots, g_t \rangle = I$.

proof: Clearly $\langle g_1, \ldots, g_t \rangle \subseteq I$, since $g_i \in I\ \forall i$. Let $f \in I$. Then $lm(f) \in \langle lm(g_1), \ldots, lm(g_t) \rangle$, hence $lm(f - ng_k) < lm(f)$ for some g_k and some term n. Since $f - ng_k \in I$, we get by recursiveness that $f \in \langle g_1, \ldots, g_t \rangle$. □

Example: Let $G_1 = \{x^2, xy, y^3\}$. Then G_1 is a Gröbner basis for $I_1 = \langle x^2 - 5xy, x^3 y, xy + 4y^3, y^3 \rangle$ in Lex with $x \succ y$. But note that $I_1 = \langle x^2, xy, y^3 \rangle$. For a non-monomial example, consider $G_2 = \{x + z, y - z\}$. G_2 is a Gröbner basis in Lex with $x \succ y \succ z$ for $I_2 = \langle x + y, x + z, y - z \rangle$. But we may also write $I_2 = \langle x + z, y - z \rangle$.

Now we head toward proving that Gröbner bases exist, which will also give an alternate proof of the famous Hilbert Basis Theorem. It is notable that our proof will give a constructive method for finding the basis.

Definition : For ease of notation in the following proof, we define $I : \langle a \rangle = \{r \in R : ra \in I\}$.

Dickson's Lemma : Every monomial ideal in $k[x_1, \dots, x_n]$ is finitely generated.

proof: We induct on n. Since every ideal in $k[x]$ is principal, the statement holds for $n = 1$. Suppose it is true for $n - 1$ variables. Let I be a monomial ideal in $k[x_1, \dots, x_n]$. Let $J_l = (I : \langle {x_n}^l \rangle) \cap k[x_1, \dots, x_{n-1}] = \langle S_l \rangle$. Since J_l is an ideal in $k[x_1, \dots, x_{n-1}]$, choose S_l to be finite. Thus $J_0 \subseteq J_1 \subseteq \dots$. Then $\cup J_l$ is an ideal $J \in k[x_1, \dots, x_{n-1}]$ and thus is finitely generated, $J = \langle S \rangle$. If $m \in I$ is some monomial, then $m = m' {x_n}^k$ for some $m' \in k[x_1, \dots, x_{n-1}]$ and some k. Since $m' {x_n}^k \in I$, $m' \in I : \langle {x_n}^k \rangle$, so $m \in \langle {x_n}^k S_k \rangle$. Hence $S' = S_0 \cup x_n S_1 \cup {x_n}^2 S_2 \cup \dots \cup {x_n}^k S_k$ is a finite generating set for I.$\Box$

Theorem : Every nonzero ideal $I \subset k[x_1, \dots, x_n]$ has a Gröbner basis.

proof: Dickson's Lemma gives that $LM(I)$ has a finite generating set. Write this generating set as $\{lt(g_1), \dots, lt(g_t)\}$ for $g_1, \dots, g_t \in I$. Let $G = \{g_1, \dots, g_t\}$. Then $LM(G) = LM(I)$.$\Box$

Definition: A Gröbner basis $G = \{g_1, \dots, g_t\}$ for an ideal I is called *minimal* if $\forall i, lc(g_i) = 1$ and $\forall i \neq j, lm(g_i)$ does not divide $lm(g_j)$.

Given a Gröbner basis $G = \{g_1, \dots, g_t\}$ for an ideal I, to obtain a minimal Gröbner basis, we eliminate all g_i for which $\exists j \neq i$ such that $lm(g_j)$ divides $lm(g_i)$ and divide each remaining g_i by $lc(g_i)$.

Example: Returning to our previous example of $I = \langle x^2 - 5xy, x^3y, xy + 4y^3, y^3 \rangle$, since $xy \mid x^3y$, we will eliminate x^3y. Thus, $\{x^2 - 5xy, xy + 4y^3, y^3\}$ is a minimal Gröbner basis for I.

Proposition : Given a fixed term order $\succ$, if $G = \{g_1, \dots, g_t\}$ and $F = \{f_1, \dots, f_s\}$ are minimal Gröbner bases for an ideal I, then $s = t$, and after renumbering, if necessary, $lt(f_i) = lt(g_i)$ $\forall i = 1, \dots, t$.

proof: Since $f_1 \in I$ and G a Gröbner basis for I, there exists i such that $lm(g_i) \mid lm(f_1)$. Assume $i = 1$. Now $g_1 \in I$ and since F is a Gröbner basis for I, there exists j

such that $lm(f_j) \mid lm(g_1)$. Thus $lm(f_j) \mid lm(f_1)$ and we must have that $j = 1$ since F is a minimal Gröbner basis. Hence $lm(f_1) = lm(g_1)$.

Now, $f_2 \in I$. The minimality of F and the fact that $lm(f_1) = lm(g_1)$ give that $i \neq 1$. After renumbering, if necessary, we get that $lm(f_2) = lm(g_2)$. This process continues until all f_i, g_j are used. So, $s = t$, and after renumbering, $lm(g_i) = lm(f_i)$ $\forall i = 1, \ldots, t$.□

<u>Example</u>: Once again returning to our ideal $I = \langle x^2 - 5xy, x^3y, xy + 4y^3, y^3 \rangle$, we note that both $G_1 = \{x^2 - 5xy, xy + 4y^3, y^3\}$ and $G_2 = \{x^2, xy, y^3\}$ are minimal Gröbner bases, because both satisfy the divisibility properties for a minimal Gröbner basis. Note that both of the Gröbner bases have three elements and that the leading term of each element of G_1 matches the leading term of the corresponding element of G_2.

<u>Definition</u>: Given $f, g, h \in k[x_1, \ldots, x_n]$ with $g \neq 0$, we say f *reduces* to h modulo g, written $f \rightarrow h$, iff $lm(g)$ divides a nonzero term X that appears in f and $h = f - \frac{X}{lt(g)} g$.

<u>Definition</u>: Let $f, h, f_1, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$, with $f_i \neq 0 (1 \leq i \leq s)$. Let $F = \{f_1, \ldots, f_s\}$. We say that f *reduces* to h modulo F, denoted $f \rightarrow^+ h$ iff there exists a sequence of indices $i_1, \ldots, i_t \in \{1, \ldots, s\}$ such that $f \rightarrow h_1 \rightarrow h_2 \rightarrow \ldots \rightarrow h_{t-1} \rightarrow h$.

<u>Definition</u>: A polynomial r is called *reduced* with respect to a set of polynomials $F = \{f_1, \ldots, f_s\}$ if $r = 0$ or if no monomial that appears in r is divisible by any one of the $lm(f_i), i = 1, \ldots, s$. In other words, r cannot be reduced modulo F.

<u>Definition</u>: If $f \rightarrow^+ r$ and r is reduced with respect to F, the r is called a *remainder* for f with respect to F.

<u>Example</u>: Consider our minimal Gröbner basis $G_1 = \{x^2 - 5xy, xy + 4y^3, y^3\}$ from above. $xy + 4y^3 \rightarrow^+ xy$, because $y^3 \mid 4y^3$, and $xy + 4y^3 - 4(y^3) = xy$.

<u>Definition</u> : A Gröbner basis $G = \{g_1, \ldots, g_t\}$ is called a *reduced Gröbner basis* if for all $i, lc(g_i) = 1$ and g_i is reduced with respect to $G \setminus \{g_i\}$. That is, for all i, no nonzero term in g_i is divisible by any $lm(g_j)$ for any $j \neq i$.

<u>Proposition</u> : Let $G = \{g_1, \ldots, g_t\}$ be a minimal Gröbner basis for the ideal I. Consider the following reduction process:

$g_1 \rightarrow^+ h_1$ where h_1 is reduced with respect to $H_1 = \{g_2, \ldots, g_t\}$

$g_2 \rightarrow^+ h_2$ where h_2 is reduced with respect to $H_2 = \{h_1, g_3, \ldots, g_t\}$

$g_3 \rightarrow^+ h_3$ where h_3 is reduced with respect to $H_3 = \{h_1, h_2, g_4, \ldots, g_t\}$

$\vdots$

$g_t \rightarrow^+ h_t$ where h_t is reduced with respect to $H_t = \{h_1, \ldots, h_{t-1}\}$

Then $H = \{h_1, \ldots, h_t\}$ is a reduced Gröbner basis for I.

proof: Note that since G is minimal, we have $lm(h_i) = lm(g_i)$ $\forall i = 1, \ldots, t$. Hence, H is a minimal Gröbner basis for I. Since the reduction of the g_i by $h_1, \ldots, h_{i-1}, g_{i+1}, \ldots, g_t$ is done by eliminating terms of g_i by using $lm(h_1), \ldots, lm(h_{i-1}), lm(g_{i+1}), \ldots, lm(g_t)$ and since $lm(h_j) = lm(g_j)$ $\forall j$, H is a reduced Gröbner basis.□

Example: We return to our familiar ideal $I = \langle x^2 - 5xy, x^3y, xy + 4y^3, y^3\rangle$ and consider the term order $\succ$ as Lex with $x \succ y$. Then $G_1 = \{x^2 - 5xy, x^3y, xy + 4y^3, y^3\}$ is a Gröbner basis for I with respect to $\succ$. But (as above), $xy \mid x^3y$, so that we may remove x^3y from our list and give ourselves that $G_2 = \{x^2 - 5xy, xy + 4y^3, y^3\}$ is a minimal Gröbner basis for I with respect to $\succ$. Still,

$$\begin{aligned} x^2 - 5xy &\rightarrow x^2 - 5xy + 5(xy + 4y^3) \\ &= x^2 - 20y^3 \\ &\rightarrow x^2 - 20y^3 + 20(y^3) \\ &= x^2 \end{aligned}$$

and $xy + 4y^3 \rightarrow xy + 4y^3 - 4(y^3) = xy$ so that we reduce to $G_3 = \{x^2, xy, y^3\}$, which is a reduced Gröbner basis for I with respect to $\succ$.

Theorem(Buchberger): Fix a term order. Then every nonzero ideal I has a unique reduced Gröbner basis with respect to that term order.

proof: First, we choose a term order $\succ$. We have shown that every ideal has a Gröbner basis with respect to $\succ$. We have also given a procedure to convert a Gröbner basis to a minimal Gröbner basis. The previous proposition has given us a method for converting a minimal Gröbner basis to a reduced Gröbner basis. We are only left to show uniqueness. Since reduced Gröbner bases are minimal, we can use the result which states: Given a fixed term order $\succ$, if $G = \{g_1, \dots, g_t\}$ and $F = \{f_1, \dots, f_s\}$ are minimal Gröbner bases for an ideal I, then $s = t$, and after renumbering, if necessary, $lt(f_i) = lt(g_i)\ \forall i = 1, \dots, t$. Now assume that $F \neq G$, that is that there is some $f_j \neq g_j$. Since f_j and g_j are elements of I, so is $f_j - g_j$. But $lt(f_j) = lt(g_j)$ tells us that $lm(f_j - g_j) \prec lm(f_j) = lm(g_j)$. Since F is a reduced Gröbner basis, there is no $lm(f_i)$ which divides a term of f_j. And likewise for g_i, g_j. Hence there can be no terms in $f_j - g_j$ (as those terms would have had to have been present in at least one of f_j, g_j to appear in the difference). Thus $f_j = g_j$ for all j, and $F = G$. □

We will now prove the proposition whose proof we omitted during the section. In order to do this, we will need two results.

Farkas Lemma of Linear Programming : For $a \neq 0$, the inequality $a_0 \cdot x \leq 0$ follows from $a_1 \cdot x \leq 0, \dots a_n \cdot x \leq 0$ iff $\exists$ nonnegative $\lambda_1, \dots, \lambda_n$ with $\sum \lambda_k a_k = a_0$.

Definition : The monomials which do not lie in $LM(I)$ are the *standard monomials.*

Recall that $G \subset I$ is a Gröbner basis for I if $LM(I)$ is generated by $\{lm(g) : g \in G\}$. The following proposition goes back at least as far as Macaulay.

Proposition : Fix a term order $\succ$. The (images of the) standard monomials form a k-vector space basis for the residue ring $k[x_1, \dots, x_n]/I$.

proof: We first show linear independence. Assume there is some relation $f = \sum_{i=1}^{n} a_i m_i \in I$ with monomials m_i in the standard monomials and $a_i \neq 0$, $a_i \in k$. Then we must have $lm(f) \in LM(I)$. Since $lm(f)$ must be one of the m_i, which are all in the set of standard monomials, this is a contradiction.

Now, suppose that the set of standard monomials does not span $k[x_1, \dots, x_n]/I$. From the set of elements of $k[x_1, \dots, x_n]$ not in I and not in the set of standard monomials, choose f with minimal leading term. If $lm(f)$ is in the set of standard monomials, subtract it from f to get a smaller leading term, a contradiction. So, we may assume without loss of generality that $lm(f) \in LM(I)$. Now take an element g of I with $lm(f) = lm(g)$. Then $lm(f-g) \prec lm(f)$, so our choice of $lm(f)$ was not minimal. Contradiction. $\Box$

Proposition : For any term order $\succ$ and any nonzero ideal $I \subset k[x_1, \dots, x_n]$, there exists a nonnegative integer vector $\omega \in \mathbb{R}^n$ such that $in_\omega(I) = in_\succ(I)$.

proof: Let $G = \{g_1, \dots, g_r\}$ be the reduced Gröbner basis of I with respect to $\succ$. Let $g_i = c_{i0}x^{a_{i0}} + c_{i1}x^{a_{i1}} + \cdots + c_{ij}x^{a_{ij_i}}$ with $in_\succ(g_i) = x^{a_{i0}}$. Define $C_{I,\succ}$ to be the set of all nonnegative vectors $\omega \in \mathbb{R}^n$ such that $in_\omega(g_i) = x^{a_{i0}}$ for $i = 1, \dots, r$. Equivalently, $C_{I,\succ} = \{\omega \in \mathbb{R}^n : \omega \cdot (a_{i0} - a_{il}) > 0 \ \forall i = 1, \dots, r, \ \forall l = 1, \dots, j_i\}$. We must show that $C_{I,\succ} \neq \emptyset$. Suppose that $C_{I,\succ} = \emptyset$. By the Farkas Lemma of Linear Programming, there are nonnegative integers λ_{il} with not all of these being zero, such that $\sum_{i=1}^{r} \sum_{l=1}^{j_i} \lambda_{il}(a_{i0} - a_{il}) \leq 0$. Translating this via the multiplicative property of the term order gives that $\prod_{i=1}^{r} \prod_{l=i}^{j_i} (x^{a_{i0}})^{\lambda_{il}} \preceq \prod_{i=1}^{r} \prod_{l=i}^{j_i} (x^{a_{il}})^{\lambda_{il}}$. Yet the requirement that $in_\succ(g_i) = x^{a_{i0}}$ gives that $x^{a_{i0}} \succ x^{a_{il}}$, and this implies that $\prod_{i=1}^{r} \prod_{l=i}^{j_i} (x^{a_{i0}})^{\lambda_{il}} \succ \prod_{i=1}^{r} \prod_{l=i}^{j_i} (x^{a_{il}})^{\lambda_{il}}$. This is a contradiction, so $C_{I,\succ}$ is a nonempty convex cone.

Now choose any $\omega \in C_{I,\succ} \cap \mathbb{Z}^n$. We must show that $in_\omega(I) = in_\succ(I)$. $in_\succ(I)$ is generated by monomials $in_\succ(g_i) = in_\omega(g_i) = x^{a_{i0}}$, so clearly $in_\omega(I) \supseteq in_\succ(I)$. If this were a strict containment, then it would remain strict when passing to the initial ideal with respect to $\succ$. Thus, it would mean that $in_\succ(I) \subset in_{\succ_\omega}(I)$. This would contradict the fact that the standard monomials form a k-vector space for the residue ring $k[x_1, \dots, x_n]/I$. $\Box$

SECTION 5

COMPUTING GRÖBNER BASES THEORETICALLY

Now that we have shown that Gröbner bases exist, we give a way to compute them for any ideal I. We must first define S-polynomials and give Buchberger's criterion, which is actually a third characterization of a Gröbner basis. From this criterion we derive Buchberger's algorithm for computing a Gröbner basis. We continue in our following of [CLO1] for terminology and methods.

Definition : Let $0 \neq f, g \in k[x_1, \dots, x_n]$. Then the *S-polynomial* of f and g is defined to be:

$$S(f,g) = \frac{lcm(lm(f), lm(g))}{lt(f)} f - \frac{lcm(lm(f), lm(g))}{lt(g)} g$$

Example: For both of these examples, let $\succ$ be Lex with $x \succ y$. Now let $f = x^3 + x + 1$ and let $g = y^3 + y^2 + 1$. Then

$$\begin{aligned} S(f,g) &= y^3(x^3 + x + 1) - x^3(y^3 + y^2 + 1) \\ &= -x^3y^2 - x^3 + xy^3 + y^3 \end{aligned}$$

Now, let $h = x^2y + xy^2$ and let $k = x^3 + xy$. Then

$$\begin{aligned} S(h,k) &= x(x^2y + xy^2) - y(x^3 + xy) \\ &= x^2y^2 - xy^2 \end{aligned}$$

Lemma: Let $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ be such that $lm(f_i) = X \neq 0 \ \forall i = 1, \dots, s$. Let $f = \sum_{i=1}^{s} c_i f_i$, with $c_i \in k \ \forall i$. If $lm(f) < X$, then f is a linear combination, with coefficients in k, of $S(f_i, f_j), 1 \leq i < j \leq s$.

proof: Write $f_i = a_i X +$ lower terms, $a_i \in k$. Then, by hypothesis, $\sum_{i=1}^{s} c_i a_i = 0$, since the $c_i \in k \ \forall i$. Now, by definition, $S(f_i, f_j) = \frac{1}{a_i} f_i - \frac{1}{a_j} f_j$, since $lm(f_i) = lm(f_j) = X$. Then,

$$\begin{aligned} f =& c_1 f_1 + \ldots + c_s f_s \\ =& c_1 a_1 (\frac{1}{a_1} f_1) + \ldots + c_s a_s (\frac{1}{a_s}) f_s \\ =& c_1 a_1 (\frac{1}{a_1} f_1 - \frac{1}{a_2} f_2) + (c_1 a_1 + c_2 a_2)(\frac{1}{a_2} f_2 - \frac{1}{a_3} f_3) + \ldots \\ & + (c_1 a_1 + \ldots + c_{s-1} a_{s-1})(\frac{1}{a_{s-1}} f_{s-1} - \frac{1}{a_s} f_s) + (c_1 a_1 + \ldots + c_s a_s) \frac{1}{a_s} f_s \\ =& c_1 a_1 S(f_1, f_2) + (c_1 a_1 + c_2 a_2) S(f_2, f_3) + \ldots + (c_1 a_1 + \ldots + c_{s-1} a_{s-1}) S(f_{s-1}, f_s) \end{aligned}$$

since $c_1 a_1 + \ldots + c_s a_s = 0.\square$

Example: Let $f = x^2y^3 + 3xy^2 - 4x$, $g = x^2y^3 - 8x^2 + 2y + 3$, and $h = x^2y^3 + x^2y^2 + xy^2 + xy + x + y$. Now, consider the $j = x^2y^2 - 8x^2 - 5xy^2 + xy + 9x + 3y + 3 \in \langle f, g, h, \rangle$. We calculate $S(f, g) = 3xy^2 + 8x^2 - 4x - 2y - 3$, $S(g, h) = -x^2y^2 - 8x^2 - xy^2 - xy - x + y + 3$, and $S(f, h) = -x^2y^2 + 2xy^2 - xy - 5x - y$. Then we can write $j = 0 \cdot S(f, g) + S(g, h) - 2 \cdot S(f, h)$.

Theorem : Let $G = \{g_1, \ldots, g_t\}$ be a set of nonzero polynomials in $k[x_1, \ldots, x_n]$. Then G is a Gröbner basis for the ideal $I = \langle G \rangle$ iff $\forall i \neq j$, $S(g_i, g_j) \rightarrow^+ 0$.

proof: $(\Rightarrow)$ If $G = \{g_1, \ldots, g_t\}$ is a Gröbner basis for $I = \langle g_1, \ldots, g_t \rangle$, then $S(g_i, g_j) \rightarrow^+ 0$ $\forall i \neq j$, since $S(g_i, g_j) \in I$.

$(\Leftarrow)$ Now assume $S(g_i, g_j) \rightarrow^+ 0$ $\forall i \neq j$. Let $f \in I$. Write $f = \sum_{i=1}^t h_i g_i$ with $X = max_{1 \leq i \leq t}(lm(h_i) lm(g_i))$ least possible with respect to $\succ$. If $X = lm(f)$, we are done. Otherwise, $lm(f) < X$. If we find another representation of f with smaller X, this is a contradiction. Let $T = \{i : lm(h_i) lm(g_i) = X\}$. For $i \in T$, write $h_i = c_i X_i +$ lower terms. Set $g = \sum_{i \in T} c_i X_i g_i$. Then $lm(X_i g_i) = X$ $\forall i \in T$, with $lm(g) < X$. By the previous lemma there exists $d_{ij} \in k$ such that $g = \sum_{i,j \in S, i \neq j} d_{ij} S(X_i g_i, X_j g_j)$. And, $X = lcm(lm(X_i g_i), lm(X_j g_j))$, so $S(X_i g_i, X_j g_j) = \frac{X}{lt(X_i g_i)} X_i g_i - \frac{X}{lt(X_j g_j)} X_j g_j = \frac{X}{lt(g_i)} g_i - \frac{X}{lt(g_j)} g_j = \frac{X}{lcm(lm(g_i), lm(g_j))} S(g_i, g_j)$. The hypothesis implies $S(g_i, g_j) \rightarrow 0$, and so $S(X_i g_i, X_j g_j) \rightarrow 0$. This gives $S(X_i g_i, X_j g_j) = \sum_{l=1}^t h_{ijl} g_l$, where $max_{1 \leq l \leq t}(lm(h_{ijl}) lm(g_l)) = lm(S(X_i g_i, X_j g_j)) < max(lm(X_i g_i), lm(X_j g_j)) = X$. Substituting into g and then substituting g into f gives $f = \sum_{i=1}^t h'_i g_i$, with $max_{1 \leq i \leq t}(lm(h'_i), lm(g_i)) < X$. Contradiction.$\square$

Example: Take $\succ$ to be Lex with $x \succ y$ and consider the ideal $I = \langle xy^3 - y^4, x^4 - x^2y^2 \rangle$. Then

$$\begin{aligned} S(f,g) &= x^3(xy^3 - y^4) - y^3(x^4 - x^2y^2) \\ &= -x^3y^4 + x^2y^5 \\ &\rightarrow -x^3y^4 + x^2y^5 + x^2y(xy^3 - y^4) \\ &= 0 \end{aligned}$$

Thus, $\{xy^3 - y^4, x^4 - x^2y^2\}$ is a Gröbner basis for I.

Buchberger's Algorithm:

```
INPUT: $F = \{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n]$ with $f_i \neq 0 \; \forall i = 1, \ldots, s$.
OUTPUT: $G = \{g_1, \ldots, g_t\}$, a Gröbner basis for $\langle f_1, \ldots, f_s \rangle$
INITIALIZATION: $G := F$, $\Gamma := \{\{f_i, f_j\} : f_i \neq f_j \in G\}$
WHILE $\Gamma \neq \emptyset$ DO
choose any $\{f, g\} \in \Gamma$
$\Gamma := \Gamma \setminus \{f, g\}$
$S(f,g) \rightarrow^{+} h$, where $h$ is reduced with respect to $G$
IF $h \neq 0$, THEN
$\Gamma := \Gamma \cup \{\{u, h\} \; \forall u \in G\}$
$G := G \cup \{h\}$
```

This is a familiar algorithm, stated for example in [CLO1, page 89].

Theorem : Given $F = \{f_1, \ldots, f_s\}$ with $f_i \neq 0$ $(1 \leq i \leq s)$, Buchberger's algorithm will produce a Gröbner basis for the ideal $I = \langle f_1, \ldots, f_s \rangle$.

proof: That the algorithm terminates is assured by Dickson's Lemma, since each nonzero h that must be added to G gives another monomial $lm(h)$, with $lm(g_1) \nmid lm(h)$ for any $g_i \in G$, so that the ideal generated by the leading monomials strictly increases for each nonzero reduced h which is added. Correctness is implied by Buchberger's Theorem.□

Example: Let $I = \langle f, g \rangle$, where $f = x^4 - x^3y$ and $g = x^2y^2 - y^4$. Choose Lex with $x \succ y$ as our term order $\succ$. Then,

$$\begin{aligned} S(f,g) &= y^2(x^4 - x^3y) - x^2(x^2y^2 - y^4) \\ &= x^4y^2 - x^3y^3 - x^4y^2 + x^2y^4 \\ &= x^3y^3 - x^2y^4 \\ &\to x^3y^3 - x^2y^4 - xy(g) \\ &= -x^2y^4 + xy^5 \\ &\to -x^2y^4 + xy^5 + y^2(g) \\ &= xy^5 - y^6 = h \end{aligned}$$

Now, we must add h to the set (putative Gröbner basis) G and add $\{f,h\}, \{g,h\}$ to the set Γ. We compute

$$\begin{aligned} S(f,h) &= y^5(x^4 - x^3y) - x^3(xy^5 - y^6) \\ &= x^4y^5 - x^3y^6 \\ &\to x^4y^5 - x^3y^6 - y^5(f) \\ &= 0 \end{aligned}$$

So now we compute

$$\begin{aligned} S(g,h) &= y^3(x^2y^2 - y^4) - x(xy^5 - y^6) \\ &= xy^6 - y^7 \\ &\to xy^6 - y^7 - y(h) \\ &= 0 \end{aligned}$$

Thus, $\{f,g,h\}$ is a Gröbner basis for I with respect to the Lex with $x \succ y$ term order.

We make two notes about computing that are of interest when one is practically computing a Gröbner basis. We have seen neither result previously discussed. The first is the existence of a “linear translation invariance” property in Gröbner bases which allows one to translate solution points to the origin (or to some other chosen point) to attempt to reduce the heights of coefficients needed within the Buchberger algorithm.

Proposition : Suppose that $I = \langle f_1, \dots, f_t \rangle \subset k[x_1, \dots, x_n]$, and $\tilde{I} = \langle \tilde{f_1}, \dots, \tilde{f_t} \rangle \subset k[x_1, \dots, x_n]$, where $\tilde{f_i} = f(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$. Now let $G = \{g_1, \dots, g_s\}$ be a Gröbner basis for I with respect to some term order $\succ$. Then $\tilde{G} = \{\tilde{g_1}, \dots, \tilde{g_s}\}$ is a Gröbner basis for $\tilde{I}$ with respect to $\succ$.

proof: Take a polynomial f with leading term $t = cx_1{}^{e_1}x_2{}^{e_2} \cdots x_n{}^{e_n}$ and perform the translation. Then $\tilde{f}$ has term $\tilde{t} = c(x_1 - a_1)^{e_1}(x_2 - a_2)^{e_2} \cdots (x_n - a_n)^{e_n}$ which has leading term $t = cx_1{}^{e_1}x_2{}^{e_2} \cdots x_n{}^{e_n}$, the same as t. This will also apply to the lower terms with respect to $\succ$. Thus $lt(\tilde{f}) = lt(f) = t$. Now, we must have elements of the Gröbner basis being members of $\tilde{I}$. But the elements of $\tilde{G}$ are all members of $\tilde{I}$ with the proper leading terms. Hence $\tilde{G}$ is a Gröbner basis for $\tilde{I}$ with respect to $\succ$. □

Example: Consider the ideal $I = \langle x^2 + y, y^2 + x \rangle$. Let $\succ_1$ be Lex with $x \succ y$ and $\succ_2$ be DegRevLex with $x \succ y$. Then the reduced Gröbner basis with respect to $\succ_1$ is $G_1 = \{y^4 + y, x + y^2\}$, and the reduced Gröbner basis with respect to $\succ_2$ is $G_2 = \{x^2 + y, y^2 + x\}$. Consider the translation $x \mapsto x+1, y \mapsto y-4$. Then $\tilde{I} = \langle (x+1)^2 + (y-4), (y-4)^2 + (x+1) \rangle$. Computing the reduced Gröbner basis $\tilde{G_1}$ with respect to $\succ_1$ gives $\tilde{G_1} = \{y^4 - 16y^3 + 96y^2 - 255y + 252, x + y^2 - 8y + 17\} = \{(y-4)^4 + (y-4), (y-4)^2 + (x+1)\}$. And, likewise computing $\tilde{G_2}$ yields $\tilde{G_2} = \{y^2 + x - 8y + 17, x^2 + 2x + y - 3\} = \{(y-4)^2 + (x+1), (x+1)^2 + (y-4)\}$.

Our second result comes as a counterexample to an exercise in [CLO1, page 446, problem 16] which is used to prove their Proposition 8 on pages 442-443. If the statement they give in the exercise were true, one could decompose two-dimensional ideals into primary factors and parallelize the Buchberger algorithm in ways that could reduce the necessary computation significantly.

In the exercise, we are asked to show that $LM(I) \cdot LM(J) = LM(I \cdot J)$. It is fairly simple to see the forward inclusion. It is also fairly easy to show that the reverse inclusion is not true. Consider $I = \langle x-1, y-1\rangle$ and $J = \langle x+1, y-1\rangle$, and let $\succ$ be Lex with $x \succ y$. Then $IJ = \langle x^2 - 1, y - 1\rangle$, so that $LM(IJ) = \langle x^2, y\rangle$. But $LM(I) = \langle x, y\rangle = LM(J)$, and thus $LM(I)LM(J) = \langle x^2, xy, y^2\rangle$, so that $LM(IJ) \neq LM(I)LM(J)$.

Note that this mirrors one of the obstacles to generating sets for an ideal being Gröbner bases for that ideal. The one problem that occurs in generating sets is cancellation of terms in sums of the generators. Consider $f = x^2 + x + 1$ and $g = -x^2$. Then $lt(f) = x^2$ and $lt(g) = -x^2$, so that $lt(f) + lt(g) = 0$. Yet, $lt(f + g) = x$, something that could not have been predicted by only looking at the leading terms.

SECTION 6

COMPUTING GRÖBNER BASES PRACTICALLY

There are many arguments about the computational complexity of constructing a Gröbner basis, but each argument is either tangential to the Buchberger algorithm or heuristic in nature. In this section we will report on the calculations, conjectures, and results that appear in the literature and give some general ideas about the difficulties encountered in computation of Gröbner bases.

For the following discussion, we make certain assumptions. Let F be a set of t polynomials in $k[x_1, \dots, x_n]$. Assume that the maximum of the degrees of the elements of F is d.

Hermann [He] gave bounds for the degrees of polynomials needed to express an element of an ideal in terms of its generators in the early 1900's. Her work was on an algebraic construct similar to Gröbner bases that was termed Hermann bases. These bounds that she found are often cited when the Buchberger algorithm is discussed. From the initial set F, she showed that certain types of Hermann bases would have elements of maximal degree $d^2 + d$. In [Se] Seidenberg showed that a more general bound for all Hermann bases was possible. Seidenberg showed that the maximal degree of the elements of Hermann bases is always bounded by d^4.

In 1978 Kollreider [Ko] pointed out the importance of choosing a term order in the calculation of a Gröbner basis. In 1983 Buchberger [B5] gave ideas on the bounds of his algorithm, particularly in the bivariate case. He reported bounds that both he and Lazard had discovered over $k[x, y]$. In particular he proved Kollreider's conjectures, showing that a DegRevLex Gröbner basis would have elements of a reduced Gröbner basis of degree $\leq 2d - 1$, while a general term order would yield elements of the reduced Gröbner basis of degree $\leq d^2$. Buchberger also showed that the number of elements of a minimal Gröbner basis G in an arbitrary term order would be less than or equal to one more than the minimum of the degrees of the elements of F, where F is a set of bivariate polynomials. Finally, he showed that the Buchberger algorithm would terminate in fewer than $\frac{3}{2}(|F| + 2 \cdot (d+2)^2)^4$ steps in the bivariate case. He also showed that all of these bounds are tight.

Möller and Mora [MoMo] gave both upper and lower bounds for the degrees of certain Gröbner bases in 1984.

Mayr and Meyer [MM] showed that calculating certain elements in answering the uniform word problem for commutative semigroups involved doubly exponential growth. The problem they approached is a special case of deciding the membership problem for polynomial ideals given by bases.

Huynh [Hu] gave superexponential lower bounds for Gröbner bases in 1986 and Kalkbrener [K] used that work to show that for all m, there exists a prime ideal P and two reduced Gröbner bases for P, F and G such that $|F| = O(m)$ and $|G| \geq 2^{2^m}$. Kalkbrener also showed that for homogeneous ideals I, we can relate the maximum degree of elements in two reduced Gröbner bases. Let reduced Gröbner basis F of I have elements of maximal degree d. Then for any other reduced Gröbner basis G of I, the degree of the elements of G is less than $((n+1)(d+1)+1)^{(n+1)2^{dim(I)+1}}$. Kalkbrener also showed that the situation is better if F and G are in adjacent cones of the Gröbner fan. (Here there is no homogeneity assumption on the ideal.) Once again, assume reduced Gröbner basis F has elements of maximal degree d. Then elements of an adjacent Gröbner basis G has degrees less than $2 \cdot d^2 + (n+1) \cdot d$, where n is the number of variables.

Most recently Tran [T] has explored the Gröbner walk through a Gröbner fan. Tran uses the term Gröbner walk to describe a traversal through the Gröbner fan of an ideal terminating in a specific cone of the Gröbner fan. (That target cone can have any dimension.) He defines the length w of the Gröbner walk as the number of different computations of reduced Gröbner necessary to reach the target cone. The degree of polynomials in the reduced Gröbner basis of the target cone is bounded by $2^{2^w-1}d^{2^w} + 2^{2^{w+1}}d(n+1)(d+1)^{2^w-2}(n+2)^{2^{w+1}-1}$, where d and n have the same definitions as above.

One can notice that there are several choices made in an implementation of the Buchberger algorithm. Any choice made can be a help or a hindrance to the efficiency of the algorithm. The first choice that one must make is that of a term order. Another is the order in which S-polynomials are computed. While we have seen no progress on the latter, there has been some work on the former. In [FGLM] a polynomial time algorithm is given which will convert a Gröbner basis for a zero-dimensional ideal in any term order into a Gröbner basis for that same ideal in any other term order. Thus, calculating a Gröbner basis for a zero-dimensional ideal in any one term order is essentially equivalent to calculating a Gröbner basis in the desired term order.

The initial choice in the implementation of the Buchberger algorithm is that of a term order. This first decision seems to play a vital role in the running time of the algorithm. Many believe that in general the Lex-type orders are the worst possible. And, it is believed that DegRevLex is generally the best term order for computation. Both of these assertions are supported by much experimental evidence (see, for instance, [BS], [Ko], [MoMo]), and we offer heuristic reasons that suggest why they should be true in Section 13. Still, these characterizations are not universally true for all ideals but are generalizations over the class of all ideals. There are numerous examples in which the Lex term order works most efficiently (for instance, if the set of generators for the ideal is already a Gröbner basis in Lex order). It is only on average that we think of Lex as a worst term order and DegRevLex as a best term order, and we know of no results which predict when these ideas will be upheld or contradicted in general.

The second choice which must be made in the Buchberger algorithm is the order in which S-polynomials are computed. Computational evidence shows us that in general there is a point in the Buchberger algorithm where there are “enough” elements to form a Gröbner basis, that is there is a point where every element needed as a generator of

$LM(I)$ has appeared as a $lt(g_i)$, where g_i is one of the elements of the set G which is formed in Buchberger's algorithm. After this every ensuing S-polynomial reduces to 0 and the algorithm terminates very quickly. If we could find a fastest path to the point of having "enough" polynomials for the Gröbner basis, we could save a great deal of time and computation. This quickest way would necessitate a proper ordering of S-polynomial computations.

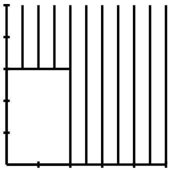
Not a great deal is known about the Buchberger algorithm. The choices of term order and order of S-polynomial computation are important in the time of computation, as much experimental evidence shows. Perhaps because of these choices, there is still no thorough treatment of the complexity of the Buchberger algorithm.

SECTION 7

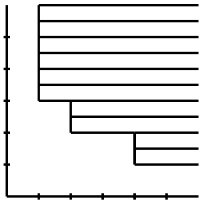
IDEALS AND GEOMETRY

Consider a monomial ideal $M = \langle x^{\alpha_1}, \dots, x^{\alpha_t} \rangle \subset k[x_1, \dots, x_n]$. In this section we will give a geometric description of ideals of this form. These geometric descriptions are already reported in the literature, and [CLO1] is a source where one may find a brief discussion of these descriptions.

Our goal is to have a geometric picture of all elements contained in M. First, we plot the points which are described by the exponent vectors $\alpha_1, \dots, \alpha_t$. Now, for each α_i, shade the region defined by $\alpha_i \oplus (\mathbb{R}_{\geq 0})^2$. The lattice points contained in the union of all of these shaded regions is identical to the elements of the monomial ideal M. Here we show a geometric view of the monomial ideal $M = \langle x^2, y^3 \rangle$:



Here is a view of $N = \langle x^4y, x^2y^2, xy^3 \rangle$:



We will choose to look particularly at the two variable case. From Buchberger on, many have chosen to look at ideals over a bivariate polynomial ring. There are many reasons for this. The most obvious is that the case of two variables is the first of any interest. For univariate polynomials there is only one choice of term order. Since term orders are multiplicative, the leading term of a polynomial f is always the term having highest degree. We will show in the next section that there are uncountably many bivariate term orders.

Also of importance in choosing the bivariate case is that many of the interesting problems that occur in cases of more variables already surface with two variables. With only two variables we have more of an opportunity to get a handle on situations which become very complicated as the number of variables grows. This applies for geometric reasons also. In the bivariate case we are dealing with Newton polygons. Anyone who has attempted the jump from plane geometry to solid geometry knows of the increase in difficulty of studying the latter subject. Studies of Newton polygons give us a chance to see trends and extrapolate them to higher dimensional Newton polytopes.

SECTION 8

CLASSIFYING AND TOPOLOGIZING $Term(2)$

Section 8 and section 9 are new approaches to a problem that some have already investigated. In [R] Robbiano does classify term orders on n variables. This is the space that we call $Term(n)$. Our approach is a departure from the approach of Robbiano and yields new results. An extensive literature search and correspondence with Little, O'Shea, and Sturmfels all indicate that the work of the next two sections is all original.

In this section we will give a new "common sense" description of bivariate term orders and show that this description will form some space $Term(2)$. We will give this space a natural order topology. We will then show that the space $Term(2)$ is homeomorphic to the Cantor set by the use of $Term(2)$'s topological properties. Finally we will give results that follow from $Term(2)$ being homeomorphic to the Cantor set.

Sturmfels gives a way to describe term orders using weight vectors and arbitrary term orders as tiebreakers (see Section 3). A simpler method in the case of two variables is to convert these weight vectors to slopes. Thus the weight vector (p, q) is converted to $\frac{q}{p}$, where $p \neq 0$ and the slope m represents the weight vector $(1, m)$.

We will consider two term orders $\succ_1$, $\succ_2$ to be distinct if there exist two monomials m, n such that $m \succ_1 n$ while $n \succ_2 m$.

We start with a couple of propositions about irrational slopes.

Proposition: A positive irrational m gives a term order.

proof: Let $\omega_m = (1, m)$ with m irrational, and choose an arbitrary term order $\succ$. Now we can compare any two exponent vectors $e_1 = (a_1, b_1)$ and $e_2 = (a_2, b_2)$ using $\succ_m$. But since m is irrational, $a_1 + b_1 m \neq a_2 + b_2 m$ unless $a_1 = a_2$ and $b_1 = b_2$. Hence the $\succ$ is irrelevant, and ω_m represents a term order for any ideal I. $\square$

Proposition: Distinct irrationals give different term orders.

proof: Take $m_1 \neq m_2$, two positive irrational numbers. Then there exists a rational $\frac{p}{q}$ such that, without loss of generality, $m_1 < \frac{p}{q} < m_2$. Now consider the ideal $\langle f \rangle = \langle x^p + y^q \rangle$. $\{f\}$ is a reduced Gröbner basis in any term order (since the ideal is principal). But $lt_{m_1}(f) = x^p$ and $lt_{m_2}(f) = y^q$. Hence m_1 and m_2 represent distinct term orders. $\square$

So irrational numbers give term orders with no need for a "tiebreaking" term order. This is not the case with rational numbers. Consider $q = \frac{s}{r}$, where r and s are positive integers. Then the polynomial $f = x^s + y^r$ has a tie between the two potential leading terms. Here a tiebreaking term order is needed. But, since we are in two variables, it is a simple choice. We can choose our term order as either Lex with $x \succ y$ or Lex with $y \succ x$. Keeping track of these term orders becomes cumbersome, so we use the convention that q^- represents the term order defined by q with the tiebreaker of Lex with $x \succ y$ and q^+ represents the term order defined by q with the tiebreaker of Lex with $y \succ x$.

Proposition: q^+ and q^- give distinct term orders.

proof: Let $q = \frac{s}{r}$ and consider $\langle f \rangle = \langle x^s + y^r \rangle$. $lt_{q^+}(f) = y^r$, while $lt_{q^-}(f) = x^s$. $\square$

Proposition: Distinct rationals q_1, q_2 give different term orders.

proof: Choose $q_1 < q_2$. Then there exists $\frac{s}{r}$ such that $q_1 < \frac{s}{r} < q_2$. Consider $f = x^s + y^r$. $lt_{q_1^-}(f) = lt_{q_1^+}(f) = x^s$ and $lt_{q_2^-}(f) = lt_{q_2^+}(f) = y^r$. $\square$

Proposition: Any positive irrational m gives a term order distinct from q^-, q^+ for any $q \in \mathbb{Q}$.

proof: Choose an irrational m. Then between m and any q, there exists a rational $\frac{s}{r}$. Without loss of generality, let $q < \frac{s}{r} < m$. Now let $f = x^s + y^r$. Then $lt_{q^+}(f) = lt_{q^-}(f) = x^s$, but $lt_m(f) = y^r$. $\square$

In general q^+ and q^- are considered for positive rational numbers. There are two exceptions. For the term order described by slope 0, we need only consider the case of 0^+. For the term order described by slope ∞, we need only deal with ∞^-. (Slope 0 amounts to taking a dot product with the vector $(1, 0)$, so that weight is given to the x component of the exponent vector, but no weight is given to the y component. Thus, sorting has already been done on the x components of the exponent vectors and we only have need for a tiebreaker to sort on y components of the exponent vectors. Slope ∞ corresponds to dot product with a vector $(0, 1)$, so a symmetric argument applies.) This leads us to the following:

Theorem: The set of term orders on $k[x, y]$ is in bijection with the elements of the set $Term(2) = \{0^+, \infty^-, q^+, q^-, m\}$, for q ranging over the positive rationals and m ranging over the positive irrationals.

proof: The previous five propositions have shown the reverse inclusion. Now, take an arbitrary term order $\succ$. We compute the set $\Lambda(\succ) = \{m \in \mathbb{Q} : lt_{\succ}(x^s + y^r) = y^r$, where $m = \frac{s}{r}\}$ for $\succ$. Take the least upper bound of the elements of $\Lambda(\succ)$, and call it l. If $l \notin \mathbb{Q}$, we set $m = l$. If $l \in \mathbb{Q}$, suppose $l = \frac{r}{s}$, and there are two cases. If $l \in \Lambda(\succ)$, then $m = l^+$. If $l \notin \Lambda(\succ), m = l^-$. Hence $\succ$ has a representative in $Term(2)$. $\Box$

This classification agrees with the classification of Robbiano in [R, Theorem 5] for the case $n = 2$, although Robbiano did not seek topological descriptions of his classifications.

Now we seek to determine the kind of space that these term orders form. We will endow $Term(2)$ with an order topology and use the following:

FACT: Any compact, perfect, totally disconnected metric space is homeomorphic to the Cantor set. [HY, page 100, Corollary 2-98]

We introduce one simple notion, that q^+ is the immediate successor of q^-, and this leads to an order topology on the set of term orders.

Lemma 1: $Term(2)$ is metrizable.

We use the Urysohn Lemma to show this. Urysohn states that any regular space with a countable basis is metrizable.

sublemma a : $Term(2)$ is regular

proof: Fact: Let X be a topological space. Let one-point sets in X be closed. Then X is regular iff given a point $x \in X$, and a neighborhood U of x, there exists a neighborhood V of x such that $\overline{V} \subset U$. [M, 196: Lemma 4.2.1(a)]

Take $x \in Term(2)$ and U open such that $x \in U$. Now, $x \in (a^+, b^-) \subseteq U$ for some basic open set (a^+, b^-). But there exists an $a_0, b_0 \in \mathbb{Q}$ with $a < a_0 < x < b_0 < b$. Now let $V = ({a_0}^-, {b_0}^+)$. Then $x \in V$ and $\overline{V} = [{a_0}^-, {b_0}^+] \subset (a, b) \subseteq U$. Hence $Term(2)$ is regular. □

sublemma b: $Term(2)$ has a countable basis.

proof: The set

$B = \{\{(q^-, r^-) \cup (q^-, r^+) \cup (q^+, r^-) \cup (q^+, r^-), , q < r \in \mathbb{Q}$ ranges over $\mathbb{Q}\ \} \cup \{(0^+, r^-) \cup (0^+, r^+)$, r ranges over $\mathbb{Q}\} \cup \{(q^+, \infty^-) \cup (q^-, \infty^-)$, q ranges over $\mathbb{Q}\ \}\}$ is a countable basis for $Term(2)$. □

Thus $Term(2)$ is metrizable.

For the next lemma, we will need the following:

FACT: Let X be a simply ordered set having the least upper bound property. In the order topology, each closed interval in X is compact. [M, p. 173, Theorem 6.1]

Lemma 2: Every closed interval in $Term(2)$ is compact.

proof: Consider the mapping $\pi : Term(2) \to \hat{\mathbb{R}}$ (where $\hat{\mathbb{R}}$ denotes the extended real numbers) defined by $\pi(m) = m$ for m irrational, $\pi(q^+) = \pi(q^-) = q$ for $q \in \mathbb{Q}$, and $\pi(\infty^-) = \infty$ and take a bounded set $A \subseteq Term(2)$. The set $\pi(A)$ is bounded and since $\hat{\mathbb{R}}$ has the least upper bound property, $\pi(A)$ must have a least upper bound. Call this number l. Then there are two cases. If $l \notin \mathbb{Q}$, set $l = lub(A)$. Otherwise, $l \in \mathbb{Q}$, and there are two cases again. If $l^+ \notin A$, set $l^- = lub(A)$. If $l^+ \in A$, then $l^+ = lub(A)$. Thus, $Term(2)$ has the least upper bound property. Since $Term(2)$ is simply ordered, the fact gives that every closed interval in $Term(2)$ is compact. □

Corollary: $Term(2)$ is compact.

proof: $[0^+, \infty^-] = Term(2)$ is a closed interval in $Term(2)$. □

Lemma 3: $Term(2)$ is perfect.

proof: Let $x \in Term(2)$, and suppose x is represented by $\succ$. Then $x = lim(\Lambda(\succ))$, as previously defined in the classification theorem. □

Lemma 4: $Term(2)$ is totally disconnected.

proof: Suppose (a, b) is connected, where $a < b$. So long as there exists $q \in \mathbb{Q}$, $q \in (a, b)$, we have $A = (a, q^-]$ and $B = [q^+, b)$, so that (a, b) is not connected. Hence there exist no connected sets that consist of more than a singleton point, since there is a $q \in \mathbb{Q}$ in each larger interval. $\square$

This gives us:

Theorem: $Term(2)$ is homeomorphic to the Cantor set.

This classification will lead to a natural approach to some of the recent results of Mora and Robbiano in the bivariate case [MR, Lemma 2.6]. This natural approach is shown in the corollary in section 9 and in the bivariate Gröbner fan algorithm in section 11.

There are specific links between the Cantor set and the set $Term(2)$ that should be noted here. We offer thanks to Will Kazez for the ideas behind the following insight.

Take the set $Term(2)$ and add on a closed interval $[q^-, q^+]$ for every rational q. Call this space A. Then $Term(2)$ sits inside A in the same way that the Cantor set C sits inside $\mathbb{R}$. In the familiar process of forming the Cantor set, we delete “middle thirds” intervals. In the process of gleaning $Term(2)$ from A, the deletions take place at those closed intervals $[q^-, q^+]$.

Rod Canfield has asked whether or not the isomorphism between the set of bivariate term orders and the “middle thirds” Cantor set is order preserving. It appears that this is the case as the gaps between q^- and q^+ occur at each of the disconnection points formed when the “middle thirds” are removed from the real line in the “usual” Cantor set construction, but we have not checked all of the details.

SECTION 9

TOPOLOGIZING $Term(n)$

There is a very natural topology on the space $Term(n)$ of term orders on the polynomial ring $k[x_1, \dots, x_n]$. [St] and [MR] give variants of the following idea but do not extend the idea to introduce a topology on $Term(n)$.

A great deal of thanks goes to Robert Rumely and Mitch Rothstein. Rumely suggested that a topology on $Term(n)$ might be approached by the Robbiano classification. Rothstein shared many important ideas about Robbiano's paper which were helpful in the formulation of this section. Our wholehearted gratitude is extended to these two.

Definition : Given a nonzero ideal $I \subset k[x_1, \dots, x_n]$, let $U_I[t] := \{t' \in Term(n) : LM_t(I) = LM_{t'}(I)\}$.

Proposition : The $U_I[t]$ are a basis of open sets for a topology on $Term(n)$.

proof: Let $M = \langle m_1, \dots, m_s \rangle$ be a monomial ideal, where each m_i is a monomial and no m_i divides an m_j for $i \neq j$. Then $G = \{m_1, \dots, m_s\}$ is a reduced Gröbner basis with respect to every $t \in Term(n)$.

Now suppose $t \in U_I[t_1] \cap U_J[t_2]$. Then $t \in U_{I+J}[t] \subset U_I[t_1] \cap U_J[t_2]$. $\square$

Our main result is that with this topology, for any $n \geq 2$, $Term(n)$ is homeomorphic to a compact subset of the Cantor set. To attain this result, as in [R], we start our analysis with a larger set of orders on monomials.

Definition : We define $Total(n)$ to be the collection of all total orders on the exponent vectors of the monomials of $k[x_1, \dots, x_n]$ which satisfy an additivity property, i.e. $Total(n)$ consists of all those relations t on $(\mathbb{Z}_{\geq 0})^n$ which satisfy the following three conditions:

(trichotomy) exactly one of $a\ t\ b$, $b\ t\ a$, or $a = b$ holds

(transitivity) if $a\ t\ b$ and $b\ t\ c$, then $a\ t\ c$

(additivity) if $a\ t\ b$, then $(a + c)\ t\ (b + c)$ for all $c \in (\mathbb{Z}_{\geq 0})^n$

(One may think of t as analogous to $\succ$ of section 3.)

Note that two elements $t_1, t_2 \in Total(n)$ are distinct if there are $a, b \in (\mathbb{Z}_{\geq 0})^n$ with $a \neq b$ such that $a\ t_1\ b$ and $b\ t_2\ a$.

Definition : We view $Term(n)$ as the collection of relations of $Total(n)$ also having the following property on the exponent vectors of the monomials of $k[x_1, \ldots, x_n]$: (positivity of the standard basis) $e_i\ t\ 0$ for the standard basis vectors e_i. (Note that positivity of the standard basis will imply that $a\ t\ 0$ for all $a \in (\mathbb{Z}_{\geq 0})^n, a \neq 0$ by the previous additivity property.)

Note that $Term(n) \subseteq Total(n)$, since $Term(n)$ are the elements of $Total(n)$ which satisfy further restrictions, and the elements of $Term(n)$ correspond exactly to term orders in the sense of section 3.

Definition : We define $\mathbb{Q}^{n*}$ to be the set of nonzero rational vectors and let $F = \{\pm 1\}^{\mathbb{Q}^{n*}}$, the set of all functions from $\mathbb{Q}^{n*}$ to $\{\pm 1\}$.

In following the tradition of Robbiano [R], we extend the relations on $(\mathbb{Z}_{\geq 0})^n \setminus \{\vec{0}\}$ to rational vectors. In Lemma 1 of [R], it is shown that there is a unique extension of $Total(n)$ on $(\mathbb{Z}_{\geq 0})^n \setminus \{\vec{0}\}$ to $\mathbb{Q}^{n*}$.

We have often asked whether $a\ t\ b$, where $a \neq b$ in $(\mathbb{Z}_{\geq 0})^n$. An equivalent question is whether $(a-b)\ t\ 0$. Note that now $a - b \in \mathbb{Z}^n$ and $a - b \neq 0$. Now we construct a collection of functions as follows:

$$\phi : Total(n) \longrightarrow F$$

by

$$t \mapsto f_t$$

where $f_t(c) = 1$ if $qc = (a-b)$ for some $q \in \mathbb{Q}_{>0}$ and $a, b \in \mathbb{Z}^n_{\geq 0}$ with $a\ t\ b$ and $f_t(c) = -1$ otherwise.

Lemma : ϕ is injective.

proof : Suppose t_1, t_2 are distinct in $Total(n)$. Then $\exists a, b \in (\mathbb{Z}_{\geq 0})^n$ such that $a\ t_1\ b$ and $b\ t_2\ a$. Let $c = a - b$. Then $f_{t_1}(c) = 1$. For, let $q = 1$ in the above definition of $f_t(c)$. And we claim that $f_{t_2}(c) = -1$. Suppose $q(a - b) = a' - b'$ for $q = \frac{r}{s} \in \mathbb{Q}_{>0}$ and $a', b' \in {\mathbb{Z}_{\geq 0}}^n$. Consider $s(a' - b') = sq(a - b) = r(a - b)$. Since $b\ t_2\ a$, the additivity property gives that $2b\ t_2\ 2a, \ldots, rb\ t_2\ ra$. If we assume that $a'\ t_2\ b'$, then additivity gives that $sa'\ t_2\ sb'$ or equivalently that $ra\ t_2\ rb$, which is a contradiction. Thus, $f_{t_2}(c) = -1$. □

We will endow $\mathbb{Q}^{n*}$ with the discrete topology. We also give $\{\pm 1\}$ the discrete topology. Now we consider the topology of pointwise convergence in order to give us a topology on F (and thus on $Total(n)$ and $Term(n)$). Given $x \in \mathbb{Q}^{n*}$ and open $U \subseteq \{\pm 1\}$, $S(x, U) = \{f_t : f_t(x) \in U\}$ is a subbasis for a topology on F. ([M, page 280])

We can also view F as the product space of copies of the discrete space $\{\pm 1\}$ indexed by $\mathbb{Q}^{n*}$. (see [M, 280-281]) Because $\{\pm 1\}$ is compact, the Tychonoff Theorem implies that $F = \{\pm 1\}^{\mathbb{Q}^{n*}}$ is compact.

We will use a fact from Munkres to prove the following lemma. [M, page 287, Theorem 5.3]: Let X be locally compact Hausdorff; let $C(X, Y)$ have the compact-open topology. Then the map $eval : X \times C(X, Y) \longrightarrow Y$ defined by the equation $eval(x, f) = f(x)$ is continuous. (Here, $C(X, Y)$ is the space of continuous function from X to Y).

Lemma : $eval : \mathbb{Q}^{n*} \times F \longrightarrow \{\pm 1\}$ is continuous.

proof: Note that $F = C(\mathbb{Q}^{n*}, \pm 1)$ because any function $f : \mathbb{Q}^{n*} \longrightarrow \{\pm 1\}$ is continuous since $\mathbb{Q}^{n*}$ has the discrete topology. The topology on $\mathbb{Q}^{n*}$ is discrete and thus Hausdorff. $\mathbb{Q}^{n*}$ with the discrete topology is locally compact since every singleton set is both open and compact. The discrete topology on $\mathbb{Q}^{n*}$ implies that compact subsets of $\mathbb{Q}^{n*}$ are finite. Thus the compact-open topology is identical to the point-open topology. Hence by the above fact from [M], $eval$ is continuous. □

Proposition : $\Phi = \phi(Total(n))$ is closed in F.

proof : For $d, e \in \mathbb{Q}^{n*}$ with $d + e \neq 0$, let $C(d,e) = \{f \in F : iff(d) = f(e),\text{ then } f(d) = f(e) = f(d+e)\}$. For $\gamma \in \mathbb{Q}^{n*}$, let $O(\gamma) = \{f \in F : f(-\gamma) = -f(\gamma)\}$. First we claim that $\Phi = \cap_{d,e\in\mathbb{Q}^{n*},d+e\neq 0} C(d,e) \cap (\cap_{\gamma\in\mathbb{Q}^{n*}} O(\gamma))$.

First, take an f such that $\cap_{d,e\in\mathbb{Q}^{n*},d+e\neq 0} C(d,e) \cap (\cap_{\gamma\in\mathbb{Q}^{n*}} O(\gamma))$. Define, $\forall a, b \in (\mathbb{Z}_{\geq 0})^n$ with $a \neq b$, $a\ t\ b \Leftrightarrow f(a-b) = 1$. Trichotomy holds, as either $f(a-b) = 1$ and thus $a\ t\ b$ or else $f(a-b) = -1$. Since $f \in O(\gamma)$ for $\gamma = a - b$, $f(a-b) = -1 \Rightarrow f(b-a) = 1$ and thus $b\ t\ a$. Next, transitivity holds. Suppose that $a\ t\ b$ and $b\ t\ c$. Then $f(a-b) = f(b-c) = 1$. Letting $d = a-b$ and $e = b-c$, either we get $f((a-b)+(b-c)) = f(a-c) = 1$, and thus $a\ t\ c$ because $f \in C(d,e)$ for $d = a-b, e = b-c$ or we get that $d + e = 0$. If $d+e = 0$, then $d = -e$. Letting $\gamma = e$ gives that $f(d) = f(-e) = -f(e)$ because $f \in O(\gamma)$. But this is impossible because $f(d) = f(e)$. Finally, additivity holds. Suppose $a\ t\ b$. Then $f(a-b) = 1 = f((a+c)-(b+c))$ for any $c \in (\mathbb{Z}_{\geq 0})^n$. Hence $(a+c)\ t\ (b+c)$ for any c.

Now, take an $f \in \Phi$, i.e. $f = f_t$ for $t \in Total(n)$. First, suppose that $f(d) = f(e) = 1$ for $d, e \in \mathbb{Q}^{n*}$, $d+e \neq 0$. Take $q \in \mathbb{Q}_{>0}$ so that both $qd, qe \in \mathbb{Z}^{n*}$. Then $\exists b \in (\mathbb{Z}_{\geq 0})^n, b \neq 0$ such that $a = b - qd$ and $c = b + qe$ are both in $(\mathbb{Z}_{\geq 0})^n$. Now $b\ t\ a$ since $f(a-b) = f(qd) = f(d) = -1$ and $f \in O(\gamma)\ \forall\gamma$ and $c\ t\ b$ since $f(b-c) = f(qe) = f(e) = -1$ and $f \in O(\gamma)\ \forall\gamma$. Therefore, $c\ t\ 1$ by transitivity of t. Hence $-1 = f(a-c) = f(qd+qe) = f(q(d+e)) = f(d+e)$, and $f \in C(d,e)$.

Now suppose that $f(d) = f(e) = -1$ for $d, e \in \mathbb{Q}^{n*}$, $d+e \neq 0$. Take $q \in \mathbb{Q}_{>0}$ so that both $qd, qe \in \mathbb{Z}^{n*}$. Then $\exists b \in (\mathbb{Z}_{\geq 0})^n, b \neq 0$ such that $a = b + qd$ and $c = b - qe$ are both in $(\mathbb{Z}_{\geq 0})^n$. Now $a\ t\ b$ since $f(a-b) = f(qd) = f(d) = 1$ and $b\ t\ c$ since $f(b-c) = f(qe) = f(e) = 1$. Therefore, $a\ t\ c$ by transitivity of t. Hence $1 = f(a-c) = f(qd+qe) = f(q(d+e)) = f(d+e)$, and $f \in C(d,e)$.

Now suppose that $f(\gamma) = 1$. Then there exist $a, b \in (\mathbb{Z}_{\geq 0})^n$ such that $q\gamma = a - b$ for $q \in \mathbb{Q}_{>0}$ and $a\ t\ b$. Now, $q(-\gamma) = b - a$. Since $a\ t\ b$, it cannot be the case that $b\ t\ a$ by trichotomy. Hence $f(-\gamma) = -1$, and $f \in O(\gamma)$.

Next we show that the sets $C(d,e)$ and $O(\gamma)$ are closed in F.

Lemma : $C(d,e)$ is a closed subset of F.

proof : Note that

$$\begin{aligned} B(d,e) := \{f : f(d) =& f(e) = 1, f(d+e) = -1\} \cup \{f : f(d) = f(e) = -1, f(d+e) = 1\} \\ =& (eval_d{}^{-1}(1) \cap eval_e{}^{-1}(1) \cap eval_{d+e}^{-1}(-1)) \\ & \cup (eval_d{}^{-1}(-1) \cap eval_e{}^{-1}(-1) \cap eval_{d+e}^{-1}(1)) \end{aligned}$$

is the complement of $C(d,e)$. Note that both sets in the first union are open, as they are the intersection of three open sets. Each set in each intersection is open because $\{1\}$ and $\{-1\}$ are open sets of $\{\pm 1\}$ and $eval_d, eval_e$, and $eval_{d+e}$ are all continuous functions. Thus $B(d,e)$ is open. Hence its complement $C(d,e)$ is closed. $\Box$

Lemma : $O(\gamma)$ is a closed subset of F.

proof : Let $O_+(\gamma) = \{f \in F : f(\gamma) = 1, f(-\gamma) = -1\}$ and let $O_-(\gamma) = \{f \in F : f(\gamma) = -1, f(-\gamma) = 1\}$. Then $O(\gamma) = O_+(\gamma) \cap O_-(\gamma)$. Now $O_+(\gamma) = eval_\gamma{}^{-1}(1) \cap eval_{-\gamma}{}^{-1}(-1)$, and both of $eval_\gamma{}^{-1}(1)$ and $eval_\gamma{}^{-1}(-1)$ are closed in F by continuity of $eval$ and since $\{1\}$ and $\{-1\}$ are closed in $\{\pm 1\}$. Thus, $O_+(\gamma)$ is closed. Likewise, $O_-(\gamma)$ is closed so that $O(\gamma)$ is closed. $\Box$

By the lemmas, Φ is closed in F, and the proposition is proved. $\Box$

Now consider $Term(n) \subseteq Total(n)$. Recall that $Term(n)$ consists of those elements of $Total(n)$ which satisfy the further constraint of positivity of the standard basis.

We will now show that positivity of the basis is a closed condition. Then $P = \phi(Term(n))$ is a closed subset of the compact space Φ, so that P is a compact space.

Lemma : Positivity of the basis is a closed condition.

proof: Let $D_i := \{f_t \in F : f_t(e_i) = 1\}$, and define $D_1, D_2, \ldots, D_n$. $D_i = eval_{e_i}^{-1}(1)$ is closed since $\{1\}$ is a closed set. Hence $D_1 \cap D_2 \cap \ldots D_n$ is closed, and positivity of the basis is a closed condition. $\Box$

Thus, P is a compact space. (†)

We will need the following proposition, which is analogous to a result in [St, page 12].

Proposition: For a given nonzero ideal I and a given term order t, assume $G = \{g_1, \ldots, g_s\}$ is the reduced Gröbner basis for I with respect to t. Then $U_I[t] = \{t' \in Term(n) : lm_t(g_i) = lm_{t'}(g_i)\ \forall i\}$.

proof : Assume $G = \{g_1, \ldots, g_s\}$ is the reduced Gröbner basis for I with respect to t. By the second characterization of a Gröbner basis, $LM_t(I) = LM_t(G)$. Now take the reduced Gröbner basis for I with repect to t' and call it $G' = \{g'_1, \ldots, g'_r\}$. By the second characterization of a Gröbner basis and the fact that $t' \in U_I[t]$, $LM_t(G) = LM_t(I) = LM_{t'}(I) = LM_{t'}(G')$. Since $LM_t(G)$ and $LM_{t'}(G')$ are equal as monomial ideals, they must have the same elements. Since both are reduced Gröbner bases, there are no extraneous elements in either set so that $r = s$, and after renumbering if necessary $lt_t(g_i) = lt_{t'}(g'_i)$ for each i. As defined in section 4, the reduction process yields a unique answer and is only dependent on the leading monomials. Hence we must have that $g_i = g'_i$ for all $i = 1, \ldots, r = s$. $LM_t(I) = \langle lm_t(g_1), \ldots, lm_t(g_s)\rangle = \langle lm_{t'}(g_1), \ldots, lm_{t'}(g_s)\rangle = LM_{t'}(I)$. Thus $U_I[t] = \{t' \in Term(n) : lm_t(g_i) = lm_{t'}(g_i)\ \forall i\}$. $\square$

Proposition : The topology on $Term(n)$ defined by the $U_I[t]$ (call this description T) and the topology on $Term(n)$ as a subspace P of the function space F are identical.

proof: Take a basic open set $U = U_I[t] \in T$. $U_I[t] = \{t' \in Term(n) : lm_t(g) = lm_{t'}(g)\ \forall g \in G\}$, where $G = \{g_1, \ldots, g_s\}$ is the reduced Gröbner basis with respect to t. We map $U_I[t]$ by ϕ onto $A = \cap_a\{f_t : f_t(a) = 1\}$, where a runs over the elements $b_i - c_{ij}$ with $b_i = lm_t(g_i)$ and c_{ij} runs over the terms of g_i which are not b_i. Since G is a reduced Gröbner basis, it is finite. Hence this intersection is finite. So A is a finite intersection of subbasis elements for P and hence is a basic open subset of P.

Now take S a subbasic open set of P. Then S is defined by a collection of f_t such that $a\ t\ 0$ for some $a \in \mathbb{Q}^{n*}$. But if we let $I = \langle x^a + 1\rangle$ if $a \in (\mathbb{Z}_{\geq 0})^n \setminus \{\vec{0}\}$, then $\{x^a + 1\}$ is a reduced Gröbner basis for I. If a has negative entries $-a_i$, then we will form a vector $\tilde{a} = a_i$ in the entries where a has a negative entry, and is 0 in all other entries. Now consider the ideal $I = \langle x^{a+\tilde{a}} + x^{\tilde{a}} \rangle$. S is defined by those t which make $\{x^{a+\tilde{a}} + x^{\tilde{a}}\}$ a reduced Gröbner basis for I, which is a basic open set of T. □

We will now show that $Term(n)$ is homeomorphic to a subset of the Cantor set in a manner like we showed that $Term(2)$ is homeomorphic to the Cantor set. Alternately, one could check that $F = \{\pm 1\}^{Q^{n*}}$ is homeomorphic to the Cantor set. Since $P \subset F$, P is homeomorphic to a subset of the Cantor set.

Lemma 1 : $Term(n)$ is compact.

This was shown previously (†) in this section.

Lemma 2 : $Term(n)$ is metrizable.

proof: $\{\pm 1\}$ is metrizable, and products of metrizable spaces are metrizable. ([M,page 126]) Thus, $\{\pm 1\}^{\mathbb{Q}^{n*}}$ is metrizable. $Term(n)$ is a subspace of $\{\pm 1\}^{\mathbb{Q}^{n*}}$, and subspaces of metrizable spaces are metrizable. Thus $Term(n)$ is metrizable. □

Lemma 3 : $Term(n)$ is totally disconnected.

proof: Take a minimal connected set $U \subseteq P$. Since P is a subspace of a product space, there exists some factor of U which consists of the entire space $\{\pm 1\}$. Say that this occurs in the i^{th} factor. Then ${U_i}^+ = U$ restricted to 1 in the i^{th} factor and ${U_i}^- = U$ restricted to -1 in the i^{th} factor is a separation of U by open sets. Thus $Term(n)$ is totally disconnected. □

Theorem : $Term(n)$ is homeomorphic to a subset of the Cantor set.

proof : ([HY, page 100, Corollary 2-99]) states that a compact, totally disconnected metric space is homeomorphic to a subset of the Cantor set. By the previous three lemmas, we have that $Term(n)$ with the given topology is a compact, metrizable, totally disconnected so that $Term(n)$ with the given topology is homeomorphic to a subset of the Cantor set. □

Corollary: The set of leading monomial ideals for a fixed nonzero ideal I is finite.

proof: Given the nonzero ideal $I \subset k[x_1, \ldots, x_n]$, consider the open cover of $Term(n)$ formed by the sets $U_I[t]$. $Term(n)$ is a compact space, so there exists a finite subcover of this cover. Since the $U_I[t]$ are either disjoint or equal, the number of distinct $U_I[t]$ must be finite. And hence the number of leading monomial ideals of I is finite. □

We are presently unable to say whether $Term(n)$ with the given topology is perfect, although we conjecture that it is. If $Term(n)$ with the given topology is perfect, then $Term(n)$ is homeomorphic to the Cantor set. ([HY, page 100, Corollary 2-98])

In [R] Robbiano gives a classification of term orders on the monomials of $k[x_1, \dots, x_n]$. Robbiano describes such a term order by a system of s orthogonal vectors $v_1, \dots, v_s \in \mathbb{R}^n$, where $1 \leq s \leq n$. He calls the number s the type of the term order. For each of the n entries, the first nonzero appearance of a number in that entry must be positive, and every positive multiple cv of a vector v is considered equivalent to v. Robbiano also defines the number d_i as the dimension of the $\mathbb{R}$- subvectorspace spanned by the $\mathbb{Q}$-linear combinations of the entries of v_i. This definition allows an easy statement of the final condition on the s vectors: $d_1 + d_2 + \ldots + d_s = n$. Robbiano proves that this collection of ordered sets of vectors classifies the term orders on $k[x_1, \dots, x_n]$.

The following is our conjecture that $Term(n)$ with our given topology is perfect and reasons why we believe this should be true.

Definition : Recall that a space X is perfect if every $p \in X$ is a limit point of X. We will use the following

Lemma : $\{p\}$ is not open in $X \Rightarrow p$ is a limit point of X.

proof : Let $U \subset X$ be any open neighborhood of p. Then $\{p\}$ not open implies that $\{p\} \subset U$ and $\{p\} \neq U$. So U contains a point p' of X such that $p \neq p'$. Thus p is a limit point of X. □

Conjecture : $Term(n)$ is perfect.

sketch: Suppose that $t \in Term(n)$ is such that $\{t\}$ is an open set of $Term(n)$. If $\{t\}$ is open, then it must be a finite intersection of basis elements $\{t\} = U_{I_1}[t] \cap U_{I_2}[t] \cap \ldots \cap U_{I_m}[t]$. Then t is the only element of $Term(n)$ which meets all of the finitely many conditions $a_{ij}\ t\ b_{ijk}$, where $a_{ij} = ev(lm(g_{ij}))$, where $g_{ij} =$ the j^{th} polynomial of the reduced Gröbner basis for U_i with respect to t and b_{ijk} runs over the terms of g_{ij} which are not a_{ij}. And, of course, t must satisfy the implications necessitated by the trichotomy, additivity, transitivity, and positivity of basis conditions.

Now assume that t is such that t has type 1. Then $U_{I_1}[t] \cap U_{I_2}[t] \cap \ldots \cap U_{I_m}[t]$ also contains a $t' \neq t$ of type 1, because the relations implied by $a_{ij}\ t\ b_{ij}$ (and the trichotomy, additivity, transitivity, and positivity conditions) are all rational relations.

It is our belief, that with induction or a certain amount of convex geometry, one should be able to show that the term orders of Robbiano type $s \geq 2$ should be able to be perturbed in a similar manner to the term orders of Robbiano type 2.

Then one would have that $\{t\} \subset U_{I_1}[t] \cap U_{I_2}[t] \cap \ldots \cap U_{I_m}[t]$, but $\{t\} \neq U_{I_1}[t] \cap U_{I_2}[t] \cap \ldots \cap U_{I_m}[t]$.

And then lemmas 1-3 plus the proved conjecture would imply the following:

Conjecture : For $n \geq 2$, $Term(n)$ is homeomorphic to the Cantor set.

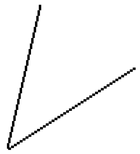
SECTION 10
POLYHEDRAL GEOMETRY

Although Gröbner bases appear to be very algebraic in nature, there is a good deal of geometry associated with them. In this section we will build the necessary prerequisites so that we can show the link between computational algebra and polyhedral geometry.

A good source for information on polyhedral geometry and its relation to Gröbner bases is [St]. Much of this section is derived from Sturmfels's discussions in that text.

Definition : A *polyhedron* P is a finite intersection of closed half-spaces in $\mathbb{R}^n$. We may write $P = \{x \in \mathbb{R}^n : A \cdot x \leq b\}$, where A is a matrix with n columns and b is a constant. If $b = 0$, then there are vectors $u_1, u_2, \ldots, u_m \in \mathbb{R}^n$ such that P is the positive convex hull of those vectors, $P = \{\lambda_1 u_1 + \cdots + \lambda_m u_m : \lambda_i \geq 0 \ \forall i\}$. A polyhedron of this form is called a *polyhedral cone* or simply a *cone*. A compact polyhedron is called a *polytope*. A polytope Q can be realized as the convex hull of a finite set of points, i.e. $Q = \{\lambda_1 v_1 + \cdots + \lambda_m v_m : \lambda_i \geq 0 \ \forall i, \sum \lambda_i = 1\}$.

Below we give examples of polyhedra, cones, and polytopes. Both of these figures are polyhedra. This first figure is a cone:



This figure is a polytope.

Definition : Let P be a polyhedron in $\mathbb{R}^n$ and $\omega \in \mathbb{R}^n$. Then the *face of P with respect to ω* , is defined as $face_\omega(P) = \{u \in P : \omega \cdot u \geq \omega \cdot v \ \forall v \in P\}$. The *dimension* of a face

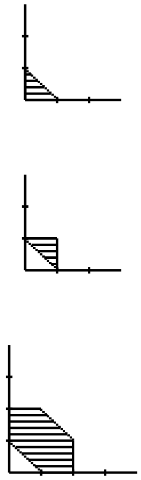
F of a polyhedron P is the dimension of its affine span. Faces of dimension 0 are called *vertices*, and faces of dimension 1 are called *edges*. Note that if $\omega = 0$, then $face_0(P) = P$.

We will need an operation of addition on polytopes. *Minkowski addition of polytopes* is defined by $P_1 + P_2 = \{p_1 + p_2 : p_1 \in P_1, p_2 \in P_2\}$. An important fact about Minkowski sums is that

Proposition:$face_\omega(P_1 + P_2) = face_\omega(P_1) + face_\omega(P_2)$.

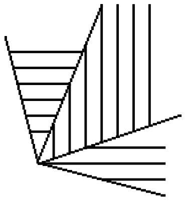
proof: By definition of Minkowski sum, a point $u \in P_1+P_2$ must have form $u = u_1+u_2$, where $u_1 \in P_1$ and $u_2 \in P_2$. Now, without loss of generality, suppose $u_1 \notin face_\omega(P_1)$, so that there exists a $p_1 \in P_1$ such that $p_1 \cdot \omega > u_1 \cdot \omega$. Then $(u_1+u_2)\cdot\omega < (p_1+u_2)\cdot\omega \; \forall u_2 \in P_2$. Hence $u_1 + u_2 \notin face_\omega$ for any $u_2 \in P_2$. So if $u_1 + u_2 = u \in face_\omega(P_1 + P_2)$, we must have that $u_1 \in face_\omega(P_1)$. By symmetry $u_2 \in face_\omega(P_2)$. $\Box$

Note, then, that a vertex v of $P_1 + P_2$ must be a unique sum of vertices p_1 of P_1 and p_2 of P_2. Below, we see the Minkowski sum of two polytopes. The third polytope is the sum of the first two.

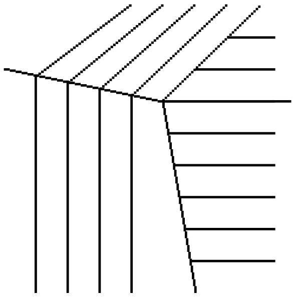


Definition : A *polyhedral fan* or simply a *fan* Δ is a finite collection of polyhedral cones in $\mathbb{R}^n$ such that if $P \in \Delta$ and F is a face of P, then $F \in \Delta$ and for every two cones $P_1, P_2 \in \Delta$, the intersection $P_1 \cap P_2$ is a face of both P_1 and P_2. The *support* of a fan Δ, $\mid \Delta \mid$, is the union of the cones which comprise the fan Δ. Δ is called a *complete fan* if $\mid \Delta \mid = \mathbb{R}^n$.

Here we see a polyhedral fan:



This polyhedral fan is a complete fan:



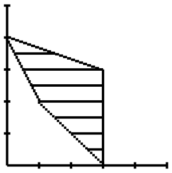
SECTION 11

THE GRÖBNER FAN OF AN IDEAL

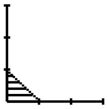
Now we make the relation between polyhedral geometry and computational algebra that was promised in the beginning of the last section. Once again, Sturmfels [St] adds much to this discussion.

<u>Definition</u> : The *Newton polytope* of a polynomial $f = \sum_{i=1}^{m} c_i x^{a_i}, c_i \neq 0$, *New(f)* , is the polytope formed as the convex hull of points represented by the exponent vectors a_i.

Here we can see examples of Newton polytopes of some different polynomials. This Newton polytope is $New(f)$, where $f = x^3y^3 - 8x^3 + 4xy^2 + 7y^4$.

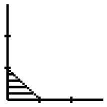


This Newton polytope is $New(g)$, where $g = 2x - y + 1$.

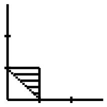


<u>Lemma</u> : New$(f \cdot g)$ = New(f) + New(g), where the sum is to be interpreted as a Minkowski sum.

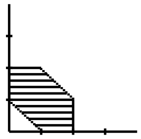
The proof of this statement would take us far afield. We refer the reader to [St, page 11, Lemma 2.2] for the proof. We see this result in action as follows. Let $f = 2x - y + 1$ and let $g = xy + x + y$. Then $f \cdot g = 2x^2y - xy^2 + 2x^2 + 2xy - y^2 + x + y$. This first picture us $New(f)$.



The second picture here is $New(g)$.



This final picture is $New(f) + New(g)$, which we notice is identical to $New(f \cdot g)$.



Definition : Now fix an ideal $I \subset k[x_1, \dots, x_n]$. Two weight vectors ω and ω' are called *equivalent with respect to I* if and only if $in_\omega(I) = in_{\omega'}(I)$.

Definition : For a given ideal I, we define $C[\omega]$ to be the equivalence class of weight vectors that contains the initial ideal represented by the weight vector ω. Equivalently, $C[\omega] = \{\omega' : in_{\omega'}(I) = in_\omega(I)\}$.

Proposition : Each equivalence class $C[\omega]$ of weight vectors is a relatively open convex polyhedral cone. (By relatively open, we mean that the cone is open in its linear span.)

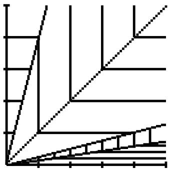
We will omit this proof and refer the reader to [St, page 12, Proposition 2.3].

Definition : The *Gröbner fan of an ideal I, $GF(I)$* , is the set of closed cones $\overline{C[\omega]}$ for all $\omega = (\omega_1, \omega_2, \dots, \omega_n) \in \mathbb{R}^n$ which have a representative in the first (positive) orthant, that is $GF(I)$ consists of all $\overline{C[\omega]}$ which have a representative such that $\omega_i \geq 0 \ \forall i$.

Proposition : The Gröbner fan GF(I) is a polyhedral fan.

proof: [St, page 13, Proposition 2.4]

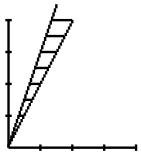
One such Gröbner fan is $GF(I)$ for $I = \langle x^3y - 2x^2y^2 + x, 3x^4 - y \rangle$.



Now that we have defined the Gröbner fan, we present an algorithm for constructing the Gröbner fan of an ideal. Most important in this algorithm is finding the boundary between two cones of the fan. We will determine these boundaries by using exponent vectors to find the proper boundary weight vectors, as is indicated in the following proposition in [St, page 12]: If $G = \{g_1, \ldots, g_s\}$ is the reduced Gröbner basis for an ideal $I \subseteq k[x_1, \ldots, x_n]$ with respect to ω, then $C[\omega] = \{\omega' : in_{\omega'}(g_i) = in_{\omega}(g_i) \; \forall i = 1, \ldots, s\}$.

Take an ideal I and choose an arbitrary $\succ$. Compute the reduced Gröbner basis of I with respect to $\succ$ and call it G. Say $G = \{g_1, g_2, \ldots, g_s\}$. For each g_i, consider the system of inequalities formed as $a_i - b_{ij} > 0$, where $a_i = lm_{\succ}(g_i)$ and where b_{ij} runs over all of the terms of g_i which are not equal to $a_i = lm_{\succ}(g_i)$. Form the corresponding system for each $i = 1, \ldots, s$. Now solve all of the systems simultaneously. The cone which solves all of the inequalities simultaneously is the cone $C[\omega]$ around the weight vector which represents $\succ$ in the sense of the chapter 3 definition.

Example: Let $I = \langle x^3 - y, x^2y - y^2 \rangle$ and take $\omega = (2, 5)$. We compute the reduced Gröbner basis with respect to ω, $G = \{x^3 - y, y^2 - x^2y\}$. The first polynomial gives that slopes less than 3 occur in this cone of the Gröbner fan, while the second tells us that slopes greater than 2 are in this cone. This gives a cone in the plane that looks like the following:



We note that Mora and Robbiano give an algorithm that appears to produce the Gröbner region of an ideal in [MR]. (The Gröbner region of an ideal I is the support of $GF(I)$, $|GF(I)|$.) A slight addition to their algorithm should produce the Gröbner fan of an ideal, but the algorithm given here may be the first written procedure for finding a Gröbner fan for an ideal. A perusal of [MR] shows that our procedure is quite distinct from the algorithm given there.

Gröbner fan procedure

Calculate a reduced Gröbner basis with respect to some term order $\succ$ using the Buchberger algorithm.

Use the discussion above to calculate the boundaries of the cone which contains $\succ$.

While there are regions of the positive orthant not yet filled by some cone of the Gröbner fan, choose a term order (or, equivalently, a weight vector) in an unfilled portion of that first orthant. Use the Buchberger algorithm to find a reduced Gröbner basis. Now calculate the boundaries of the cone containing that term order.

When the first orthant is filled, you have the Gröbner fan of the ideal. The first orthant will fill in finitely many steps because of the result in section 9 that there are finitely many leading monomial ideals (and thus finitely many reduced Gröbner bases) for a given ideal. It will be correct by construction.

In the bivariate case we can give a precise algorithm.

Bivariate Gröbner fan algorithm

INPUT: An ideal $I = \langle f_1, \dots , f_s\rangle$

OUTPUT: The Gröbner fan of the ideal, $GF(I)$.

INITIALIZATION: $m = 0$, $GF(I) = \emptyset$

WHILE: $m \geq 0$, $m \neq \infty$

compute the reduced Gröbner basis of I with respect to m^+, $G_{m^+} = \{g_{m1}, g_{m2}, \cdots , g_{mt}\}$

calculate $n, k \in \mathbb{Q}$, where $n \leq m < k$ and n is the largest rational less than or equal to m and k is the smallest rational greater than m such that $\exists g_{mi}, g_{mj}$ (not necessarily distinct) such that $in_k(g_{mi})$ and $in_n(g_{mj})$ are nonmonomial

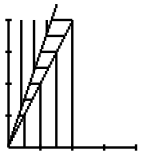
$GF(I) := GF(I) \cup$ the cone from slope n to slope k

$m := k$

Theorem : Given an ideal $I = \langle f_1, \dots , f_s\rangle$, the bivariate Gröbner fan algorithm produces the Gröbner fan of the ideal, $GF(I)$.

proof : The algorithm terminates because $GF(I)$ has only finitely many cones, as shown in section 9 and [MR]. The algorithm produces the correct Gröbner fan by construction. □

Example: Consider the previous ideal $I = \langle x^3 - y, x^2y - y^2 \rangle$. The reduced Gröbner basis for I with respect to the term order 0^+ (Lex with $x \succ y$) is $G_1 = \{y^3 - y^2, xy^2 - y^2, x^3 - y, x^2y - y^2\}$. The first polynomial gives us that slopes greater than 0 are in $C[0^+]$. The second tells us that slopes less than ∞ are in $C[0^+]$. The third gives that slopes less than 3 occur in $C[0^+]$, while the final polynomial gives that slopes less than 2 are in $C[0^+]$. Taking the intersection of all of these inequalities tells us that $C[0^+]$ spans the portion of the first quadrant from slope 0 to slope 2. So, we compute the reduced Gröbner basis of I with respect to 2^+ and call it G_2. $G_2 = \{x^3 - y, y^2 - x^2y\}$. The first polynomial in G_2 tells us that slopes in $C[2^+]$ are less than 3, while the second polynomial reaffirms the boundary of 2 with the first cone. Computing the reduced Gröbner basis with respect to 3^+ yields $G_3 = \{y - x^3, x^6 - x^5\}$. The first polynomial of G_3 reaffirms the boundary with the cone of G_2, while the second gives a final boundary of ∞^-. See the picture below:



If we apply our comment from the end of section 9, we may be able to expand the Gröbner fan algorithm to $Term(n)$ by introducing an explicit order on the elements of $Term(n)$. Our imposed order now tells us with which term order we should start and, in the same way as in the bivariate Gröbner fan algorithm, where to proceed from there. In this way we may be able to move from having a general Gröbner fan procedure to having an actual Gröbner fan algorithm.

The computation of a Gröbner fan begs several questions. We will ask some of those questions and give partial answers to a number of them.

For the first question, we start at the beginning. When does the Gröbner fan have precisely one top-dimensional cone? The most obvious answer is when $I = \langle x^{\alpha_1}, \ldots , x^{\alpha_t} \rangle$ is a monomial ideal. Another case is in a certain class of ideals which have the property that there is only one term that can possibly be the leading term of each polynomial. This happens when the lower order terms of each polynomial are divisors of the leading term of that same polynomial. (There is a geometric analogue of this situation for the bivariate case, and we will look at it in section 13.) A specific example of this case involves when the ideal consists of several univariate polynomials. If $I = \langle f_1(x_1), \ldots, f_k(x_k) \rangle$, then the Gröbner fan also has exactly one top-dimensional cone because each lower degree term in a given polynomial must divide the leading term.

So we look at the other end of the spectrum. How many top-dimensional cones can a Gröbner fan have? The answer turns out to be arbitrarily (finitely) many, and we can show that using a principal bivariate ideal. Let $t(n)$ denote the n^{th} triangular number and consider the ideal $I = \langle x^{t(n)} + x^{t(n)-1}y + x^{t(n)-3}y^2 + \ldots + y^n \rangle$. This ideal has $n+1$ top-dimensional cones in the Gröbner fan, with boundary vectors having slopes $1, 2, \ldots, n+1$. From slope $m = 0$ to 1, $lm_m(I) = x^{t(n)}$; from slope $m = 1$ to 2, $lm_m(I) = x^{t(n)-1}y$; and, in general, from slope $m = k$ to $k+1$, $lm_m(I) = x^{t(n)-k}y^k$.

SECTION 12

UNIVERSAL GRÖBNER BASES AND GRÖBNER WALKS

The concept of a universal Gröbner basis was introduced by Weipsfenning [W] in 1987.

Definition : A finite subset $G \subset I$ is a *universal Gröbner basis* if G is a Gröbner basis of I with respect to all term orders $\succ$ simultaneously.

We recall the following definition and proposition that were given in section 4.

Definition : The monomials which do not lie in $LM(I)$ are the *standard monomials.* Recall that $G \subset I$ is a Gröbner basis for I if $LM(I)$ is generated by $\{lm(g) : g \in G\}$. The following proposition goes back at least as far as Macaulay.

Proposition : Fix a term order $\succ$. The (images of the) standard monomials form a k-vector space basis for the residue ring $k[x_1, \ldots , x_n]/I$.

proof: We first show linear independence. Assume there is some relation $f = \sum_{i=1}^{n} a_i m_i \in I$ with monomials m_i in the standard monomials and $a_i \neq 0$, $a_i \in k$. Then we must have $lm(f) \in LM(I)$. Since $lm(f)$ must be one of the m_i, which are all in the set of standard monomials, this is a contradiction.

Now, suppose that the set of standard monomials does not span $k[x_1, \ldots , x_n]/I$. From the set of elements of $k[x_1, \ldots , x_n]$ not in I and not in the set of standard monomials, choose f with minimal leading term. If $lm(f)$ is in the set of standard monomials, subtract it from f to get a smaller leading term, a contradiction. So, we may assume without loss of generality that $lm(f) \in LM(I)$. Now take an element g of I with $lm(f) = lm(g)$. Then $lm(f - g) \prec lm(f)$, so our choice of $lm(f)$ was not minimal. Contradiction. □

Arguments similar to the following can be found in [MR] and [St]. We note that this result was proved in a new way in section 9 as an application of the topology on $Term(n)$ and will be proved for the bivariate case in a geometric way in section 13.

Theorem : Every ideal $I \subset k[x_1, \dots, x_n]$ has only finitely many distinct leading monomial ideals.

proof: Suppose I has an infinite set L_0 of leading monomial ideals. Choose a nonzero $f_1 \in I$. f_1 is a polynomial, so it has only finitely many terms. Each term of f_1 is in some element of L_0, so there exists a monomial m_1 of f_1 such that $L_1 := \{M \in L_0 : m_1 \in M\}$ is infinite. $\langle m_1 \rangle$ is strictly contained in some leading monomial ideal of I, so the previous proposition implies that the monomials lying outside of $\langle m_1 \rangle$ are k-linearly dependent mod I. So, there exists a nonzero $f_2 \in I$ such that none of its terms are in $\langle m_1 \rangle$. f_2 is a polynomial, so it has only finitely many terms. So there is a monomial m_2 of f_2 such that $L_2 = \{M \in L_1 : m_2 \in M\}$ is infinite. Now, $\langle m_1, m_2 \rangle$ is strictly contained in a leading monomial ideal of I, so the previous proposition implies that the monomials lying outside of $\langle m_1, m_2 \rangle$ are k-linearly dependent mod I. We will continue the constructions to get a strictly increasing chain of monomial ideals $\langle m_1 \rangle \subset \langle m_1, m_2 \rangle \subset \langle m_1, m_2, m_3 \rangle \subset \dots$. Since $k[x_1, \dots, x_n]$ is noetherian, this is a contradiction. □

Corollary : Every ideal $I \subset k[x_1, \dots, x_n]$ possesses a (finite) universal Gröbner basis G.

proof: The previous theorem shows that there are only finitely many leading monomial ideals. Each leading monomial ideal lifts to a unique reduced Gröbner basis because the reduction process for polynomials is only dependent upon leading terms, as seen in section 4. The union of all of the elements of these reduced Gröbner bases gives a universal Gröbner basis. □

Given our Gröbner fan algorithm, we can now find a universal Gröbner basis for any given ideal I. First, perform the Gröbner fan algorithm. Now, take the reduced Gröbner basis from each cone. The union of all of the elements from all of these Gröbner bases is a universal Gröbner basis.

Example: We return to the Gröbner fan example where $I = \langle x^3 - y, x^2y - y^2 \rangle$. We computed that

$$G_1 = \{y^3 - y^2, xy^2 - y^2, x^3 - y, x^2y - y^2\}$$
$$G_2 = \{x^3 - y, y^2 - x^2y\}$$
$$G_3 = \{y - x^3, x^6 - x^5\}$$

were the only three Gröbner bases for I. Thus $U = \{y^3-y^2, xy^2-y^2, x^3-y, x^2y-y^2, x^6-x^5\}$ is a universal Gröbner basis for I. (We formed this universal Gröbner basis by taking the union of the elements of the three Gröbner bases and discarding extra copies of repeated elements.)

This algorithm leads us to investigate some questions. We know that a principal ideal with lower order terms dividing the leading terms gives us a one-generator universal Gröbner basis. Are there two-generator universal Gröbner bases? Can we classify all of them? One such two generator universal Gröbner basis is the case of $I = \langle f(x), g(y) \rangle$. For I, $G = \{f(x), g(y)\}$ is a Gröbner basis in any term order. But are there others? It is our conjecture that there are none of finite codimension. (For instance, any two generator monomial ideal M such that neither generator evenly divides the other will itself be a universal Gröbner basis for the ideal M.)

Concept : A *Gröbner walk* is an approach for a calculation of a Gröbner basis into several smaller calculations following a path in the Gröbner fan of an ideal. A Gröbner walk is an attempt to parallelize some computations and to take advantage of computationally "better" term orders for certain ideals. There are not strict requirements on a Gröbner walk, but for the sake of computational efficiency, one would not want to revisit a cone one had already visited. [CKM], [K], and [T] discuss using a Gröbner walk for such computational efficiency. An intelligent Gröbner walk should provide computational benefits due to some coincidences in adjacent cones of the Gröbner fan, which we see as follows:

As we cross over boundary vectors of the Gröbner fan there are changes that must occur. The reason we cross a boundary is that the leading terms must have changed in at least some of the elements. Since the Buchberger algorithm involves the computation of S-polynomials, and S-polynomials are defined by leading terms of polynomials, there is the potential for certain polynomials to occur in one cone of the Gröbner fan but not to appear in other cones of the Gröbner fan. Likewise, some elements may occur in more than one cone.

Definition : We call an element that occurs in two adjacent cones an *unchanging element* across the boundary, and an element that occurs in only one of the two cones is a *changing element.* The *unchanging part U* of the reduced Gröbner bases across a boundary consists of the unchanging elements, while the *changing part C* of reduced Gröbner bases across a boundary consists of the changing elements. These notions play a large role in the efficacy of Gröbner walks as an alternate way of computing adjacent cones of the Gröbner fan, but they need to be studied in more depth. We have found no mention of these concepts in the literature. The closest investigation is that of Tran in [T], who gave certain conditions one wants to avoid in making one's Gröbner walk through a Gröbner fan of an ideal. Basically, Tran suggests that one should be certain not to choose certain cones of the Gröbner fan as destination or even intermediate points of one's Gröbner walk. Tran states that one should never choose a cone of the Gröbner fan that has dimension less than the top dimension possible. That is, if one wants to form an efficient Gröbner walk for an ideal in $k[x_1, \ldots, x_n]$, one should make certain that each cone one visits in the Gröbner walk has dimension n. If one chooses a cone of smaller dimension, the computation balloons, since one encounters an initial ideal which is nonmonomial. (In fact, many computational algebra systems would not know how to treat such a case. Others, such as Macaulay2, have built-in tiebreaking term orders which forces one into a top-dimensional cone.)

Example: We return to the example of this section and use $I = \langle x^3 - y, x^2y - y^2 \rangle$. The first cone of the Gröbner fan has reduced Gröbner basis $G_1 = \{y^3 - y^2, xy^2 - y^2, x^3 -$

$y, x^2y - y^2\}$, while the second cone has reduced Gröbner basis $G_2 = \{x^3 - y, y^2 - x^2y\}$. The unchanging part across this boundary is $U = \{x^3 - y, y^2 - x^2y\}$, while the changing part $C = \{y^3 - y^2, xy^2 - y^2\}$.

SECTION 13

GRÖBNER FANS AND SOME GEOMETRY

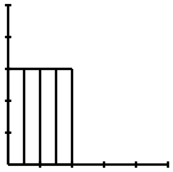
The Gröbner fan has some interesting geometric properties. First, we recall that the boundaries of cones in the Gröbner fan are determined by inequalities which are derived from using the exponent vectors of terms of polynomials in reduced Gröbner bases as coefficients. Then we recall that a Newton polytope of a polynomial is the polytope formed as the convex hull of points which are the exponent vectors of terms of reduced Gröbner bases. This implies an orthogonal relation between these two objects.

We describe this relationship. For the sake of simplicity, let $I = \langle f \rangle$ be a principal ideal in $k[x, y]$. Choosing any arbitrary term order gives that $G = \{f\}$ is the reduced Gröbner basis with respect to that term order. Now we draw the Newton polygon of f, $New(f)$. Recall that $New(f)$ is obtained by taking the convex hull of the exponent vectors x^α that appear with nonzero coefficient in f.

Definition : We say that α is a *leading vertex* of a Newton polygon $New(f)$ if $\alpha + (\mathbb{R}_{\geq 0})^2 \cap New(f) = \alpha$. An edge of a Newton polygon $New(f)$ is an *extremal edge* if at least one of its vertices is a leading vertex of $New(f)$.

Now, the boundary vectors of cones of the Gröbner fan are orthogonal to the extremal edges of the Newton polygon. For, the Newton polygon is defined as the convex hull of exponent vectors of a polynomial. We determine the boundaries between top-dimensional cones of a Gröbner fan by finding the weight vector where the leading term of the polynomial would change from one term to another. This boundary is the place where the initial form ideal is nonmonomial, where the exponent vectors of two monomials both maximize a linear functional. The vector which defines that linear functional is the boundary between two top-dimensional cones of $GF(\langle f \rangle)$. It must be an edge of the Newton polygon, since the edge of a Newton polygon is the set of points which maximizes a linear functional. It is an extremal edge because the leading vertex must have the potential to be a leading monomial of f. These vertices are those that do not divide another monomial present in f, precisely the set of leading vertices.

Here we see a geometric representation of the standard monomials of an ideal. This picture is of the standard monomials of the ideal $I = \langle x^2, y^3 \rangle$.



In the case of principal ideals in $k[x, y]$, the above discussion allows us great latitude in constructing Gröbner fans. If we want to choose an ideal which has only one two-dimensional cone in its Gröbner fan, we can pick any nonzero polynomial f whose Newton polygon has one leading vertex (the edges emanating from it will have nonnegative slope). And, if we want to choose an ideal having n two-dimensional cones in its Gröbner fan, we choose a polynomial f whose Newton polygon has exactly n leading vertices.

There is another relationship that should be noted. Let I be an ideal of finite codimension c. Then the dimension of the set of standard monomials, $dim(\frac{k[x_1,\dots,x_n]}{I})$, is precisely c. Returning to our geometric description of monomial ideals in section 9, we see that the unshaded areas of our graph correspond to the standard monomials of the ideal I. (Note that the union of the graph of the leading monomial ideal of an ideal and the graph of the standard monomials of that same ideal yields the entire positive orthant.)

We note that this corresponds to a so-called Young diagram of the partition of the integer c. This will give us a necessary condition for a set of generators to be a Gröbner basis. If $G = \{g_1, \dots, g_t\}$ is to be a Gröbner basis in any term order, then the monomial ideal $M = \langle lm(g_1), \dots, lm(g_t) \rangle$ must have standard monomials which represent a valid partition of the integer c in the sense of the Young diagrams.

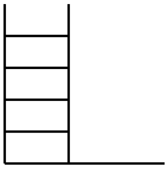
Of course this relationship gives a simple geometric argument for the theorem at the end of section 9. We restate that theorem and then give this alternate proof.

Theorem: In the bivariate case, the set of leading monomial ideals for a fixed ideal I is finite.

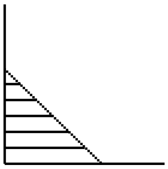
proof: First, suppose that I has finite codimension c. Then any reduced Gröbner basis will have a Young diagram which represents a partition of c. Each Young diagram gives a unique reduced Gröbner basis by the uniqueness of remainders in the reduction process. There are finitely many partitions of any integer c, so there are finitely many reduced Gröbner bases.

Now, suppose that I has infinite codimension. Then $I = \langle f \rangle \cdot J$ where f is the greatest common divisor of all the elements of I (or more simply, f is the gcd of a set of generators for I) and J has finite codimension. By the above, there are finitely many reduced Gröbner bases for J. Since f is a polynomial, there are finitely many choices for $lt(f)$. There are finitely many combinations of these two, so there exist finitely many reduced Gröbner bases for I. □

This relationship has a further application. Certain pieces of computational evidence have shown that Lex is in general a bad choice of term order while in general DegRevLex is the best choice. This is heuristically borne out by the above discussion. During the reduction process, there is a space of terms to which a given monomial m can be reduced. These are precisely the monomials smaller than m. And the monomials smaller than m are determined by the term order. Using Lex gives an unbounded space of smaller monomials in general, as seen here:



Using DegRevLex, on the other hand, gives the smallest possible bounded space.



These relationships once again have to do with the orthogonal property that term orders and Newton polytopes possess.

SECTION 14

FURTHER QUESTIONS

We have raised many questions that are either partially answered or have not been investigated at all. In this section we will try to compile many of those questions.

Although there are many questions about computing a Gröbner basis, we start with more fundamental questions. Given a polynomial g, can we give a criterion which will show that g is an element of some reduced Gröbner basis G for a given ideal I? Or can we show when a given g will not be an element of any reduced Gröbner basis for an ideal I? Further, can we show that a set of polynomials $G = \{g_1, \ldots , g_t\}$ is not a Gröbner basis for I for any term order? Some obvious partial results come from the Buchberger S-polynomial definition, but a thorough treatment of this question has not been given.

In section 5 we discuss the Buchberger algorithm for computing a reduced Gröbner basis. Many questions come from this algorithm. What are good (or bad) classes of problems for Gröbner basis methods? How do we make an intelligent choice of term order for a particular ideal and a particular set of generators? In what order should we calculate S-polynomials? Can we give a thorough treatment of the complexity of the Buchberger algorithm? Is there a link between the Buchberger algorithm and the simplex algorithm?

Our analysis of term orders (sections 8 and 9) leaves several questions unanswered. First, what are further applications of this classification? Are there unexplored implications of the space $Term(2)$ being homeomorphic to the Cantor set? Are there further results implied because the space $Term(n)$ is homeomorphic to a compact subset of the Cantor set? Is $Term(n)$ actually perfect and thus homeomorphic to the Cantor set?

The Gröbner fan (section 11) is also not completely understood. When does the Gröbner fan have one cone? When does it have two cones? Do the sizes of cones in the fan imply anything about the computational complexity or the "sizes" of elements in certain Gröbner bases?

Universal Gröbner bases (section 12) were defined 1987. So there are many unanswered questions about them. Are there two-generator universal Gröbner bases other than for $I = \langle f(x), g(y) \rangle$? Is there a criterion analogous to the Buchberger criterion which will tell us when a set of generators is a universal Gröbner basis?

The Gröbner walk (section 13) is very recent, appearing only as late as 1997. So we would like to know if there are Gröbner walks of minimal size. Are there Gröbner walks involving minimal computation? If there are, can we determine how to choose such a Gröbner walk a priori?

In section 11 we discuss the relation between sets of standard monomials and Young diagrams of partitions of an integer. We wonder if there is any significance to which Young diagrams appear or do not appear for a given ideal. Do certain Young diagrams imply that a Gröbner basis calculation for a particular cone of the Gröbner fan is more efficient or less efficient?

Canfield's question is also important. Certainly there is not an *a priori* order on $Term(n)$. But, if we inject the usual order upon the "middle thirds" Cantor set and then use the isomorphism between $Term(n)$ and a compact subset of this Cantor set, we may be able to impose an order on $Term(n)$.

Finally we ask a more existential question. Now that we have spent so much time studying Gröbner bases, (and so many software packages have applied Gröbner basis methods to ideal-theoretic questions) is there a more efficient method for the computations we want to perform? Others have mentioned (but no great study has been attempted on) resultants, polynomial remainder sequences, resolvents, and characteristic sets. Might Gröbner basis methods in conjunction with one or more of these other methods yield more efficient algorithms?

REFERENCES

[BM] Bayer, David and Morrison, Ian, (1986) *Standard Bases and Geometric Invariant Theory I. Initial Ideals and State Polytopes,* Journal of Symbolic Computation 6, 209-217.

[BS] Bayer, David and Stillman, Michael, (1987) *A theorem on refining division orders by the reverse lexicographical order,* Duke Math Journal 55, 321-328.

[B1] Buchberger, Bruno, (1965) *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomidealen,* Dissertation, Universität Innsbruck.

[B2] Buchberger, Bruno, (1970) *Ein algoritmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems,"* Aequationes Matematicae 4, 374-383.

[B3] Buchberger, Bruno, (1976a) *A theoretical basis for the reduction of polynomials to canonical form,* ACM SIGSAM Bulletin 10(3), 19-29.

[B4] Buchberger, Bruno, (1976b) *Some properties of Gröbner bases for polynomial ideals,* ACM SIGSAM Bulletin 10(4), 19-24.

[B5] Buchberger, Bruno, (1983) *A Note on the Complexity of Constructing Gröbner Bases,* in EUROCAL '83, Springer Lecture Notes in Computer Science 162, 137-145.

[CKM] Collart, S., Kalkbrener, M., and Mall, D., (1997) *Converting bases with the Gröbner walk,* Journal of Symbolic Computation 24, 465-469.

[CLO1] Cox, David, Little, John, and O'Shea, Donal, (1992) *Ideals, Varieties, and Algorithms,* Springer-Verlag, New York.

[CLO2] Cox, David, Little, John, and O'Shea, Donal, (1996) *Using Algebraic Geometry,* Springer-Verlag, New York.

[E] Eisenbud, David, (1995) *Commutative Algebra with a View Toward Algebraic Geometry,* Springer-Verlag, New York.

[FGLM] Faugère, F.C., Gianni, P., Lazard, D. and Mora, T., (1993), *Efficient computation of zero-dimensional Gröbner bases by change of ordering,* Journal of Symbolic Computation 16, 329-344.

[He] Hermann, G., (1926) *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale,* Math. Ann. 95, 763-788.

[HY] Hocking, John G., and Young, Gail S., (1961) *Topology,* Addison-Wesley Publishing Company: Reading, MA.

[Hu] Huynh, D. T., (1986) *A superexponential lower bound for Gröbner bases and Church-Rosser commutative Thue systems,* Information Control 68, 196-206.

[Ka] Kalkbrener, Michael, (1999) *On the Complexity of Gröbner Bases Conversion,* Journal of Symbolic Computation 28, 265-273.

[Ko] Kollreider, C., (1978) *Polynomial reduction: the influence of the ordering of terms on a reduction algorithm,* Camp. Linz. Bericht Nr. 124.

[L] Lazard, D., (1983) *Gröbner bases Gaussian elimination and resolution of systems of algebraic equations,* Proceedings of EUROCAL 83, Springer Lecture Notes in Computer Science 162, 146-156, Springer-Verlag, Berlin.

[Mac] Macaulay, F.S., (1927) *Some properties of enumeration in the theory of modular systems,* Proceedings of the London Mathematical Society 26, 531-555.

[MaMe] Mayr, E.W. and Meyer, A.R., (1982) *The complexity of the word problem for commutative semigroups and polynomial ideals,* Advances in Mathematics 46, 305-329.

[MoMo] Möller, H.M. and Mora, T., (1984) *Upper and lower bounds for the degree of Gröbner bases,* Proceedings of EUROCAL 84, Cambridge, U.K., Springer Lecture Notes in Computer Science 174, 172-183, Springer-Verlag, Berlin.

[MR] Mora, Teo, and Robbiano, Lorenzo, (1988) *The Gröbner fan of an Ideal,* Journal of Symbolic Computation 6, 183-208.

[M] Munkres, James R., (1975) *Topology: a first course,* Prentice Hall: Englewood Cliffs, NJ.

[R] Robbiano, Lorenzo, (1985) *Term Orderings on the Polynomial Ring,* Proceedings of EUROCAL 85. Springer Lecture Notes in Computer Science 174, 513-517.

[Se] Seidenberg, A., (1974) *Constructions in Algebra,* Transactions of the American Mathematical Society 197, 273-313.

[St] Sturmfels, Bernd, (1996) *Gröbner Bases and Convex Polytopes,* American Mathematical Society, Providence, RI.

[T] Tran, Quoc-Nam, (2000) *A Fast Algorithm for Gröbner Basis Conversion and its Applications,* Journal of Symbolic Computation 30, 451-467.

[W] Weipsfenning, V., (1987) Constructing universal Gröbner Bases, Proceedings of AAECC 5 (Menorca).