2006

Grobner Bases and Ideals of Points

Eun R. Chang
Virginia Commonwealth University

Acknowledgment

I wish to express my appreciation to Dr. James K. Deveney for his great support, and excellent teaching. I also like to thank my advisor Dr. Hassan Sedaghat for his guidance and help throughout my graduate study program. With great teachers like them I cannot fail.

To my wonderful children, Jiyun and Eric Chang

GROBNER BASES AND IDEALS OF POINTS

A thesis submitted in partial fulfillment of
the requirements for the degree of
Master of Science at Virginia Commonwealth University

By
Eun Ryung Chang
B.S., Virginia Commonwealth University, May 2004.

Director: Dr. James K. Deveney
Professor
Department of Mathematics

Virginia Commonwealth University
Richmond, Virginia
April, 2006

Contents.

Introduction.

The main point of this thesis is an introduction to the theory of Grobner bases. The concept of Grobner basis and construction of the Grobner basis by Buchberger's Algorithm, in which the notion of S-polynomials is introduced, and a few modified or improved versions of Grobner basis algorithm are reviewed in this paper.

In Chapter 1, we have a review of ideals, the definitions and types of monomial ordering, the multivariate polynomial division algorithm and its examples. After ascertaining the monomial ordering on multivariate polynomials, we establish a leading term of a polynomial.

In Chapter 2, after defining Grobner bases, we study some nice and useful properties of Grobner bases, such as a uniqueness of reduced Grobner basis and existence of a Grobner basis.

In Chapter 3, we explore the Buchberger-Moller algorithm to construct Grobner bases and return a set of polynomials whose residue classes form a basis of a quotient of a polynomial ring. Also, we survey a generalized Buchberger-Moller algorithm to determine directly a Grobner basis for the intersection of a finite number of ideals.

In Chapter 4, we conclude this paper with some applications of Grobner bases.

Chapter 1.

Ideals and General Polynomial Division.

The theory of Grobner bases is very useful. Especially for solving one problem where the problem can become the key to more complicated and various other problems in different areas of mathematics and even outside mathematics (KR 2). To explain Grobner bases, we will need preliminary definitions and some concepts of ideals. Thus, the main purpose of this chapter is to recall a ring, an ideal and general polynomial division.

1.1 A Review of a Ring and an Ideal

Definitions

(1) A **ring** $(R, +, \times)$ has three properties.

a. $(R, +)$ is a commutative group.

b. $\times$ is associative.

c. $\times$ is distributive over $+$.

(2) The ring R is **commutative** if multiplication is commutative.

(3) A **subring** is a subgroup of R, which is closed under $\times$.

(4) For R a commutative ring, a polynomial in x is of the form;

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$$

where $a_i \in R$.

The set of all such polynomials is called the **polynomial ring**, denoted $R[x]$.

(5) Let R and S be rings and $\phi : R \to S$ be a homomorphism.

The **kernel** of ϕ ($\ker \phi$) is a subring of R which maps to 0 in S has a sticky property.

a. Closure under multiplication.

$\forall a \in \ker \phi,\ r \in R$ both $ra, ar \in \ker \phi$.

(6) An **ideal** (I) of a ring (R) has two properties as follows.

a. Subgroup property.

b. Kernel's sticky property under multiplication.

$\forall a \in I$, $r \in R$ both $ra, ar \in I$.

The trivial ideal is $\{0\}$. A ideal is proper if $I \neq R$.

Example 1.1

(1) The rational numbers, Q, is an example of a ring.

(2) Q is commutative under $\times$ and has an identity. Note that a ring is

commutative under $+$, but a commutative ring commutes under $\times$.

(3) $Z/13Z$, is denoted for consisting of the thirteen residue classes,

$$\overline{0}, \overline{1}, \overline{2}, \overline{3}, ..., \overline{11}, \overline{12},$$

is categorized by their remainder of an integer after division by 13. For example an integer 23 is divided by 13, returned the remainder 10, so 23 is an element in the residue class $\overline{10}$. Thus any integers in this residue class are $\overline{10} = \{... - 16, -3, 10, 23, 36, ...\}$, and also are called them the integers congruent to $10 \bmod 13$.

$Z/13Z$ is a ring.

(4) Q is a subring of the real numbers.

(5) In the natural projection $Z \to Z/13Z$, $13Z$ is the kernel, because the multiples of 13 in Z map to 0.

(6) $13Z$ is an ideal of Z, because $13Z$ is a subgroup of Z and anything in $13Z$, say 13, and anything in R, say 2, both 2×13 and 13×2 are in $13Z$.

(7) It is a fact that any ideal I, in the polynomial ring with n variables $K[x_1, x_2, ..., x_n]$, where K is a field, is finitely generated, that is there are

$f_1, ..., f_n$ in I such that for any g in I

$$g = r_1 f_1 + ... + r_n f_n$$

$$\text{where } f_i \in I, \text{ and } r_i \in K[x_1, x_2, ..., x_n]$$

(DF 317). These ideals are called **Noetherian**.

Why are we interested in ideal I? Ideal is used in many different fields of mathematics, such as coding theory. Ideal is a basis for interpolation problems of numerical analysis. Ideal membership problem and test were explained in "Computational Commutative Algebra" by Kreuzer et al,and briefly explained as follows.

Suppose we want to know the solution to the following problem. Let

$$f_1(x_1, ..., x_n) = 0$$

$$\vdots$$

$$f_r(x_1, ..., x_n) = 0$$

be a system of polynomial equations with $n - variables$, and $r - equations$ defined over any arbitrary field, and let

$$f(x_1, ..., x_n) = 0$$

be an additional equation to the system of the equations. Then how do we know that

$$f(x_1, ..., x_n) = 0$$

holds for all solutions of the given system of the equations? A part of the problem is an ideal membership decision. For instance, if there are polynomials $g_1, ..., g_r$ such that

$$f = g_1 \cdot f_1 + ... + g_r \cdot f_r$$

if $f \in I$, then the solution of $f_1 = ... = f_r = 0$, is a solution of $f = 0$.

Example 1.2

Let $I = (x^2y^2 + x, x^3y^4 + y)$ be the ideal, then are $(-x^2 + y)$ and $(x - x^5y^3)$ in the same ideal I ?

$$(-x^2 + y) = (-x) \cdot (x^2y^2 + x) + (x^3y^2 + y).$$

$$(x - x^5y^3) = (x^2y^2 + x) - x^2y(x^3y^2 + y).$$

So both $(-x^2 + y)$ and $(x - x^5y^3)$ are elements of I.

Two elements of a ring are called congruent modulo I, if the difference between them is in the ideal I.

Example 1.3

Let $I = (x^2y^2 + x, x^3y^4 + y)$ be the ideal, and $f_1 = x^2y^2$ and $f_2 = y$. Then $f_1, f_2 \notin I$.How about the difference between them?

$$\begin{aligned} & x^2y^2 - y \\ & = (xy^2) \cdot (x^2y^2 + x) - (x^3y^4 + y) \\ & = x^3y^4 + x^2y^2 - x^3y^4 - y \\ & = x^2y^2 - y \in I \end{aligned}$$

Thus, two polynomials f_1 and f_2 are congruent modulo I.

Then, when do we use the fact that $f \in I$, where $f \in K[x_1, ..., x_n]$? The following Fermat polynomial is one example that uses the fact.

Fermat Polynomials.

The Fermat polynomials are

$$F_n = x^n + y^n - z^n (n \geq 1).$$

They are from Diophantine equation $x^n + y^n = z^n$, but Fermat claimed there is no integer solutions for $n > 2$. So we call them Fermat polynomials. If this F_n is in I,then we can write F_n as a linear combination of $F_1, F_2, ..., F_k$ with their coefficients are from $Q[x, y, z]$. Writing F_n as a linear combination of $F_1, F_2, ..., F_k$, means F_n is generated by $F_1, F_2, ..., F_k$.

This solution by the Grobner bases method was provided in "Grobner Bases and Applications" edited by Buchberger and Winkler in 1998, which connected possible approaches to solving the Fermat problem. We compute a Grobner basis G for Ideal (F_1, F_2, F_3) and check by the reduction of $F_4 \mathrm{mod} G$. If F_4 is in Ideal (F_1, F_2, F_3), then the reduction of $F_4 \mathrm{mod} G$ gives 0. Then we can write

$$F_4 = S_0 \cdot F_1 - S_1 \cdot F_2 + S_2 \cdot F_3$$

where S_i are the elementary symmetric polynomials in x, y, z. ($S_0 = xyz$, $S_1 = xy + xz + yz$, $S_2 = x + y + z$). Since we know that F_4 is in Ideal (F_1, F_2, F_3), then $(F_1, F_2, F_3) = (F_1, F_2, F_3, F_4)$ and so the Grobner basis is the same. Now, check by reduction of $F_5 \mathrm{mod} G$.

If F_5 is in Ideal (F_1, F_2, F_3, F_4), then the reduction of $F_5 \mathrm{mod} G$ gives 0. Then we can write

$$F_5 = S_0 \cdot F_2 - S_1 \cdot F_3 + S_2 \cdot F_4.$$

This Fermat ideal generated by the many F_n is already generated by the first three Fermat polynomials (BW 5).

Remark. From the above pattern, we note that for arbitrary $n \geq 1$,

$$F_{n+3} = S_0 \cdot F_n - S_1 \cdot F_{n+1} + S_2 \cdot F_{n+2}$$

Proof Starting from the right hand side of the equation:

$$
\begin{aligned}
& S_0 \cdot F_n - S_1 \cdot F_{n+1} + S_2 \cdot F_{n+2} \\
& = xyz(x^n + y^n - z^n) - (xy + xz + yz)(x^{n+1} + y^{n+1} - z^{n+1}) \\
& + (x + y + z)(x^{n+2} + y^{n+2} - z^{n+2}) \\
& = x^{n+1}yz + xy^{n+1}z - xyz^{n+1} - (x^{n+2}y + xy^{n+2} - xyz^{n+1} + \\
& x^{n+2}z + x^{n+2}z + xy^{n+1}z - xz^{n+2} + x^{n+1}yz + y^{n+2}z - yz^{n+2}) \\
& + x^{n+3} + xy^{n+2} - xz^{n+2} + x^{n+2}y + y^{n+3} \\
& - yz^{n+2} + x^{n+2}z + y^{n+2}z - z^{n+3} \\
& = x^{n+3} + y^{n+3} - z^{n+3} = F_{n+3}.
\end{aligned}
$$

we end the left side of the equation. Done.

1.2 Definition and Types of Monomial Ordering

Definitions.

A **monomial** is a polynomial with only one nonzero term.

$\geq$ is a **monomial ordering** (often called a term ordering), if the following properties hold.

(Well Ordering) Any non-empty set of monomials has a least element.

(Partial Ordering) (a) Reflexive: $\forall m_1, m_1 \geq m_1$

(b) Transitive: $\forall m_1 m_2, m_3$, if $m_1 \geq m_2$ and $m_2 \geq m_3$, then $m_1 \geq m_3$.

(c)Anti-Symmetric: $\forall m_1 m_2$ if $m_1 \geq m_2$ and $m_2 \geq m_1$, then $m_1 = m_2$.

(Total Ordering) $\forall m_1, m_2$, $m_1 \geq m_2$ or $m_2 \geq m_1$.

(Compatibility) $\forall m_1, m_2$, m, if $m_1 \geq m_2$ then $m\ m_1 \geq m\ m_2$.

Types of Monomial Ordering.

(1) Lexicographic ordering (lex for short): $x_1^{a_1} \cdot x_2^{a_2} \cdot ... \cdot x_n^{a_n} > x_1^{b_1} \cdot x_2^{b_2} \cdot ... \cdot x_n^{b_n}$ if there exists $i, 1 \leq i \leq n$, $a_j = b_j$, for $j < i$ and $a^i > b^i$.

(2) Graded lexicographic ordering (grlex for short): If a monomial ordering on the n variables,

$$x_1^{a_1} x_2^{a_2} ... x_n^{a_n} > x_1^{b_1} x_2^{b_2} ... x_n^{b_n} \Leftrightarrow a_1 + a_2 + ... + a_n > b_1 + b_2 + ... + b_n, \text{ or else}$$

$a_1 + a_2 + ... + a_n = b_1 + b_2 + ... + b_n$ and either $a_1 > b_1$, or $a_1 = b_1$ and $a_2 > b_2$, etc

(3) Graded reverse lexicographic order (grelex for short):

$$x_1^{a_1} x_2^{a_2} ... x_n^{a_n} > x_1^{b_1} x_2^{b_2} ... x_n^{b_n} \Leftrightarrow a_1 + a_2 + ... + a_n > b_1 + b_2 + ... + b_n, \text{ or else}$$

$a_1 + a_2 + ... + a_n = b_1 + b_2 + ... + b_n$ and either $a_n < b_n$, or $a_n = b_n$ and $a_{n-1} < b_{n-1}$, etc

(C 3).

Example 1.4.

(1) With a fixed lexicographic ordering as follows,

$$x_1 > x_2 > ... > x_n, x_1^{a_1} \cdot x_2^{a_2} \cdot ... \cdot x_n^{a_n} > x_1^{b_1} \cdot x_2^{b_2} \cdot ... \cdot x_n^{b_n}$$

if $(a_1 > b_1)$, or$(a_1 = b_1$ and $a_2 > b_2,)$,or $(a_1 = b_1$ and $a_2 = b_2$ and $a_3 > b_3)$ and so on.

Since a monomial ordering is a well ordering, every descending sequence of monomials has only a finite number of monomials.

$$x_1^2 > x_1 x_2^{100} > x_1 x_2^{99} > x_1 x_2 x_3^{100} > ... > x_n$$

this terminates.

(2) $f(x_1, x_2, x_3) = x_1^5 x_2^7 x_3^3 + x_1^6 x_2^6 x_3^2 + x_1 x_2 x_3^{12}$.

Rewrite $f(x_1, x_2, x_3)$ in descending ordering with respect to (w.r.t) lex, w.r.t grlex and w.r.t grelex respectively.

$$f(x_1, x_2, x_3) = x_1^6 x_2^6 x_3^2 + x_1^5 x_2^7 x_3^3 + x_1 x_2 x_3^{12}.\text{(w.r.t.lex)}.$$

$$f(x_1, x_2, x_3) = x_1^5 x_2^7 x_3^3 + x_1^6 x_2^6 x_3^2 + x_1 x_2 x_3^{12}.\text{(w.r.t.grlex)}.$$

$$f(x_1, x_2, x_3) = x_1^5 x_2^7 x_3^3 + x_1 x_2 x_3^{12} + x_1^6 x_2^6 x_3^2.\text{(w.r.t.grelex)}.$$

An ideal I in $K[x_1, x_2, ..., x_n]$ is generated by a collection of polynomials

$f_1, ..., f_r \in K[x_1, x_2, ..., x_n]$,

$$I = (f_1, f_2, ..., f_r) = \left\{ \sum_{i=1}^{r} h_i f_i \mid h_i \in K[x_1, x_2, ..., x_n] \right\}.$$

By the definition of the ideal, each f_i is in I and by the closure under multiplication property, each f_i times any polynomials h_i would give us something in I

Definitions.

(1) With a fixed monomial ordering, the **leading term** of a polynomial f, (denoted $LT(f)$) in $K[x_1, ..., x_n]$ is the monomial term of maximal order in f.

(2) The **ideal of leading terms**;(denoted $LT(I)$) is the ideal generated by the leading terms of all elements of I.

(3) A **monomial ideal** is an ideal generated by monomials.

Later, we will see how a different monomial ordering not only affects the computational time, but also gives the different Grobner basis of the same ideal.

For polynomials in one variable, by using the Division Algorithm, we get $f(x) = q(x) \cdot g(x) + r(x)$. First we compute $LT(f)/LT(g)$, if it is divisible

we get the quotient, say a_1, is added to $q(x)$, then we subtract $a_1 \cdot g(x)$ from the dividend. We reiterate until the degree of the remainder is less than the degree of a divisor. If we extend this concept to the polynomials with many variables, the only extension would be placing the $LT(f)$ into the remainder, and do the process again until we get the zero dividend.

Note that for one variable, when $LT(f)$ is not divisible by $LT(g)$, we would stop, because it already has been reduced.

1.3 General Polynomial Division Algorithm

A reduction algorithm reduces a polynomial to a polynomial which is smaller with respect to the term ordering. A reduction modulo is very similar to general polynomial division with respect to divisors, but the reduction modulo is not necessary getting rid of the leading term. For example, let $x > y$ be the term ordering, and let $f = x^3y^2 + 4xy^2 - 6y^3$ and $g = xy + 5x$, then reduce f to a some polynomial modulo g using xy^2.

$$f - \left(\frac{4xy^2}{xy}\right) \cdot g = x^3y^2 - 6y^3 - 20xy$$

So we note that their leading term x^3y^2 is still present. Thus we want a general polynomial division algorithm.

General Polynomial Division.

With a fixed monomial ordering on $K[x_1, x_2, ...x_n]$,let f be any polynomial in $K[x_1, x_2, ...x_n]$ and $\{g_1, ..., g_m\}$ be a set of polynomials.

We test whether $LT(f)$ is divisible by $LT(g_i)$ for any $i = 1, ..., m$, or not.

Step 1: If $LT(f)$ is divisible by $LT(g_i)$, then go to *Step 2.*

If $LT(f)$ is not divisible by $LT(g_i)$, for any $i = 1, ..., m$, then go to *Step 3.*

Step 2: Since it is divisible, (*i.e.*) $LT(f) = a_i \cdot LT(g_i)$, then add a_i to the quotient q_i.

Replace f by the dividend $f - a_i \cdot (g_i)$. (So the new polynomial has a lower order leading term).

Go to *Step 1* to start the process over until the dividend is 0.

Step 3: Add the leading term of f to the remainder r.

Replace f by the dividend $f - LT(f)$.

Go to *Step 1* to start the process over until the dividend is 0.

When the process stops, we can write

$$f = q_1 g_1 + ... + q_m g_m + r.$$

Note that any non-zero elements of the remainder r are not divisible by any $LT(g_i)$ (DW 320).

1.4. Examples of General Polynomial Division

Example 1.5.

With a fixed monomial ordering $x > y$ on $K[x, y]$, let $f = 2x^4y^2 + 5x^3y^4$ and $g = 3xy^3$. Then $LT(f) = 2x^4y^2$ and $LT(g) = 3xy^3$. The $LT(f)$ is not divisible by $LT(g)$, so we go to Step 3. Add $LT(f) = 2x^4y^2$ to the remainder r.

$$r = [2x^4y^2]$$

Replace f by $f - LT(f) = 2x^4y^2 + 5x^3y^4 - 2x^4y^2 = 5x^3y^4$. (Note that this step gets rid of the leading term). And we start the process over. Now we have $5x^3y^4$, which is divisible by $LT(g)$. So $5x^3y^4 = \left(\frac{5}{3}x^2y\right) \cdot (3xy^3)$, with the quotient $a = \frac{5}{3}x^2y$. Add $\frac{5}{3}x^2y$ to the quotient q.

$$q = \left[\frac{5}{3}x^2y\right]$$

Replace the new dividend $5x^3y^4 - \left(\frac{5}{3}x^2y\right) \cdot (3xy^3) = 0$ Since we get a zero, we are finished

$$r = [2x^4y^2] \text{ and } q = \left[\frac{5}{3}x^2y\right].$$

Therefore,

$$f = 2x^4y^2 + 5x^3y^4 = qg + r = \left(\frac{5}{3}x^2y\right) \cdot (3xy^3) + 2x^4y^2.$$

Example 1.6.

Now with a different monomial ordering, $y > x$, and the same example $f = 2x^4y^2+5x^3y^4$ and $g = 3xy^3$. $LT(f) = 5x^3y^4$ and $LT(g) = 3xy^3$. $LT(f)$ is divisible by $LT(g)$. So $5x^3y^4 = \left(\frac{5}{3}x^2y\right) \cdot (3xy^3)$, with the quotient $a = \frac{5}{3}x^2y$. Add $\frac{5}{3}x^2y$ to the quotient q.

$$q = \left[\frac{5}{3}x^2y\right].$$

Replace the dividend $f = 2x^4y^2 + 5x^3y^4 - \left(\frac{5}{3}x^2y\right) \cdot (3xy^3) = 2x^4y^2$. And we start it over Step 1. Now $2x^4y^2$ is not divisible by $LT(g)$, then we go to Step 3. Add $2x^4y^2$ to the remainder.

$$r = [2x^4y^2].$$

Therefore

$$f = 2x^4y^2 + 5x^3y^4 = qg + r = \left(\frac{5}{3}x^2y\right) \cdot (3xy^3) + 2x^4y^2.$$

Note that on the above two examples that changing the monomial ordering on its dividend does not make any difference, because g is a monomial. If we have g with more than one term, it would affect the answer, which we see in

the following examples 1.7 and 1.8.

Example 1.7.

With a fixed monomial ordering $x > y$ on $K[x, y]$, let $f = 2x^4y^2 + 5x^3y^4$ and $g = 3xy^3 - 4x^3$.

$LT(f) = 2x^4y^2$ and $LT(g) = -4x^3$. Step 1; $LT(f)$ is divisible by $LT(g)$, $(i.e)\ 2x^4y^2 = \left(-\frac{1}{2}xy^2\right) \cdot (-4x^3)$. Step 2; Add the quotient $a = -\frac{1}{2}xy^2$ to q.

$$q = \left[-\frac{1}{2}xy^2\right]$$

Replace

$$f \to 2x^4y^2 + 5x^3y^4 - \left(-\frac{1}{2}xy^2\right) \cdot (3xy^3 - 4x^3) = 5x^3y^4 + \frac{3}{2}x^2y^5.$$

Since the new dividend is not zero, we go to Step 1. $5x^3y^4$ is divisible by $LT(g)$.

Step2, we have $5x^3y^4 = \left(-\frac{5}{4}y^4\right) \cdot (-4x^3)$, with the quotient $a = -\frac{5}{4}y^4$, add it to the quotient q.

$$q = \left[-\frac{1}{2}xy^2 + \left(-\frac{5}{4}y^4\right)\right]$$

Replace the new dividend f by

$$f - a \cdot g = 5x^3y^4 + \frac{3}{2}x^2y^5 - \left(-\frac{5}{4}y^4\right) \cdot (3xy^3 - 4x^3) = \frac{3}{2}x^2y^5 + \frac{15}{4}xy^7.$$

$\frac{3}{2}x^2y^5$ is not divisible by $LT(g)$. Go to Step 3. Add $\frac{3}{2}x^2y^5$ to r;

$$r = \left[\frac{3}{2}x^2y^5\right]$$

Replace f by the dividend $f - LT(f) = \frac{3}{2}x^2y^5 + \frac{15}{4}xy^7 - \frac{3}{2}x^2y^5 = \frac{15}{4}xy^7$.
$\frac{15}{4}xy^7$ is not divisible by $LT(g)$,go to Step 3. Add $\frac{15}{4}xy^7$ to r;

$$r = \left[\frac{3}{2}x^2y^5 + \frac{15}{4}xy^7\right]$$

Replace f by the dividend $\frac{15}{4}xy^7 - \frac{15}{4}xy^7 = 0$. Stop the process.

$$r = \left[\frac{3}{2}x^2y^5 + \frac{15}{4}xy^7\right] \text{ and } q = \left[-\frac{1}{2}xy^2 + \left(-\frac{5}{4}y^4\right)\right].$$

Therefore

$$f = 2x^4y^2+5x^3y^4 = qg+r = \left(-\frac{1}{2}xy^2 + \left(-\frac{5}{4}y^4\right)\right)\cdot(3xy^3-4x^3)+\left(\frac{3}{2}x^2y^5 + \frac{15}{4}xy^7\right).$$

Example 1.8.

Now we do it again with a different monomial ordering $y > x$ on $K[x, y]$, and

the same example

$f = 2x^4y^2 + 5x^3y^4$ and $g = 3xy^3 - 4x^3$.

$LT(f) = 5x^3y^4$ and $LT(g) = 3xy^3$. Step 1; $LT(f)$ is divisible by $LT(g)$,

$(i.e)\ 5x^3y^4 = \left(\frac{5}{3}x^2y\right) \cdot (3xy^3)$. Step 2; Add the quotient $a = \frac{5}{3}x^2y$ to q.

$$q = \left[\frac{5}{3}x^2y\right]$$

Replace $f \to 2x^4y^2 + 5x^3y^4 - \left(\frac{5}{3}x^2y\right) \cdot (3xy^3 - 4x^3) = 2x^4y^2 + \frac{20}{3}x^5y$.

Since the dividend is not zero, we go to Step 1.

$2x^4y^2$ is not divisible by $LT(g)$. So Step3; add $2x^4y^2$ to r.

$$r = \left[2x^4y^2\right]$$

Replace f by $2x^4y^2 + \frac{20}{3}x^5y - 2x^4y^2 = \frac{20}{3}x^5y$.
$\frac{20}{3}x^5y$ is not divisible by $LT(g)$, so Step 3; add $\frac{20}{3}x^5y$ to r.

$$r = \left[2x^4y^2 + \frac{20}{3}x^5y\right].$$

Replace f by $\frac{20}{3}x^5y - \frac{20}{3}x^5y = 0$. Stop.

Therefore

$$f = 2x^4y^2 + 5x^3y^4 = q \cdot g + r = \left(\frac{5}{3}x^2y\right)(3xy^3 - 4x^3) + \left(2x^4y^2 + \frac{20}{3}x^5y\right).$$

As we expected, we found two different ways to write for the same polynomial.

Now what if we have more than one divisor, say, g_1 and g_2 as in examples 1.9 and 1.10. We will examine the effect of changing the order of divisors.

Example 1.9.

$f = 2x^4y^2 + 5xy$ and $g_1 = x^2y^2 + 1$ and $g_2 = x + y$.

(Term ordering $x > y$ and divide by g_1 first and by g_2 second).

$LT(f)$ is divisible by $LT(g_1)$, (i.e.) $2x^4y^2 = (2x^2) \cdot (x^2y^2)$. Add the quotient $2x^2$ to the quotient q_1.

$$q_1 = \left[2x^2\right].$$

Replace f by $2x^4y^2+5xy-(2x^2)\cdot(x^2y^2+1) = 5xy-2x^2.-2x^2$ is not divisible by $LT(g_1)$, but it is divisible by $LT(g_2)$; $(i.e.)$ $-2x^2 = (-2x)\cdot x$. So $-2x$ goes to q_2.

$$q_2 = [-2x].$$

Replace the dividend by $5xy-2x^2-(-2x)\cdot(x+y) = 7xy$. $7xy$ is not divisible by $LT(g_1)$, but it is divisible by $LT(g_2)$;

$(i.e.)$ $7xy = (7y) \cdot x$.

So $7y$ is added to q_2.

$$q_2 = [-2x + 7y]$$

Replace the dividend by

$$7xy - (7y) \cdot (x + y) = -7y^2.$$

$-7y^2$ is not divisible by either $LT(g_1)$ or $LT(g_2)$,s so add $-7y^2$ to r.

Thus, $r = [-7y^2]$. Replace $-7y^2 - (-7y^2) = 0$. Stop.

Therefore

$$f = 2x^4y^2+5xy = q_1 \cdot g_1+q_2 \cdot g_2+r = (2x^2) \cdot (x^2y^2+1)+(-2x+7y) \cdot (x+y)-7y^2.$$

How about changing of order between g_1 and g_2, meaning first divide by g_2 and then by g_1? Are they going to affect the answer? The answer is "Yes". We can predict that division using a different order of the divisors (g_1 and g_2 in these examples) would have the same effect as when the quotients and the remainders are different when changing the monomial order.

Thus we need a tool to get a unique remainder, which would be a Grobner basis in Chapter 2.

Example 1.10.

$f = 2x^4y^2+5xy$ and $g_1 = x^2y^2+1$and $g_2 = x+y$ (Term ordering $x > y$ and use g_2 first and then g_1). $LT(f)$ is divisible by $LT(g_2)$, (*i.e.*) $2x^4y^2 = (2x^3y^2) \cdot (x)$. Add the quotient $2x^3y^2$ to the quotient q_2.

$$q_2 = [2x^3y^2]$$

Replace f by $2x^4y^2+5xy-(2x^3y^2) \cdot (x+y) = 5xy-2x^3y^3$. $-2x^3y^3$is divisible by $LT(g_2)$.

$(i.e.) - 2x^3y^3 = (-2x^2y^3) \cdot x.$

$$q_2 = \left[2x^3y^2 - 2x^2y^3\right].$$

$5xy - 2x^3y^3 - (-2x^2y^3) \cdot (x+y) = 5xy + 2x^2y^4$. $2x^2y^4$ is divisible by $LT(g_2)$,

$(i.e.) 2x^2y^4 = (2xy^4) \cdot x.$

$$q_2 = \left[2x^3y^2 - 2x^2y^3 + 2xy^4\right]$$

Replace $5xy + 2x^2y^4 - \ (2xy^4) \cdot (x+y) = 5xy - 2xy^5$. $-2xy^5$is divisible by

$LT(g_2)$,

$(i.e.) \ -2xy^5 = (\ -2y^5) \cdot x$

$$q_2 = \left[2x^3y^2 - 2x^2y^3 + 2xy^4 - 2y^5\right]$$

Replace to $5xy - 2xy^5 - (\ -2y^5) \cdot (x+y) = 5xy + 2y^6$.

$5xy$ is divisible by $LT(g_2), (i.e.)\ 5xy = (\ 5y) \cdot x$

$$q_2 = \left[2x^3y^2 - 2x^2y^3 + 2xy^4 - 2y^5 + 5y\right].$$

Replace to

$$5xy + 2y^6 - (\ 5y) \cdot (x+y) = 2y^6 - 5y^2.$$

$2y^6$ is not divisible by $LT(g_2)$ or $LT(g_1)$. So add $2y^6$ to r.

$$r = \left[2y^6\right].$$

Replace to

$$2y^6 - 5y^2 - 2y^6 = -5y^2$$

$-5y^2$ is not divisible by $LT(g_2)$ or $LT(g_1)$.. So add $-5y^2$ to r.

$$r = \left[2y^6 - 5y^2\right].$$

Replace to $-5y^2 - 5y^2 = 0$. Stop.

Therefore

$$f = 2x^4y^2+5xy = q_1 \cdot g_1+q_2 \cdot g_2+r = (2x^3y^2-2x^2y^3+2xy^4-2y^5+5y) \cdot (x+y)+\left(2y^6 - 5y^2\right).$$

1.5 Euclidean Algorithm

The computation of Grobner Bases is analogous to the Euclidean Algorithm. We use the Euclidean Algorithm, to get a greatest common divisor of any two integers a and b by iterating the Division Algorithm. If $a, b \in Z$, then we get a sequence of quotient (q_i) and remainders (r_i) as in followings.

$$a = q_0 b \ + r_0$$

$$b = q_1 r_0 + r_1$$

$$r_0 = q_2 r_1 \ + r_2$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n$$

$$r_{n-1} = q_{n+1} r_n + 0$$

We note that the $GCD(a, b)$ is a linear combination of a and b, and $GCD(a, b) = r_n$ (DF 5).

So for example, let $a = 12345$ and $b = 6789$.

$$12345 = 1(6789) + 5556$$

$$6789 = 1(5556) + 1233$$

$$5556 = 4(1233) + 624$$

$$1233 = 1(624) + 609$$

$$624 = 1(609) + 15$$

$$609 = 40(15) + 9$$

$$15 = 1(9) + 6$$

$$9 = 1(6) + 3$$

$$6 = 2(3) + 0$$

$$GCD\ (12345, 6789) = 3$$

It is very interesting to note that computing Grobner bases for one variable polynomials is a generalization of Euclidean Algorithm. Notice that in this Euclidean Algorithm, each procedure gets strictly smaller, so this process terminates. Also in computing Grobner Bases, the procedure gets strictly smaller with respect to the monomial ordering, and will terminate when the all remainders are zeros, which we will see in Chapter 2.

Chapter 2.
Grobner Basis

Austrian Mathematician Bruno Buchberger first invented the concept of a Grobner basis, named after his dissertation advisor Wolfgang Grobner in 1965, when he was given the problem of finding a linearly independent basis for the residue class ring modulo an arbitrary polynomial ideal given by finitely many generators.

2.1 Definition of a Grobner Basis

Definition.

In $K[x_1, ..., x_n]$, a set of generators $\{g_1, ..., g_m\}$ of I whose lead monomials

generate $LT(I)$ is called a **Grobner basis** of I.

$$I = (g_1, ..., g_m) \text{ and } LT(I) = (LT(g_1), ..., LT(g_m)).$$

i.e. every element in I is a linear combination of the generators.

Before we learn how to construct a Grobner basis from a given ideal, we want to know whether a given set of generators is a Grobner basis or not.

Example 2.1.

Fix a monomial order $(x > y)$, and $I = (x^3y + x, x^3 + y)$ then in I, we can have a polynomial

$$f = (x^3y + x) \cdot (-y)(x^3 + y) = x - y^2$$

but $LT(f) = x$ cannot be generated by either $LT(x^3y+x) = x^3y$, or $LT(x^3 + y) = x^3$, because that is cannot be written as

$$f_1(x^3y) + f_2(x^3), \text{ where } f_i \in K[x, y].$$

So $I = (x^3y + x, x^3 + y)$ is not a Grobner basis. Consequently we would like to know how to compute a Grobner basis for I. Before we compute a Grobner basis, how do we know that a Grobner basis always exists for any I?

Remark (Existence of Grobner Basis)

Any ideal I has a Grobner basis.

Proof: By the Hilbert Basis Theorem, any ideal I' in $K[x_1, x_2, ...x_n]$ is finitely generated;

$$I' = (f_1, ..., f_r), \text{where } f_i \in K[x_1, x_2, ...x_n].$$

The proof of Hilbert Basis Theorem is in (DF 316).

Thus $LT(I)$ is also finitely generated.

$$(LT(I)) = (h_1, ..., h_r).$$

Choose any g_i in I whose lead monomial is h_i.

Claim: $\{g_i\}$ is a Grobner basis. Given $m \in I$, divide m by $\{g_1, ..., g_r\}$;

$$m = f_1 g_1 + ... + f_r g_r + rem$$

Assume there is a remainder. Since all g_is are in I, then all $f_i g_i$s are in I too, by the sticky property of the ideal. Also since m is in I, the remainder has to be in I. Then the lead monomial of the remainder is divisible by g_i. It contradicts the assumption. Therefore, the remainder is zero, and we can write it in the form of

$$m = f_1 g_1 + ... + f_r g_r$$

Since m is any arbitrary polynomial in I, and the remainder of m on division by $\{g_1, ..., g_r\}$ is zero, then $\{g_1, ..., g_r\}$ is a Grobner basis. Done.

Buchberger's algorithm is used to construct a Grobner basis from an arbitrary generating set by using S-polynomials and polynomial reduction modulo. In the S-polynomials, "S" refers to subtraction. The basic concept of S-polynomials is similar to the following elementary arithmetic.

Example 2.2.

$f_1 = 2$, $f_2 = 3$ we want to make f_1 and f_2 cancel out to zero by manipulating the other factor of their least common multiple. We make $f_1$and f_2 equal by using the other factor of its own LCM's, that is

$$f_1 \rightarrow \frac{2 \cdot 3}{2} \cdot 2 = 3 \cdot 2 \text{ and } f_2 \rightarrow \frac{3 \cdot 2}{3} \cdot 3 = 2 \cdot 3$$

and we take the difference. Now we get a zero. Note how we get a zero as follows;

$$f_1 \rightarrow \frac{LCM(f_1, f_2)}{f_1} \cdot f_1, \ f_2 \rightarrow \frac{LCM(f_1, f_2)}{f_2} \cdot f_2$$

$$\frac{LCM(f_1, f_2)}{f_1} \cdot f_1 - \frac{LCM(f_1, f_2)}{f_2} \cdot f_2$$

that is what S-polynomials do!

2.2 Buchberger's Algorithm

The following criterion gives an algorithm to detect Grobner bases, and suggest what to do when we do not have a Grobner basis (C 8).

Buchberger Criterion.

A basis $\{g_1, ..., g_u\} \subset I$ is a Grobner basis of I (denoted G), if and only if the remainder of $S(g_i, g_j)$ on division by G is zero for all i, j. We denote that

$$S(g_i, g_j) \equiv 0 \bmod G.$$

The proof of this Buchberger Criterion is in (DF 324).

S-Polynomials.

Let f_1 and f_2 be monic polynomials, and $f_1, f_2 \in K[x_1, x_2, ...x_n]$. The $S-$polynomial of $f_1, f_2 \in K[x_1, ..x_n]$ is defined to be

$$S(f_1, f_2) = \frac{M}{LT(f_1)} f_1 - \frac{M}{LT(f_2)} f_2,$$

where $M = LCM(LM(f_1), LM(f_2))$ and $LM(f_i)$ is the leading monomial of f_i (BW 19).

Although in this S-polynomial, we use f_1 and f_2 as monic polynomials, in

general, the difference between $LM(f_i)$ and $LT(f_i)$ is that $LM(f_i)$ is the leading term $LT(f_i)$ with the coefficient removed, making it a monic, where $LT(f_i)$ is not necessarily monic.

Buchberger's Algorithm.

Let $G = \{f_1, ..., f_s\} \subset K[x_1, ..., x_n]$.

Step 1: Compute remainders of $S(f_i, f_j)$ on division by G, for all $f_i, f_j \in G$ with $i < j$.

Step 2: If the remainder of $S(f_i, f_j)$ on division by G for all f_i, f_j is zero, then G is a Grobner basis. So return G. Stop.

Step 3: If the remainder of $S(f_i, f_j)$ on division by G for any f_i, f_j is not zero, then append the remainder to G. So G is increased by additional polynomial, which is another set of generators. Continue with Step 1.

Reiterate these steps, until the remainders of $S(f_i, f_j)$ on division by G are all zeros Then return G.

This algorithm will terminate after finitely many steps. It returns a Grobner basis G (C 8, KR 123).

Not only the proof of Buchberger's Algorithm, but also the optimizations of Buchberger's Algorithm are in "Computational Commutative Algebra 1" by

Kreuzer in 2000.

Example 2.3.

Let $f_1 = x^3y + 5xy$ and $f_2 = x^2 + 5x^2y^2 - x$ be polynomials. (Fixed term ordering $x > y$).

$LT(f_1) = x^3y$, and $LT(f_2) = 5x^2y^2$.

So $M = LCM(LM(f_1), LM(f_2)) = x^3y^2$.

$$\begin{aligned} S(f_1, f_2) &= \frac{M}{LT(f_1)} f_1 - \frac{M}{LT(f_2)} f_2 \\ &= \frac{x^3y^2}{x^3y} \cdot (x^3y + 5xy) - \frac{x^3y^2}{5x^2y^2} \cdot (x^2 + 5x^2y^2 - x) \\ &= x^3y^2 + 5xy^2 - \frac{1}{5}x^3 - x^3y^2 + \frac{1}{5}x^2 \\ &= 5xy^2 - \frac{1}{5}x^3 + \frac{1}{5}x^2. \end{aligned}$$

So the S-Polynomials get rid of the leading terms while combining f_1 and f_2, but we note that $LT\left(5xy^2 - \frac{1}{5}x^3 + \frac{1}{5}x^2\right) = -\frac{1}{5}x^3$ is not divisible by $LT(f_1)$ or $LT(f_2)$. Therefore f_1, f_2 are not a Grobner basis of $< f_1, f_2 >$.

Generally we can tell if it is a Grobner basis or not by using $S-$polynomials. Still we have not completed the Buchberger's Algorithm, because we don't have a Grobner basis of $< f_1, f_2 >$ yet.

We continue with Example 2.4.

Example 2.4.

Let's use the same polynomials as in Example 2.3 above $F = \{f_1, f_2\}$,

where $f_1 = x^3y + 5xy$, $f_2 = x^2 + 5x^2y^2 - x$.

Step 1: We compute the remainder of $S(f_1, f_2)$. We computed it as in the above example 2.3 :

$$5xy^2 - \frac{1}{5}x^3 + \frac{1}{5}x^2$$

Since we have a non-zero remainder, go to Step 3. Let the remainder be f_3,so $f_3 = 5xy^2 - \frac{1}{5}x^3 + \frac{1}{5}x^2$, and add f_3 to F_1. Thus we have

$$F_1 = \{f_1, f_2, f_3\} = \left\{x^3y + 5xy, x^2 + 5x^2y^2 - x, 5xy^2 - \frac{1}{5}x^3 + \frac{1}{5}x^2\right\}.$$

Step 1: Do the reduction again to compute the remainders.

Now $LT(f_3) = -\frac{1}{5}x^3$ is divisible by $LT(f_3)$, so the remainder is zero.

$$S(f_1, f_2) \equiv 0 \bmod F_1 \text{ (by } f_3).$$

Check the remainder of $S(f_1, f_3)$,and $S(f_2, f_3)$on division by F_1.

$$\begin{aligned} S(f_1, f_3) &= \frac{x^3y}{x^3y}(x^3y + 5xy) - \frac{x^3y}{-\frac{1}{5}x^3}(5xy^2 - \frac{1}{5}\mathbf{x}^3 + \frac{1}{5}x^2) \\ &= x^3y + 5xy + 5y(5xy^2 - \frac{1}{5}\mathbf{x}^3 + \frac{1}{5}x^2) \\ &= x^3y + 5xy + 25xy^3 - x^3y + x^2y \\ &= 5xy + 25xy^3 + x^2y. \end{aligned}$$

Step 3: Since $LT(5xy + 25xy^3 + x^2y) = x^2y$ is not divisible by any $LT(f_i)$ for $i = 1, 2, 3$, we let the remainder by f_4

$$f_4 = 5xy + 25xy^3 + x^2y.$$

And let $F_2 = \{f_1, f_2, f_3, f_4\}$. Then the remainder of $S(f_1, f_3)$ is now divisible by f_4

$$S(f_1, f_3) \equiv 0 \bmod F_2 \text{ (by } f_4).$$

Step 1: We still need to check the remainders of others;

$$\begin{aligned} S(f_2, f_3) &= \frac{x^3y^2}{5x^2y^2}(x^2 + 5x^2y^2 - x) - \frac{x^3y^2}{-\frac{x^3}{5}}(5xy^2 - \frac{x^3}{5} + \frac{x^2}{5}) \\ &= \frac{1}{5}x(x^2 + 5x^2y^2 - x) + 5y^2(5xy^2 - \frac{x^3}{5} + \frac{x^2}{5}) \\ &= \frac{1}{5}x^3 + x^3y^2 - \frac{1}{5}x^2 + 25xy^4 - x^3y^2 + x^2y^2 \\ &= \frac{1}{5}x^3 - \frac{1}{5}x^2 + 25xy^4 + x^2y^2 \end{aligned}$$

We have $LT(\frac{1}{5}x^3 - \frac{1}{5}x^2 + 25xy^4 + x^2y^2) = \frac{1}{5}x^3$ is divisible by $LT(f_3)$, so reducing,

$$\begin{aligned} &\left(\frac{1}{5}x^3 - \frac{1}{5}x^2 + 25xy^4 + x^2y^2\right) + (f_3) \\ &= \left(\frac{1}{5}x^3 - \frac{1}{5}x^2 + 25xy^4 + x^2y^2\right) + \left(5xy^2 - \frac{1}{5}x^3 + \frac{1}{5}x^2\right) \\ &= 25xy^4 + 5xy^2 + x^2y^2 \end{aligned}$$

Now $LT\left(25xy^4+5xy^2+x^2y^2\right)=x^2y^2$ is divisible by $LT(f_2)$, so keep reducing,

$$\begin{aligned}
&\left(25xy^4+5xy^2+x^2y^2\right)-\frac{1}{5}\left(f_2\right)\\
&=\left(25xy^4+5xy^2+x^2y^2\right)-\frac{1}{5}\left(x^2+5x^2y^2-x\right)\\
&\equiv 25xy^4+5xy^2-\frac{1}{5}x^2+\frac{1}{5}x \bmod F_2
\end{aligned}$$

Step 3: Since $LT(25xy^4+5xy^2-\frac{1}{5}x^2+\frac{1}{5}x)=-\frac{1}{5}x^2$ is not divisible by any $LT(f_i)$, let it be f_5;

$$f_5=25xy^4+5xy^2-\frac{1}{5}x^2+\frac{1}{5}x$$

$$F_3=\{f_1,f_2,f_3,f_4,f_5\}$$

$$S(f_2,f_3)\equiv 0 \bmod F_3(\text{by } f_5).$$

Step 1: Since the previous zero remainder is still zero, we need to check

$$S(f_2,f_4), S(f_2,f_5), S(f_3,f_4), S(f_3,f_5), S(f_4,f_5), S(f_1,f_4) \text{ and } S(f_1,f_5)$$

$$\begin{aligned}
S(f_2,f_4)&=\frac{x^2y^2}{5x^2y^2}(x^2+5x^2y^2-x)-\frac{x^2y^2}{x^2y}(5xy+25xy^3+x^2y)\\
&=\frac{1}{5}(x^2+5x^2y^2-x)-y(5xy+25xy^3+x^2y)\\
&=\frac{1}{5}x^2+x^2y^2-\frac{1}{5}x-5xy^2-25xy^4-x^2y^2\\
&=\frac{1}{5}x^2-\frac{1}{5}x-5xy^2-25xy^4
\end{aligned}$$

Thus, whenever, the remainder of S-polynomial on division by F_i is not zero, then we add this remainder to the basis F_{i+1} and do all over again. Note that once we get the remainder is zero, then add it to a Grobner basis and don't compute again (DF 325). In this example, if we keep calculating by using this algorithm, we would have

$$\begin{aligned} F_4 &= \{f_1, f_2, f_3, f_4, f_5, f_6\} \\ &= \{x^3y + 5xy, x^2 + 5x^2y^2 - x, \\ &5xy^2 - \frac{1}{5}x^3 + \frac{1}{5}x^2, 5xy + 25xy^3 + x^2y, \\ &25xy^4 + 5xy^2 - \frac{1}{5}x^2 + \frac{1}{5}x, \\ &125xy^5 + 50xy^3 + 6xy\}. \end{aligned}$$

Now, we have a very large Grobner basis, so we need to reduce it.

2.3 Properties of Grobner Bases.

Definition. Given a monomial ordering on $R = F[x_1, ..., x_n]$, a Grobner basis $\{g_1, ..., g_m\}$ for ideal I in R is called a **reduced Grobner basis** if no term in g_j is divisible by $LT(g_i)$ for $j \neq i$, and $LT(g_i)$ is monic for all i (DF 326)

How do we simplify to a reduced Grobner basis?

First we replace each g_i with its remainder on division by $g_1, ..., g_m$, then discard any remainders that are zero.

Second, whatever left, make their coefficients of leading terms monic (C 9).

Thus, we get a reduced Grobner basis by inter-reducing it, within the Grobner basis.

Example 2.5.

From the above example 2.4

$$\begin{aligned} F_4 &= \{f_1, f_2, f_3, f_4, f_5, f_6\} \\ &= \{x^3y + 5xy, x^2 + 5x^2y^2 - x, \\ &5xy^2 - \frac{1}{5}x^3 + \frac{1}{5}x^2, 5xy + 25xy^3 + x^2y, \\ &25xy^4 + 5xy^2 - \frac{1}{5}x^2 + \frac{1}{5}x, \\ &125xy^5 + 50xy^3 + 6xy\}. \end{aligned}$$

First we replace each f_i with its remainder.

$$G = \left[0, 0, 0, 0, 25xy^4 + 5xy^2 - \frac{1}{5}x^2 + \frac{1}{5}x, 125xy^5 + 50xy^3 + 6xy\right]$$

Second, get rid of zeros, and make a monic leading term, so we get a reduced

Grobner basis as follows:

$$G = \left[x^2 - 125xy^4 - 25xy^2 - x, xy^5 + \frac{2}{5}xy^3 + \frac{6}{125}xy\right].$$

Theorem (Uniqueness of Remainder of a Grobner Basis for I.)

Fix a monomial ordering on $K[x_1, ..., x_n]$ and let $\{g_{1,...,}g_m\}$ be the Grobner basis for the ideal I in $K[x_1, ..., x_n]$. Then every polynomial $f \in K[x_1, ..., x_n]$ can be written uniquely in the form

$$f = f_I + r$$

where $f_I \in I$ and no monomial term of the r is divisible by any $LT(g_i)$ (DF 321).

Proof

For any $f \in K[x_1, ..., x_n]$, Divide f by $\{g_{1,...,}g_m\}$. $f = q_1g_1 + q_2g_2 + ... + q_mg_m + r$

So $f_I = q_1g_1 + q_2g_2 + ... + q_mg_m \in I$

where no term of remainder is divisible by any of the leading monomials of any g_i.

Note that $q_1g_1 + q_2g_2 + ... + q_mg_m$ will be unique if the remainder is, because

$$[q_1g_1 + q_2g_2 + ... + q_mg_m] = f - r$$

Assume that the remainder is not unique.

$$f = q_1 g_1 + q_2 g_2 + ... + q_m g_m + r_1$$

$$f = h_1 g_1 + h_2 g_2 + ... + h_m g_m + r_2$$

$$f - f = 0$$

$$= [q_1 g_1 + q_2 g_2 + ... + q_m g_m] - [h_1 g_1 + h_2 g_2 + ... + h_m g_m]$$

$$+ r_1 - r_2$$

Since $f \in I, ([q_1 g_1 + q_2 g_2 + ... + q_m g_m] - [h_1 g_1 + h_2 g_2 + ... + h_m g_m]) \in I$, $r_1 - r_2 \in I$.

If $[r_1 - r_2] \neq 0$, since $r_1 - r_2 \in I$, the lead monomial of $[r_1 - r_2]$ is divisible by the lead monomial of someg_i. This contradicts the assumption. Therefore $[r_1 - r_2] = 0$, and $r_1 = r_2$, so it is unique.

Theorem (Uniqueness of a Grobner Basis)

Every ideal I has a unique reduced Grobner basis.

A proof can be found in (DF 326), which is based on the fact that two reduced bases have the same number of elements and the same leading terms.

Chapter 3
Other Algorithms for Grobner Bases.

Although the Grobner basis theory is very powerful, its computation can use a lot of computer power. Thus, there are some modified versions of the Buchberger's Algorithm, to compute a Grobner basis more efficiently. The following Buchberger-Moller Algorithm (abbreviated B-M Algorithm) is one of them, which is in the article "Computing Ideals of Points", by Abbott et al. (AB 343).

3.1 Buchberger-Moller Algorithm

Definitions. Let I be the ideal, the additive cosets of R/I form a ring.

$$(a+I)+(b+I)=(a+b)+I$$

$$(a+I)\times(b+I)=(ab)+I$$

This ring of coset is called the quotient ring of R by I = ker and denoted R/I (DF 242).

For example, let K be a field, and consider $K[x]/I$, and let $I=(f(x))=\{g(x)f(x)\mid g(x)\in K[x]\}$. By the Division Algorithm, every polynomial $h(x)\in K[x]$ can be written uniquely in the form

$$h(x)=q(x)f(x)+r(x)$$

where the remainder is $r(x)$, and the degree of $r(x)$ is strictly smaller than the degree of $f(x)$, at most one less than the degree of $f(x)$ Since $q(x)f(x) \in I$ (by ideal's sticky property), every element of the quotient is represented by $r(x)$ (DF 390). Thus a basis for this quotient ring $K[x]/I$ will be

$$\left[\overline{1}, \overline{x}, \overline{x^2}, ..., \overline{x^{n-1}}\right]$$

B-M Algorithm. Let σ be a term ordering on $K[x_1, ..., x_n]$ and let $P_i = (p_{i1}, ..., p_{in}) \in K^n$ for $i = 1, ..., s$.

Step 1: Start with $G = [\,], Q = [\,], S = [\,]$, $L = [\,1\,]$ and a matrix $M = (m_{ij})$ with all zeros in rows and s columns.

Step 2: If L is not empty, then the smallest element of L, say t, according to the ordering σ, delete t from the list L, and go to *Step 4*.

Step 3: If L is empty, then return $[G, Q]$ and stop.

Step 4: Compute the evaluation vector $(t(p_1), ..., t(p_s))$ and reduce it against the rows of M.

$$(v_1, ..., v_s) = (t(p_1), ..., t(p_s)) - \sum_i a_i(m_{i1}, ..., m_{is}) \text{ where } a_i \in K.$$

Step 5: If $(v_1, ..., v_s) = (0, ..., 0)$ then attach the polynomial $t - \sum_i a_i(S_i)$ to the list G, where $S_i$is the i^{th} element of S. Remove from L all multiples of t.

Go to Step 2.

Step 6: If $(v_1, ..., v_s) \neq (0, ..., 0)$,then attach $(v_1, ..., v_s)$ as a new row to M, and attach $t - \sum_i a_i(S_i)$ as a new element to S. And attach t to Q and add those elements of $\{x_1 t, ..., x_n t\}$ which are neither multiples of an element of L nor of $LT(G)$ to L. Reiterate with Step 2.

Note that the B-M algorithm returns Q as the quotient basis and G as the Grobner basis of a vanishing ideal of points $P_i = (p_{i1}, ..., p_{in})$.

Example 3.1.

Let K be a field, let $n = 3$, and let σ be a term ordering $x_1 < x_2 < x_3$. Let the points be $P_1 = (1, 2, 3), P_2 = (4, 5, 6)$. Let $G = [\ ], Q = [\ ], S = [\ ]$, and $L = [\ 1\ ]$. Since the smallest element of L; $t = 1$, by Step 2, delete 1 from L. Step 4: The evaluation vector $(t(P_1), t(P_2)) = (1, 1)$, and reduce it against the rows of M, but M is now empty, so $(1, 1)$. Step 5 is skipped and Step 6, add $(1, 1)$ as a new row to M

$$M = \begin{bmatrix} 1 & 1 \end{bmatrix}$$

and add $1 - \sum_i a_i s_i$ to S, but now we have an empty S, so add 1 to S.

$$S = [1]$$

Attach the power product t to Q,

$$Q = [1]$$

Add elements $\{x_1, x_2, x_3\}$ to L, since they are neither multiples of an element of L, nor of $LT(G)$.

$$L = [x_1, x_2, x_3]$$

Continue with Step 2. Now $t = x_1$, so delete it from L;

$$L = [x_2, x_3]$$

Step 4, the evaluation vector $(t(P_1), t(P_2)) = (x_1(P_1), x_1(P_2)) = (1, 4)$ and reduce it against the rows of M.

$$(1, 4) - 1(1, 1) = (0, 3)$$

Since $(0, 3) \neq (0, 0)$, by Step 6 add $(0, 3)$ as a new row to M

$$M = \begin{bmatrix} 1 & 1 \\ 0 & 3 \end{bmatrix}$$

and $x_1 - \sum_i a_i s_i$ to S, S has 1, so include $x_1 - 1$ as a new element of S.

$$S = [1, x_1 - 1]$$

Attach $t = x_1$ to Q;

$$Q = [1, x_1]$$

and add to L those elements of $\{x_1t, x_2t, x_3t\} = \{x_1^2, x_2x_1, x_3x_1\}$which are neither multiples of an element of L nor of $LT(G)$. It would be $\{x_1^2\}$,

$$L = [x_1^2, x_2, x_3]$$

Continue with Step 2: $t = x_1^2$,

$$L = [x_2, x_3]$$

Step 4, the evaluation vector $(t(P_1), t(P_2)) = (x_1^2(P_1), x_1^2(P_2)) = (1, 16)$ and reduce it against the rows of M.

$$(1, 16) - 1(1, 1) - 5(0, 3) = (0, 0)$$

Since it is $(0, 0)$, by Step 5 attach $x_1^2 - \sum_i a_i s_i$ to list G, since s_i is i^{th} element of S; S has 1 and $x_1 - 1$,so

$$x_1^2 - (1 \cdot (1) + 5 \cdot (x_1 - 1)) = x_1^2 - 5x_1 + 4$$

is appended to the list G.

$$G = [x_1^2 - 5x_1 + 4]$$

Remove from L all multiples of t, don't have any. Again, start with Step 2, $t = x_2$,

$$L = [x_3]$$

Step 4, the evaluation vector $(t(P_1), t(P_2)) = (x_2(P_1), x_2(P_2)) = (2, 5)$ and reduce it against the rows of M.

$$(2, 5) - 2(1, 1) - 1(0, 3) = (0, 0)$$

Since it is $(0, 0)$, by Step 5 attach $x_2 - \sum_i a_i s_i$ to G, S has 1 and $x_1 - 1$,so

$$x_2 - (2 \cdot (1) + 1 \cdot (x_1 - 1)) = x_2 - x_1 - 1$$

is appended to the list G.

$$G = [x_1^2 - 5x_1 + 4, x_2 - x_1 - 1].$$

Remove from L all multiples of t, don't have any. Start with Step 2, $t = x_3$,

$$L = [\,]$$

Step 4, the evaluation vector $(t(P_1), t(P_2)) = ((x_3(P_1), x_3(P_2))) = (3, 6)$ and reduce it against the rows of M.

$$(3, 6) - 3(1, 1) - 1(0, 3) = (0, 0)$$

Since it is $(0, 0)$, by Step 5 attach $x_3 - \sum_i a_i s_i$, S has 1 and $x_1 - 1$,so

$$x_3 - (3 \cdot (1) + 1 \cdot (x_1 - 1)) = x_3 - x_1 - 2$$

is appended to the list of G.

$$G = \left[x_1^2 - 5x_1 + 4, x_2 - x_1 - 1, x_3 - x_1 - 2\right].$$

Go to Step 3, since $L = [\ ]$, we stop. So the reduced Grobner basis of a vanishing ideal of points is

$$G = \left[x_1^2 - 5x_1 + 4, x_2 - x_1 - 1, x_3 - x_1 - 2\right]$$

and the list of power products is Q, which is the quotient basis.

$$Q = [1, x_1]$$

Now we use the algorithm to find the ideal of polynomials for three points.

Example 3.2.

Let K be a field, let $n = 3$, and let σ be a term ordering $x_1 < x_2 < x_3$. Let the points be $P_1 = (1, 2, 3), P_2 = (3, 4, 5), P_3 = (2, 3, 4)$. $G = [\ ], Q = [\ ], S = [\ ]$, and $L = [\ 1\ ]$. Since the smallest element of L; $t = 1$, by Step 2, delete 1 from L.

$$L = [\ ].$$

Step 4: The evaluation vector $(t(P_1), t(P_2), t(P_3)) = (1, 1, 1)$, and reduce it against the rows of M, but M is now empty, so $(1, 1, 1)$. Step 6, add $(1, 1, 1)$ as a new row to M

$$M = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix},$$

and add $1 - \sum_i a_i s_i$ to S, but now we have an empty S, so add 1 to S.

$$S = [1].$$

Attach the power product t to Q,

$$Q = [1]$$

Add all elements of $\{x_1, x_2, x_3\}$ to L, since they are neither multiples of an element of L, nor of $LT(G)$.

$$L = [x_1, x_2, x_3]$$

Continue with Step 2. Now $t = x_1$, so delete it from L;

$$L = [x_2, x_3]$$

Step 4, the evaluation vector $(t(P_1), t(P_2), t(P_3)) = (x_1(P_1), x_1(P_2), x_1(P_3)) = (1, 3, 2)$ and reduce it against the rows of M.

$$(1, 3, 2) - 1(1, 1, 1) = (0, 2, 1)$$

Since $(0, 2, 1) \neq (0, 0, 0)$, by Step 6 add $(0, 2, 1)$ as a new row to M

$$M = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \end{bmatrix}$$

and $x_1 - \sum_i a_i s_i$ to S, S has 1, so include $x_1 - 1$ as a new element of S.

$$S = [1, x_1 - 1]$$

Attach $t = x_1$ to Q;

$$Q = [1, x_1]$$

and add to L those elements of $\{x_1t, x_2t, x_3t\} = \{ x_1^2, x_2x_1, x_3x_1\}$ which are neither multiples of an element of L nor of $LT(G)$, so it would be $\{x_1^2\}$,

$$L = [x_1^2, x_2, x_3]$$

Step 2: $t = x_1^2$,

$$L = [x_2, x_3]$$

Step 4; the evaluation vector $(t(P_1), t(P_2), t(P_3)) = (x_1^2(P_1), x_1^2(P_2), x_1^2(P_3)) = (1, 9, 4)$ and reduce it against the rows of M.

$$(1, 9, 4) - 1(1, 1, 1) - 4(0, 2, 1) = (0, 0, -1)$$

Since it is $(0, 0, -1) \neq (0, 0, 0)$, by Step 6 add $(0, 0, -1)$ as a new row to M

$$M = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & -1 \end{bmatrix},$$

and $x_1^2 - \sum_i a_i s_i$ to S, $x_1^2 - 4x_1 + 3$ as a new element of S.

$$S = [1, x_1 - 1, x_1^2 - 4x_1 + 3].$$

Attach $t = x_1^2$ to Q;

$$Q = [1, x_1, x_1^2]$$

and add to L those elements of $\{x_1t, x_2t, x_3t\} = \{ x_1^3, x_2x_1^2, x_3x_1^2\}$which are neither multiples of an element of L nor of $LT(G)$, so it would be $\{x_1^3\}$,

$$L = [x_1^3, x_2, x_3]$$

Step 2: $t = x_1^3$,

$$L = [x_2, x_3]\,.$$

Step 4, the evaluation vector $(t(P_1), t(P_2), t(P_3)) = (x_1^3(P_1), x_1^3(P_2), x_1^3(P_3)) = (1, 27, 8)$ and reduce it against the rows of M.

$$(1, 27, 8) - 1(1, 1, 1) - 13(0, 2, 1) - 6(0, 0, -1) = (0, 0, 0).$$

Since it is $(0, 0)$, by Step 5 attach $x_1^3 - \sum_i a_i s_i$ to G, ,so

$$x_1^3 - 1 \cdot (1) - 13 \cdot (x_1 - 1) - 6\left(x_1^2 - 4x_1 + 3\right) = x_1^3 - 6x_1^2 + 11x_1 - 6$$

is appended to the list G.

$$G = \left[x_1^3 - 6x_1^2 + 11x_1 - 6\right].$$

Remove from L all multiples of t, don't have any. Start with Step 2, $t = x_2$,

$$L = [x_3]$$

Step 4, the evaluation vector $(t(P_1), t(P_2), t(P_3)) = (x_2(P_1), x_2(P_2), x_2(P_3)) = (2, 4, 3)$ and reduce it against the rows of M.

$$(2, 4, 3) - 2(1, 1, 1) - 1(0, 2, 1) - 0(0, 0, -1) = (0, 0, 0)$$

Since it is $(0, 0, 0)$, by Step 5 attach $x_2 - \sum_i a_i s_i$ to G, so

$$x_2 - 2 \cdot (1) - 1 \cdot (x_1 - 1) - 0\left(x_1^2 - 4x_1 + 3\right) = x_2 - x_1 - 1$$

is appended to the list G.

$$G = \left[x_1^3 - 6x_1^2 + 11x_1 - 6, x_2 - x_1 - 1\right].$$

Remove from L all multiples of t, don't have any. Start with Step 2, $t = x_3$,

$$L = [\quad].$$

Step 4, the evaluation vector $(t(P_1), t(P_2), t(P_3)) = (x_3(P_1), x_3(P_2), x_3(P_3)) = (3, 5, 4)$ and reduce it against the rows of M.

$$(3, 5, 4) - 3(1, 1, 1) - 1(0, 2, 1) - 0(0, 0, -1) = (0, 0, 0)$$

Since it is $(0, 0, 0)$, by Step 5 attach $x_3 - \sum_i a_i s_i$ to G, so

$$x_3 - 3 \cdot (1) - 1 \cdot (x_1 - 1) - 0\left(x_1^2 - 4x_1 + 3\right) = x_3 - x_1 - 1$$

is appended to the list G.

$$G = \left[x_1^3 - 6x_1^2 + 11x_1 - 6, x_2 - x_1 - 1, x_3 - x_1 - 2\right].$$

Go to Step 3, L is empty,so stop and return.

$$G = \left[x_1^3 - 6x_1^2 + 11x_1 - 6, x_2 - x_1 - 1, x_3 - x_1 - 2\right].$$

$$Q = [1, x_1, x_1^2]$$

3.2 Generalized Buchberger-Moller Algorithm.

Now our goal is to compute a Grobner basis of the intersection of ideals, whose zero sets are a finite number of points, where each ideal is represented by a normal form vector map. So we will need to define the normal form vector map, and show that intersection of ideals of K, is an ideal of K.

Definition.

Let I be a zero-dimensional ideal in P, let $\pi : P \to P/I$, and let $\mu = \dim_k(P/I)$ and $\overline{Q} = (\bar{t}_1, \bar{t}_2, ...\bar{t}_\mu)$ be the basis of P/I as a K-vector space. The vector $(a_1, ..., a_\mu) \in K^\mu$ such that

$$\pi(f) = a_1\bar{t}_1 + a_2\bar{t}_2 + ... + a_\mu\bar{t}_\mu$$

is called the **normal form vector** of f with respect to Q and denoted $NFV_Q(f)$.

$$NFV_Q : P \to K^\mu$$

(AK 34).

Proposition. The intersection of ideals of P of a ring R is an ideal of P.

Proof:

Let $\{I_i, i = 1, ..., r\}$ be ideals of P.

We need to show that the ideal $\bigcap_{i=1}^{r} I_i$ has some properties; subring, closure under multiplication properties, and sticky property.

(Subring property): Since each I_i is an ideal of K, it is a subring of K (by the definition of an ideal).

$$\text{Let } a, b \in \bigcap_{i=1}^{r} I_i, \text{ means } a, b \in I_i \text{ for all } i.$$

$$\text{Since each } I_i \text{ is a subring,}$$

$$a + b, a - b \in I_i, \text{ for all } i.$$

(Closure under multiplication):

$$a, b \in \bigcap_{i=1}^{r} I_i$$

$$\forall i, \quad a, b \in I_i$$

$$\forall i, \quad ab \in I_i$$

$$ab \in \bigcap_{i=1}^{r} I_i$$

(Sticky Property):

Since each I_i is a subring, $\forall a \in I_i, r \in R$, both $ra, ar \in I_i$ for all $i = 1, .., r$.

$$\forall a \in \bigcap_{i=1}^{r} I_i, r \in R, \text{ both } ra, ar \in \bigcap_{i=1}^{r} I_i \ .$$

Done.

There have been many efforts to make improved versions of Buchberger's Algorithm, especially in special situations. The following Generalized B-M Algorithm is used for computing a ideal of an intersection of finitely many ideals by using normal form vector maps. The Generalized B-M Algorithm is presented in the article, "Computing Zero-Dimensional Schemes" (AK 37).

Generalized B-M Algorithm.

Let σ be a term ordering on $K[x_1, ..., x_n]$.

Step 1: $G = [\ ], Q = [\ ],\ , L = [\ 1\ ]$ and a matrix $M = (m_{ij})$ with all zeros in rows and s columns.

Step 2: If L is not empty, then the smallest element of L, say t, according to the ordering σ,

delete t from the list L, and go to Step 4.

Step 3: If L is empty, then return $[G, Q]$ and stop.

Step 4: Compute the vector $\mathbf{v} = NFV_{Q_1}(t) + .. + NFV_{Q_S}(t) \in K^{\mu}$ and reduce

it against the rows of M.

$$\mathbf{v}^* = \mathbf{v} - \sum_i a_i \mathbf{m}_i \text{ with } a_i \in K \text{ and where } \mathbf{m}_i \text{ is the } i\text{th row of the } M.$$

Step 5: If $\mathbf{v}^* = (0, ...0)$, then attach the polynomial $t - \sum_i a_i t_i$ to the list G, where t_i is the i^{th} power product in the list Q. Go to Step 2.

Step 6: If $\mathbf{v}^* \neq (0, ..., 0)$,then attach the vector $\mathbf{v}$ as a new row to M, and attach t to Q. And attach those elements of $\{x_1 t, ..., x_n t\}$ which are neither multiples of an element of L nor multiples of $LT(G)$ to L. Go to Step 2 (AK 37).

Example 3.3.

Let K be the field, and σ be the term ordering $x_1 < x_2 < x_3$.

Let one set of points be $P_1 = \{(1, 2, 3), (3, 4, 5), (2, 3, 4)\}$, and another set of points be $P_2 = \{(1, 2, 3), (4, 5, 6)\}$.

From B-M Algorithm, we calculated a Grobner basis for the vanishing ideal of three points;

$$G_1 = \left[x_1^3 - 6x_1^2 + 11x_1 - 6, x_2 - x_1 - 1, x_3 - x_1 - 2\right].$$

and a Grobner basis for the vanishing ideal of two points;

$$G_2 = \left[x_1^2 - 5x_1 + 4, x_2 - x_1 - 1, x_3 - x_1 - 2\right]$$

Note that

$$NFV_{G_1} = \left[\overline{1}, \overline{x_1}, \overline{x_1^2}\right]$$

$$NFV_{G_2} = \left[\overline{1}, \overline{x_1}\right].$$

$G = [\,], Q = [\,], S = [\,]$, and $L = [\ 1\ ]$. Since the smallest element of L; $t = 1$, by Step 2, delete 1 from L.

$$L = [\,]$$

Step 4: Compute the vector

$$\mathbf{v} = NFV_{G_1}(1) \bigoplus NFV_{G_2}(1)$$

$$= (1, 0, 0, 1, 0)$$

Reduce it against the rows of M, but now we have M with zero row and columns.

Thus

$$\mathbf{v}^* = \mathbf{v} - \sum_i a_i \mathbf{m}_i \ = (1, 0, 0, 1, 0).$$

Since $\mathbf{v}^* = (1, 0, 0, 1, 0) \neq (0, 0, 0, 0, 0)$, we go to Step 6; add $v = (1, 0, 0, 1, 0)$ as a new row to M

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

and add 1 to Q

$$Q = [1].$$

and attach $\{x_1 \cdot 1, x_2 \cdot 1, x_3 \cdot 1\}$ to L, since they are neither multiples of an element of L nor multiples of $LT(G)$,

$$L = [x_1, x_2, x_3].$$

Go to Step 2, $t = x_1$, according to the ordering, delete $t = x_1$ from the list L;

$$L = [x_2, x_3].$$

Step 4: Compute the vector

$$\begin{aligned} \mathbf{v} &= NFV_{G_1}(x_1) \bigoplus NFV_{G_2}(x_1) \\ &= (0, 1, 0, 0, 1) \end{aligned}$$

and reduce it against the rows of M.

But we have an already reduced form:

$$\mathbf{v}^* = \mathbf{v} - \sum_i a_i \mathbf{m}_i \ = (0, 1, 0, 0, 1).$$

Since $\mathbf{v}^* = (0, 1, 0, 0, 1) \neq (0, 0, 0, 0, 0)$, go to Step 6; add $v = (0, 1, 0, 0, 1)$as a new row to M

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

and add x_1 to Q

$$Q = [1, x_1].$$

and attach $\{x_1 \cdot x_1, x_2 \cdot x_1, x_3 \cdot x_1\}$ to L, if they are neither multiples of an element of L nor multiples of $LT(G)$, but only x_1^2 is the case;

$$L = [x_1^2, x_2, x_3].$$

Go to Step 2, $t = x_1^2$, according to the ordering, delete $t = x_1^2$ from the list L;

$$L = [x_2, x_3].$$

Step 4; Compute the vector

$$\mathbf{v} = NFV_{G_1}(x_1^2) \bigoplus NFV_{G_2}(x_1^2)$$

Note that $NFV_{G_2}(x_1^2)$ is not formed by the basis $NFV_{G_2} = \left[\overline{1}, \overline{x_1}\right]$, but we can normalize from the Grobner basis

$(x_1^2 - 5x + 4) \in I$ so the cosets of

(x_1^2) and $(-4 + 5x_1)$ are equal

$$\mathbf{v} = NFV_{G_1}(x_1^2) \bigoplus NFV_{G_2}(x_1^2)$$

$$= (0, 0, 1, -4, 5)$$

reduce it against the rows of M.

Thus

$$\mathbf{v}^* = \mathbf{v} - \sum_i a_i \mathbf{m}_i = (0, 0, 1, -4, 5).$$

Since $\mathbf{v}^* = (0,0,1,-4,5) \neq (0,0,0,0,0)$, go to Step 6; add $v = (0,0,1,-4,5)$as a new row to M

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & -4 & 5 \end{bmatrix}$$

and add x_1^2 to Q

$$Q = [1, x_1, x_1^2].$$

and attach $\{x_1 \cdot x_1^2, x_2 \cdot x_1^2, x_3 \cdot x_1^2\}$ to L, if they are neither multiples of an element of L nor multiples of $LT(G)$, but only x_1^3 is the case;

$$L = [x_1^3, x_2, x_3].$$

Go to Step 2, $t = x_1^3$, according to the ordering, delete $t = x_1^3$ from the list L;

$$L = [x_2, x_3].$$

Step 4; Compute the vector

$$\mathbf{v} = NFV_{G_1}(x_1^3) \bigoplus NFV_{G_2}(x_1^3)$$

Note that $NFV_{G_1}(x_1^3)$ is not formed by the basis $NFV_{G_1} = \left[\overline{1}, \overline{x_1}, \overline{x_1^2}\right]$, but

we can normalize from G_1

$$x_1^3 - 6x_1^2 + 11x_1 - 6$$

$$\rightarrow x_1^3 = 6 - 11x_1 + 6x_1^2,$$

Also $NFV_{G_2}(x_1^3)$ is not formed by the basis $NFV_{G_2} = \left[\overline{1}, \overline{x_1}\right]$, but we know that

$$x_1^2 - 5x_1 + 4$$

$$\rightarrow x_1^2 = -4 + 5x_1$$

$$x_1 \cdot x_1^2 = x_1 \cdot (-4 + 5x_1)$$

$$x_1^3 = -4x_1 + 5x_1^2$$

$$x_1^3 = -4x_1 + 5\,(-4 + 5x_1)$$

$$x_1^3 = -20 + 21x_1$$

$$\mathbf{v} = NFV_{G_1}(x_1^3) \bigoplus NFV_{G_2}(x_1^3)$$

$$= (6, -11, 6, -20, 21)$$

reduce it against the rows of M.

Thus

$$\begin{aligned}\mathbf{v}^* &= \mathbf{v} - \sum_i a_i \mathbf{m}_i \\ &= (6, -11, 6, -20, 21) - [6(1,0,0,1,0) - 11(0,1,0,0,1) \\ &+ 6(0,0,1,-4,5)] \\ &= (0,0,0,-2,2).\end{aligned}$$

Since $\mathbf{v}^* = (0,0,0,-2,2) \neq (0,0,0,0,0)$, go to Step 6; add $v = (6,-11,6,-20,21)$ as a new row to M

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & -4 & 5 \\ 6 & -11 & 6 & -20 & 21 \end{bmatrix}$$

and add x_1^3 to Q

$$Q = [1, x_1, x_1^2, x_1^3].$$

and attach $\{x_1 \cdot x_1^3, x_2 \cdot x_1^3, x_3 \cdot x_1^3\}$ to L, if they are neither multiples of an element of L nor multiples of $LT(G)$, but only x_1^4 is the case;

$$L = [x_1^4, x_2, x_3].$$

Go to Step 2, $t = x_1^4$, according to the ordering, delete $t = x_1^4$ from the list

L;

$$L = [x_2, x_3].$$

$NFV_{G_1}(x_1^4)$ is not formed by the basis $NFV_{G_1} = \left[\overline{1}, \overline{x_1}, \overline{x_1^2}\right]$, but we can normalize from G_1

$$x_1^3 - 6x_1^2 + 11x_1 - 6$$

$$\rightarrow x_1^3 = 6 - 11x_1 + 6x_1^2$$

$$x_1 \cdot x_1^3 = x_1 \cdot \left(6 - 11x_1 + 6x_1^2\right)$$

$$x_1^4 = \left(6x_1 - 11x_1^2 + 6x_1^3\right)$$

$$x_1^4 = \left(6x_1 - 11x_1^2 + 6\left(6 - 11x_1 + 6x_1^2\right)\right)$$

$$x_1^4 = \left(36 - 60x_1 + 25x_1^2\right)$$

Also $NFV_{G_2}(x_1^4)$ is not formed by the basis $NFV_{G_2} = \left[\overline{1}, \overline{x_1}\right]$, but we know

that

$$x_1^2 - 5x_1 + 4$$

$$\rightarrow x_1^2 = -4 + 5x_1$$

$$x_1^2 \cdot x_1^2 = (-4 + 5x_1) \cdot (-4 + 5x_1)$$

$$x_1^4 = \left(16 - 40x_1 + 25x_1^2\right)$$

$$x_1^4 = \left(16 - 40x_1 + 25\left(-4 + 5x_1\right)\right)$$

$$x_1^4 = -84 + 85x_1$$

Step 4; Compute the vector

$$\mathbf{v} = NFV_{G_1}(x_1^4) \bigoplus NFV_{G_2}(x_1^4)$$

$$= (36, -60, 25, -84, 85)$$

reduce it against the rows of M.

Thus

$$\mathbf{v}^* = \mathbf{v} - \sum_i a_i \mathbf{m}_i \ = (36, -60, 25, -84, 85) - [-24(1, 0, 0, 1, 0) + 50(0, 1, 0, 0, 1)$$

$$- 35(0, 0, 1, -4, 5) + 10(6, -11, 6, -20, 21)]$$

$$= (0, 0, 0, 0, 0).$$

Since $\mathbf{v}^* = (0,0,0,0,0)$, attach the polynomial

$$t - \sum_i a_i t_i = x_1^4 - \left[-24(1) + 50(x_1) - 35(x_1^2) + 10(x_1^3)\right]$$

$$= x_1^4 - 10x_1^3 + 35x_1^2 - 50x_1 + 24$$

to G

$$G = \left[x_1^4 - 10x_1^3 + 35x_1^2 - 50x_1 + 24\right]$$

Go to Step 2, $t = x_2$, according to the ordering, delete $t = x_2$ from the list L;

$$L = [x_3].$$

Step 4; Compute the vector

$$\mathbf{v} = NFV_{G_1}(x_2) \bigoplus NFV_{G_2}(x_2)$$

$$= (1,1,0,1,1).$$

and reduce it against the rows of M.

Thus

$$\mathbf{v}^* = \mathbf{v} - \sum_i a_i \mathbf{m}_i \ = (1,1,0,1,1) - [(1,0,0,1,0) + (0,1,0,0,1)]$$

$$= (0,0,0,0,0).$$

and attach the polynomial

$$t - \sum_i a_i t_i = x_2 - [1(1) + 1(x_1)]$$

$$= x_2 - x_1 - 1$$

to G

$$G = \left[x_1^4 - 10x_1^3 + 35x_1^2 - 50x_1 + 24, x_2 - x_1 - 1\right]$$

Go to Step 2, $t = x_3$, according to the ordering, delete $t = x_3$ from the list L;

$$L = [\ ].$$

Step 4; Compute the vector

$$\mathbf{v} = NFV_{G_1}(x_3) \bigoplus NFV_{G_2}(x_3)$$

$$= (2, 1, 0, 2, 1)$$

reduce it against the rows of M.

Thus

$$\mathbf{v}^* = \mathbf{v} - \sum_i a_i \mathbf{m}_i \ = (2, 1, 0, 2, 1) - [2(1, 0, 0, 1, 0) + (0, 1, 0, 0, 1)]$$

$$= (0, 0, 0, 0, 0).$$

and attach

$$t - \sum_i a_i t_i = x_3 - [2(1) + 1(x_1)]$$

$$= x_3 - x_1 - 2$$

to G;

$$G = \left[x_1^4 - 10x_1^3 + 35x_1^2 - 50x_1 + 24, x_2 - x_1 - 1, x_3 - x_1 - 2\right]$$

Go to Step 3, since L is empty, return $[G, Q]$ we are done.

$$G = \left[x_1^4 - 10x_1^3 + 35x_1^2 - 50x_1 + 24, x_2 - x_1 - 1, x_3 - x_1 - 2\right]$$

$$Q = [1, x_1, x_1^2, x_1^3].$$

Algorithm. Generally we would get a Grobner basis of intersection of ideals as in the following.

Let I and J be ideals in $K[x_1, ..., x_n]$, and be the term ordering $t > x_1 > ... > x_n$.

Then

$$I \cap J = (tI + (1 - t)J) \cap K[x_1, ..., x_n].$$

$I \cap J$ is the first elimination ideal of $(tI + (1 - t)J)$ (DF 330). So for example

3.4, we had

$$G_1 = \left[x_1^3 - 6x_1^2 + 11x_1 - 6, x_2 - x_1 - 1, x_3 - x_1 - 2\right].$$

$$G_2 = \left[x_1^2 - 5x_1 + 4, x_2 - x_1 - 1, x_3 - x_1 - 2\right]$$

$$\begin{aligned} & t \cdot G_1 + (1-t) \cdot G_2 \\ & = t \cdot \left(x_1^3 - 6x_1^2 + 11x_1 - 6, x_2 - x_1 - 1, x_3 - x_1 - 2\right) \\ & + (1-t) \cdot \left(x_1^2 - 5x_1 + 4, x_2 - x_1 - 1, x_3 - x_1 - 2\right) \end{aligned}$$

Now we can use Maple to compute the Grobner basis with a term ordering $t > x_3 > x_2 > x_1$;

$$\begin{aligned} G = [& x_1^4 - 10x_1^3 + 35x_1^2 - 50x_1 + 24, x_2 - x_1 - 1, x_3 - x_1 - 2 \\ & x_1^3 - 6x_1^2 + 9x_1 + 2tx_1 - 2t - 4] \end{aligned}$$

And then we get rid of polynomials that have the variable t in them;

$$G = \left[x_1^4 - 10x_1^3 + 35x_1^2 - 50x_1 + 24, x_2 - x_1 - 1, x_3 - x_1 - 2\right]$$

Now we have verified that the GBM gave us the intersection of two ideals.

The following modified version of GBM is more efficient, from Abbott et al's article in 2005, by building the matrix in triangular form by appending

the vector v* as a new row to M and append $t - \sum_i a_i t_i$ to Q rather than just t in Step 6 (38).

Example 3.4.

Let K be a field, and let σ be a term ordering $x_1 < x_2 < x_3$. Let the set of points be $P_1 = \{(1,2,3),(3,4,5),(2,3,4)\}$, and another set of points be $P_2 = \{(1,2,3),(4,5,6)\}$.

From B-M Algorithm, we calculated a Grobner basis for the vanishing ideal of three points;

$$G_1 = \left[x_1^3 - 6x_1^2 + 11x_1 - 6, x_2 - x_1 - 1, x_3 - x_1 - 2\right].$$

and a Grobner basis for the vanishing ideal of two points;

$$G_2 = \left[x_1^2 - 5x_1 + 4, x_2 - x_1 - 1, x_3 - x_1 - 2\right]$$

Note that

$$NFV_{G_1} = \left[\overline{1}, \overline{x_1}, \overline{x_1^2}\right]$$

$$NFV_{G_2} = \left[\overline{1}, \overline{x_1}\right].$$

$G = [\,], Q = [\,], S = [\,]$, and $L = [\ 1\ ]$. Since the smallest element of L; $t = 1$, by Step 2, delete 1 from L.

$$L = [\,]$$

.Step 4: Compute the vector

$$\mathbf{v} = NFV_{G_1}(1) \bigoplus NFV_{G_2}(1)$$

$$= (1, 0, 0, 1, 0)$$

Reduce it against the rows of M, but now we have M with zero row and columns.

Thus

$$\mathbf{v}^* = \mathbf{v} - \sum_i a_i \mathbf{m}_i \ = (1, 0, 0, 1, 0).$$

Since $\mathbf{v} = (1, 0, 0, 1, 0) \neq (0, 0, 0, 0, 0)$, we go to Step 6; add $(1, 0, 0, 1, 0)$ as a new row to M

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

and add 1 to Q

$$Q = [1].$$

and attach $\{x_1 \cdot 1, x_2 \cdot 1, x_3 \cdot 1\}$ to L, since they are neither multiples of an element of L nor multiples of $LT(G)$,

$$L = [x_1, x_2, x_3].$$

Go to Step 2, $t = x_1$, according to the ordering, delete $t = x_1$ from the list L;

$$L = [x_2, x_3].$$

Step 4: Compute the vector

$$\mathbf{v} = NFV_{G_1}(x_1) \bigoplus NFV_{G_2}(x_1)$$

$$= (0, 1, 0, 0, 1)$$

and reduce it against the rows of M.

But we have an already reduced form:

$$\mathbf{v}^* = \mathbf{v} - \sum_i a_i \mathbf{m}_i \ = (0, 1, 0, 0, 1).$$

Since $\mathbf{v} = (0, 1, 0, 0, 1) \neq (0, 0, 0, 0, 0)$, go to Step 6; add $(0, 1, 0, 0, 1)$ as a new row to M

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

and add x_1 to Q

$$Q = [1, x_1].$$

and attach $\{x_1 \cdot x_1, x_2 \cdot x_1, x_3 \cdot x_1\}$ to L, if they are neither multiples of an element of L nor multiples of $LT(G)$, but only x_1^2 is the case;

$$L = \left[x_1^2, x_2, x_3\right].$$

Go to Step 2, $t = x_1^2$, according to the ordering, delete $t = x_1^2$ from the list L;

$$L = [x_2, x_3].$$

Step 4; Compute the vector

$$\mathbf{v} = NFV_{G_1}(x_1^2) \bigoplus NFV_{G_2}(x_1^2)$$

$$= (0, 0, 1, -4, 5)$$

reduce it against the rows of M.

Thus

$$\mathbf{v}^* = \mathbf{v} - \sum_i a_i \mathbf{m}_i = (0, 0, 1, -4, 5).$$

Since $\mathbf{v} = (0, 0, 1, -4, 5) \neq (0, 0, 0, 0, 0)$, go to Step 6; add $(0, 0, 1, -4, 5)$ as a new row to M

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & -4 & 5 \end{bmatrix}$$

and add x_1^2 to Q

$$Q = \left[1, x_1, x_1^2\right].$$

and attach $\{x_1 \cdot x_1^2, x_2 \cdot x_1^2, x_3 \cdot x_1^2\}$ to L, if they are neither multiples of an element of L nor multiples of $LT(G)$, but only x_1^3 is the case;

$$L = \left[x_1^3, x_2, x_3\right].$$

Go to Step 2, $t = x_1^3$, according to the ordering, delete $t = x_1^3$ from the list

L;

$$L = [x_2, x_3].$$

Step 4; Compute the vector

$$\begin{aligned}\mathbf{v} &= NFV_{G_1}\left(x_1^3\right) \bigoplus NFV_{G_2}\left(x_1^3\right) \\ &= (6, -11, 6, -20, 21)\end{aligned}$$

reduce it against the rows of M.

Thus

$$\begin{aligned}\mathbf{v}^* &= \mathbf{v} - \sum_i a_i \mathbf{m}_i \\ &= (6, -11, 6, -20, 21) - [6(1, 0, 0, 1, 0) - 11(0, 1, 0, 0, 1) \\ &+ 6(0, 0, 1, -4, 5)] \\ &= (0, 0, 0, -2, 2).\end{aligned}$$

Since $\mathbf{v} = (0, 0, 0, -2, 2) \neq (0, 0, 0, 0, 0)$, go to Step 6; add $(0, 0, 0, -2, 2)$ as a new row to M

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & -4 & 5 \\ 0 & 0 & 0 & -2 & 2 \end{bmatrix}$$

and add

$$x_1^3 - \sum_i a_i t_i = x_1^3 - \left[6(1) - 11(x_1) + 6(x_1^2)\right]$$

$$= x_1^3 - 6x_1^2 + 11x_1 - 6$$

to Q

$$Q = \left[1, x_1, x_1^2, x_1^3 - 6x_1^2 + 11x_1 - 6\right].$$

and attach $\{x_1 \cdot x_1^3, x_2 \cdot x_1^3, x_3 \cdot x_1^3\}$ to L, if they are neither multiples of an element of L nor multiples of $LT(G)$, but only x_1^4 is the case;

$$L = \left[x_1^4, x_2, x_3\right].$$

Go to Step 2, $t = x_1^4$, according to the ordering, delete $t = x_1^4$ from the list L;

$$L = [x_2, x_3].$$

Step 4; Compute the vector

$$\mathbf{v} = NFV_{G_1}(x_1^4) \bigoplus NFV_{G_2}(x_1^4)$$

$$= (36, -60, 25, -84, 85)$$

reduce it against the rows of M.

Thus

$$\mathbf{v}^* = \mathbf{v} - \sum_i a_i \mathbf{m}_i = (36, -60, 25, -84, 85) - [36(1,0,0,1,0) - 60(0,1,0,0,1)$$

$$+ 25(0,0,1,-4,5) + 10(0,0,0,-2,2)]$$

$$= (0,0,0,0,0).$$

Since $\mathbf{v} = (0,0,0,0,0)$, attach the polynomial

$$t - \sum_i a_i t_i = x_1^4 - \left[36(1) - 60(x_1) + 25(x_1^2) + 10(x_1^3 - 6x_1^2 + 11x_1 - 6)\right]$$

$$= x_1^4 - 10x_1^3 + 35x_1^2 - 50x_1 + 24$$

to G

$$G = \left[x_1^4 - 10x_1^3 + 35x_1^2 - 50x_1 + 24\right]$$

Go to Step 2, $t = x_2$, according to the ordering, delete $t = x_2$ from the list L;

$$L = [x_3].$$

Step 4; Compute the vector

$$\mathbf{v} = NFV_{G_1}(x_2) \bigoplus NFV_{G_2}(x_2)$$

$$= (1,1,0,1,1).$$

and reduce it against the rows of M.

Thus

$$\mathbf{v}^* = \mathbf{v} - \sum_i a_i \mathbf{m}_i = (1,1,0,1,1) - [(1,0,0,1,0) + (0,1,0,0,1)]$$

$$= (0,0,0,0,0).$$

and attach the polynomial

$$t - \sum_i a_i t_i = x_2 - [1(1) + 1(x_1)]$$

$$= x_2 - x_1 - 1$$

to G

$$G = \left[x_1^4 - 10x_1^3 + 35x_1^2 - 50x_1 + 24, x_2 - x_1 - 1\right]$$

Go to Step 2, $t = x_3$, according to the ordering, delete $t = x_3$ from the list L;

$$L = [\ ].$$

Step 4; Compute the vector

$$\mathbf{v} = NFV_{G_1}(x_3) \bigoplus NFV_{G_2}(x_3)$$

$$= (2,1,0,2,1)$$

reduce it against the rows of M.

Thus

$$\mathbf{v}^* = \mathbf{v} - \sum_i a_i \mathbf{m}_i \ = (2,1,0,2,1) - [2(1,0,0,1,0) + (0,1,0,0,1)]$$

$$= (0,0,0,0,0).$$

and attach

$$t - \sum_i a_i t_i = x_3 - [2(1) + 1(x_1)]$$

$$= x_3 - x_1 - 2$$

to G;

$$G = \left[x_1^4 - 10x_1^3 + 35x_1^2 - 50x_1 + 24, x_2 - x_1 - 1, x_3 - x_1 - 2\right]$$

Go to Step 3, since L is empty, return $[G, Q]$,we are done.

$$G = \left[x_1^4 - 10x_1^3 + 35x_1^2 - 50x_1 + 24, x_2 - x_1 - 1, x_3 - x_1 - 2\right]$$

$$Q = [1, x_1, x_1^2, x_1^3 - 6x_1^2 + 11x_1 - 6].$$

The idea below will make the computation of the normal form vector easier.

Theorem

Let $u \geq 1$, let $\varphi : P \to K^\mu$ be a K-linear, surjective map whose kernel is

a zero-dimensional ideal I in P, and $\omega = \varphi(1)$. Then there exist $M_1, ...M_n$ such that

(a) $\varphi(x_i f) = M_i \cdot \varphi(f)$ for all $f \in P$ and all $i = 1, .., n$.

(b) $\varphi(f) = f(M_1, ..., M_n) \cdot \omega$ for all $f \in P$ (AK 36).

Proof (a)

Let $g_1, ..., g_u$ be polynomials such that $\varphi(g_k) = e_k \in K^u$ for $k = 1, ..., u$. where e_k is the base for k^μ, so $(a_1, ..., a_u) \in K^\mu \rightarrow \sum a_i e_i$ (linear combination). $\varphi(g_k)$ would look like $\varphi(g_k) = (0, 0, ..., 1, ..., 0)$, where k^{th}entry is 1, and all other entries are 0.

We define M_i to be the matrix whose columns are the vectors $\varphi(x_i g_1), ..., \varphi(x_i g_\mu)$.

We only show for $i = 1$, and for $i = 2, ..., n$ will be a similar proof.

$M_1 = [\varphi(x_1 g_1), ..., \varphi(x_1 g_\mu)]$ where the size of each $\varphi(x_1 g_i)$ is $\mu \times 1$,so the size of M_1 is $\mu \times \mu$.

Claim:

$$\varphi(x_i f) = M_i \cdot \varphi(f)$$

$$M_1 \cdot \varphi(f) = [\varphi(x_1 g_1), ..., \varphi(x_1 g_\mu)] \cdot \begin{bmatrix} f_1 \\ \vdots \\ f_u \end{bmatrix}$$

$$= f_1 \varphi(x_1 g_1) + ... + f_u \varphi(x_1 g_\mu) \text{ (by a block matrix multiplication)}$$

$$\left(\text{where} \varphi(f) = \begin{bmatrix} f_1 \\ \vdots \\ f_\mu \end{bmatrix}, \text{and } f_i \in R \right).$$

Since φ is homomorphism, φ is closed under scalar multiple, so

$$= \varphi(f_1 x_1 g_1) + ... + \varphi(f_\mu x_1 g_\mu)$$

$$= \varphi(f_1 x_1 g_1 + ... + f_\mu x_1 g_\mu).$$

So now we need to show

$$\varphi(x_1 f) = \varphi(f_1 x_1 g_1 + ... + f_\mu x_1 g_\mu).$$

So we need that

$$\varphi(x_1 f) - \varphi(f_1 x_1 g_1 + ... + f_\mu x_1 g_\mu) = 0.$$

That is

$$\varphi\left(x_1 f - (f_1 x_1 g_1 + ... + f_\mu x_1 g_\mu)\right) = 0.$$

$$i.e. \varphi\left(x_1 (f - (f_1 g_1 + ... + f_\mu g_\mu))\right) = 0.$$

However we know that kernel is an ideal, so all we need is

$$\varphi(f - (f_1 g_1 + ... + f_\mu g_\mu)) = 0.$$

$$\varphi(f) - \varphi(f_1 g_1) + ... + \varphi(f_\mu g_\mu)) = 0.$$

$$\varphi(f) - f_1 \varphi(g_1) - ... - f_\mu \varphi(g_\mu) = 0.$$

Since $\varphi(f) = (f_1, ...f_u)$,

$$= \begin{bmatrix} f_1 \\ \vdots \\ f_u \end{bmatrix} - f_1 \begin{bmatrix} 1 \\ \vdots \\ 0 \end{bmatrix} - ... - f_\mu \begin{bmatrix} 0 \\ \vdots \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} f_1 \\ \vdots \\ f_u \end{bmatrix} - \begin{bmatrix} f_1 \\ \vdots \\ 0 \end{bmatrix} - ... - \begin{bmatrix} 0 \\ \vdots \\ f_\mu \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

That's what we need to show. The same ideas work for all M_i.

Proof (b)

We need to show that

$$\varphi(f) = f(M_1, ..., M_n) \cdot \omega \text{ for all } f \in P.$$

Let f be any arbitrary polynomial as a sum of monomials;

$$f = \sum_{i=1}^{n} h_i, \text{ where } h_i \text{ is a monomial}$$

Since φ is a homomorphism, we only need to prove the result for monomials.

We will prove by induction on degree of the monomial.

(Base case) $n = 1$ (degree $= 1$)

$$\begin{aligned}\varphi(x_i) &= \varphi(x_i \cdot 1) \quad \text{for any } i \\ &= M_i \cdot \varphi(1) \quad \text{by (a)} \\ &= M_i \cdot \omega \qquad (\text{since } \omega = \varphi(1), \text{ by hypothesis}).\end{aligned}$$

Thus it is true for the base case.

Assume true for n, and show true for $n+1$.

$$\begin{aligned}\varphi\left(a(x_1^{r_1} \cdot x_2^{r_2} \cdot \ldots \cdot x_n^{r_n})\right) &= a \cdot \varphi\left(x_1 \cdot \left(x_1^{r_1-1} \cdot x_2^{r_2} \cdot \ldots \cdot x_n^{r_n}\right)\right) \text{ (for some constant } a) \\ &= M_1 \cdot \varphi\left(x_1^{r_1-1} \cdot x_2^{r_2} \cdot \ldots \cdot x_n^{r_n}\right) \text{(by part (a))} \\ &= M_1 \cdot M_1^{r_1-1} \cdot M_2^{r_2} \cdot \ldots \cdot M_n^{r_n} \cdot \omega \text{ (by true for } n) \\ &= M_1^{r_1} \cdot M_2^{r_2} \cdot \ldots \cdot M_n^{r_n} \cdot \omega.\end{aligned}$$

Done.

Example 3.5.

$Q[x, y] \to Q \times Q$

$\varphi : f(x, y) \to (f(1, 2), f(3, 4))$ and $\omega = (1, 1)$. And let $g_1 = \dfrac{x(y-4)}{-2}$ and $g_2 = \dfrac{(x-2)(y-2)}{2}$.

Then $M_1 = [\varphi(xg_1), \varphi(xg_2)]$ and $M_2 = [\varphi(yg_1), \varphi(yg_2)]$.

To compute M_1,

$$\varphi(xg_1) = \varphi\left(\frac{x^2(y-4)}{-2}\right) = \left(\frac{1^2(2-4)}{-2}, \frac{3^2(4-4)}{-2}\right) = (1,0)$$

$$\varphi(xg_2) = \varphi\left(\frac{x(x-2)(y-2)}{2}\right) = \left(\frac{1(1-2)(2-2)}{2}, \frac{3(3-2)(4-2)}{2}\right) = (0,3)$$

$$M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}.$$

Similarly,

$$\varphi(yg_1) = \varphi\left(\frac{yx(y-4)}{-2}\right) = \left(\frac{2\cdot 1(2-4)}{-2}, \frac{4\cdot 3(4-4)}{-2}\right) = (2,0).$$

$$\varphi(yg_2) = \varphi\left(\frac{y(x-2)(y-2)}{2}\right) = \left(\frac{2(1-2)(2-2)}{2}, \frac{4(3-2)(4-2)}{2}\right) = (0,4).$$

$$M_2 = \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}.$$

Now let's see how the proposition (a) apply here to this example.

Let $f = x^2y + y$. Then $\varphi(xf) = \varphi(x^3y + xy) = (1^3 \cdot 2 + 1 \cdot 2, 3^3 \cdot 4 + 3 \cdot 4) = (4, 120)$.

$$M_1 \cdot \varphi(f) = \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} \cdot \varphi(x^2y + y) = \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 40 \end{bmatrix} = \begin{bmatrix} 4 \\ 120 \end{bmatrix}$$

Now $\varphi(yf) = \varphi(x^2y^2 + y^2) = (1^2 \cdot 2^2 + 2^2, 3^2 \cdot 4^2 + 4^2) = (8, 160)$.

$$M_2 \cdot \varphi(f) = \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix} \cdot \varphi(x^2y + y) = \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 40 \end{bmatrix} = \begin{bmatrix} 8 \\ 160 \end{bmatrix}.$$

Example 3.6.

We use the same example as in above: $Q[x, y] \rightarrow Q \times Q$

$\varphi : f(x, y) \rightarrow (f(1, 2),\ f(3, 4))$ and $\omega = (1, 1)$. And let $f = x^2y + y$.

$$\varphi(f) = \varphi(x^2y + y) = \left(1^2 \cdot 2 + 2,\ 3^2 \cdot 4 + 4\right)$$

$$= (4,\ 40)$$

Then is $\varphi(f)$ equal to $f(M_1,\ M_2) \cdot \omega$?

In the above example that we found $M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}$ and $M_2 = \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}$.

$$
\begin{aligned}
f\ (M_1, M_2) \cdot \omega &= f\ \left(\begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix} \right) \cdot \omega \\
&= \left(\begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}^2 \cdot \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix} + \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix} \right) \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\
&= \left(\begin{bmatrix} 1 & 0 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix} + \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix} \right) \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\
&= \left(\begin{bmatrix} 2 & 0 \\ 0 & 36 \end{bmatrix} + \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix} \right) \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\
&= \begin{bmatrix} 4 \\ 40 \end{bmatrix}.
\end{aligned}
$$

Remark

In Generalized B-M algorithm Step 4, the power product t is a form of

$$t = x_j \cdot t'$$

for some power product t'. Instead of compute the $NFV_{G_1}(t)$ straight, we compute $NFV_{G_1}(t')$ first, and multiply by x_j (AK 38).

In the above proposition part (a)

$$\varphi(x_i f) = M_i \cdot \varphi(f)$$

In the proof of proposition (a), we know how to construct the matrix

$$M_i = \begin{bmatrix} \varphi(x_i g_1) & \varphi(x_i g_2) & \varphi(x_i g_3) \end{bmatrix}$$

where $\varphi(g_k) = e_k$; where is a base for k^u.

$$\left\{\overline{1}, \overline{x_1}, \overline{x_1^2}\right\} \text{ is basis of } K[x_1, x_2, x_3]/I.$$

$$g_1 = 1, g_2 = x_1, g_3 = x_1^2$$

$$\left\{\overline{1}, \overline{x_1}\right\} \text{ is basis of } K[x_1, x_2]/I.$$

So in example 3.4, we started to have $t = 1$ or $t = x_j t'$ for some power product t'.

For example, in Step 2 and 4, if $t = x_1$, according to the ordering,

$$t = x_1 \cdot 1, \text{ so } t' = 1$$

$$\mathbf{v} = NFV_{G_1}(t') \bigoplus NFV_{G_2}(t') \text{ Note that } t', \text{ instead of } t.$$

$$\mathbf{v} = NFV_{G_1}(1) \bigoplus NFV_{G_2}(1)$$

$$= (1, 0, 0) \bigoplus (1, 0)$$

we store this value, and compute $NFV_{G_i}(x_1)$ by multiplying by x_1 to the value

$$
\begin{aligned}
v &= M_{11}v'_1 + M_{22}v'_2 \\
&= \left(\begin{bmatrix} \varphi(x_1g_1) & \varphi(x_1g_2) & \varphi(x_1g_3) \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right) \bigoplus \left(\begin{bmatrix} \varphi(x_1g_1) & \varphi(x_1g_2) \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right) \\
&= \left(\begin{bmatrix} \varphi(x_1 \cdot 1) & \varphi(x_1 \cdot x_1) & \varphi(x_1 \cdot x_1^2) \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right) \bigoplus \left(\begin{bmatrix} \varphi(x_1 \cdot 1) & \varphi(x_1 \cdot x_1) \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right) \\
&= \left(\begin{bmatrix} 0 & 0 & 6 \\ 1 & 0 & -11 \\ 0 & 1 & 6 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right) \bigoplus \left(\begin{bmatrix} 0 & -4 \\ 1 & 5 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right) \\
&= \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}
\end{aligned}
$$

Next, in Step 2 we have $t = x_1^2$, according to the ordering,

$$t = x_1 \cdot x_1, \text{ so } t' = x_1$$

$$= (0, 1, 0, 0, 1)$$

we had stored this value $(0, 1, 0, 0, 1)$ above, so to compute $NFV_{G_i}(x_1^2)$ by multiplying the value to the matrix we computed

$$\begin{aligned} v &= M_{11}v_1' + M_{22}v_2' \\ &= \left(\begin{bmatrix} 0 & 0 & 6 \\ 1 & 0 & -11 \\ 0 & 1 & 6 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \right) \bigoplus \left(\begin{bmatrix} 0 & -4 \\ 1 & 5 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) \\ &= \begin{bmatrix} 0 \\ 0 \\ 1 \\ -4 \\ 5 \end{bmatrix} \end{aligned}$$

Now, we have $t = x_1^3$,

$$t = x_1 \cdot x_1^2, \text{ so } t' = x_1^2$$

$$= (0, 0, 1, -4, 5)$$

we stored this value $(0, 0, 1, -4, 5)$ above, and compute $NFV_{G_i}(x_1^3)$ by multiplying the value to the matrix

$$
\begin{aligned}
v &= M_{11}v_1' + M_{22}v_2' \\
&= \left(\begin{bmatrix} 0 & 0 & 6 \\ 1 & 0 & -11 \\ 0 & 1 & 6 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right) \oplus \left(\begin{bmatrix} 0 & -4 \\ 1 & 5 \end{bmatrix} \cdot \begin{bmatrix} -4 \\ 5 \end{bmatrix} \right) \\
&= \begin{bmatrix} 6 \\ -11 \\ 6 \\ -20 \\ 21 \end{bmatrix}
\end{aligned}
$$

Thus we obtain the same value, without computing NFV as in Marker 1.The polynomials in Grobner basis have the same roots as the original polynomials. So it is very useful for solving equations and elimination of variables with Grobner basis.

Chapter 4. Applications of Grobner Bases

The method of Grobner basis has been applied to commutative algebra,

polynomial ideal theory, algebraic geometry, interpolation, (inverse polynomial mappings) and systems theory. In commutative algebra, we can apply Grobner basis theory in ideal membership decision and solvability of algebraic systems of equations.

4.1 Optimization.

In most economic problems, we encounter either individuals restrict the choices of goods' available, or individuals are not able to choose any quantities desired such as a budget constraint. Lagrangian multiplier method is one method for solving constrained maximization problems.

Example 4.1.

Suppose individual's goal is to maximize a utility function

$$U(x, y, z) = 4x^2 + 3xy^2 + 5yz$$

but the choices of x, y and z are con strained by a budget $B = P_x \cdot x^2 + P_y \cdot y^2 + P_z \cdot z^2$ where $P_x = \$10, P_y = \$20$ and $P_z = \$30$ are the prices of goods of x, y and z respectively and the budget is \$300.

$$B(x, y, z) = 10 \cdot x^2 + 20 \cdot y^2 + 30 \cdot z^2 = 300$$

By Lagrangian multiplier method, first we set up the expression

$$L(x, y, z, \lambda) = U(x, y, z) - \lambda \left(B(x, y, z) - B\right)$$

where λ is an additional variable, which is the Lagrangian multiplier. Note that L and U have the same value, because $B(x,y,z) - B = 0$ just like polynomials in a Grobner basis have the same roots as the original polynomials.

$$
\begin{aligned}
L &= 4x^2 + 3xy^2 + 5yz - \lambda\left(10 \cdot x^2 + 20 \cdot y^2 + 30 \cdot z^2 - 300\right) \\
\frac{\partial L}{\partial x} &= 8x + 3y^2 - 2\lambda \cdot 10 \cdot x = 0. \quad \left(\text{Let } \frac{\partial L}{\partial x} \text{be } L1.\right) \\
\frac{\partial L}{\partial y} &= 6xy + 5z - 2\lambda \cdot 20 \cdot y = 0. \quad \left(\text{Let } \frac{\partial L}{\partial y} \text{be } L2.\right) \\
\frac{\partial L}{\partial z} &= 5y - 2\lambda \cdot 30 \cdot z = 0. \quad \left(\text{Let } \frac{\partial L}{\partial z} \text{ be } L3.\right) \\
\frac{\partial L}{\partial \lambda} &= -\left(10 \cdot x^2 + 20 \cdot y^2 + 30 \cdot z^2 - 300\right) = 0. \quad \left(\text{Let } \frac{\partial L}{\partial \lambda} \text{ be } L4.\right)
\end{aligned}
$$

Generally, we can solve for x, y, z and λ, if it is a linear system of four equations. However, we have a non-linear system of equations with four unknowns and four equations is not easy. So we use a Grobner basis theory with the lexicographic ordering $x > y > z > \lambda$.

If there is a mathematical software system like Maple or Mathematica, we can just enter to compute Grobner bases

$$
\begin{aligned}
&gbasis([L1, L2, L3, L4], plex(x, y, z, \lambda)); && \text{for Maple,} \\
&GroebnerBasis[L1, L2, L3, L4] && \text{for Mathematica.}
\end{aligned}
$$

into the system. Note that Mathematica spells Groebner Basis, so do Maple.

Especially for Maple to open the package we enter

$$with(Groebner):$$

The result is as in followings;

$GROBNER\ BASIS$

$$= \{-8 + 64128\lambda^3 - 25\lambda^2 + 30\lambda + 691200\lambda^6 - 460800\lambda^5 - 86592\lambda^4,$$

$$4y - 32064\lambda^3 y + 138240\lambda^5 y - 36864\lambda^4 y - 5\lambda y,$$

$$216y^2 - 3456000\lambda^5 + 2304000\lambda^4 + 432960\lambda^3 - 330240\lambda^2 + 3965\lambda - 50,$$

$$48z + 138240\lambda^4 y - 36864\lambda^3 y - 32064\lambda^2 y - 5y,$$

$$1440\lambda x - 576x - 3456000\lambda^5 + 2304000\lambda^4 + 432960\lambda^3 - 330240\lambda^2 + 3965\lambda - 50,$$

$$288xy - 691200\lambda^4 y + 184320\lambda^3 y + 160320\lambda^2 y - 1920\lambda y + 25y,$$

$$165888x^2 + 86400000\lambda^5 + 11520000\lambda^4 - 1608000\lambda^3 - 22761600\lambda^2 - 6415925\lambda + 154850\}$$

Although it looks more complicated than the Lagrangian multipliers, we can find the solution easily. First note that the first equation

$$-8 + 64128\lambda^3 - 25\lambda^2 + 30\lambda + 691200\lambda^6 - 460800\lambda^5 - 86592\lambda^4 = 0$$

has only one variable λ involved, thus solve the first equation for λ. We have $\lambda = \{\frac{2}{5}, 1\}$.

Substitute back to the second equation

$$4y - 32064\lambda^3 y + 138240\lambda^5 y - 36864\lambda^4 y - 5\lambda y = 0$$

although this example regardless of λ, we get that $y = 0$

Since the last equation has x value, we substitute $\lambda = \frac{2}{5}$

$165888x^2 + 86400000\lambda^5 + 11520000\lambda^4 - 1608000\lambda^3 - 22761600\lambda^2 - 6415925\lambda +$

$154850 = 0.$

We just keep the positive value for $x = \sqrt{30}$.

And when $\lambda = 1$,we get imaginary numbers, so unrealistic in this case.

$165888x^2 + 86400000\lambda^5 + 11520000\lambda^4 - 1608000\lambda^3 - 22761600\lambda^2 - 6415925\lambda + 154850 = 0$

$x = \frac{5}{6} \cdot \sqrt{82}i.$

Since $y = 0$, we get z as in followings;

$$48z + 138240\lambda^4 y - 36864\lambda^3 y - 32064\lambda^2 y - 5y = 0$$

$$z = 0$$

So this method is how we do in using a row reduced system of linear equation, that is how Grobner theory to a linear system of equations. To verify that we used up all of our budget \$300,

$$B(\sqrt{30}, 0, 0) = 10 \cdot \sqrt{30}^2 + 20 \cdot 0^2 + 30 \cdot 0^2 = \$300$$

with the maximized utility of 120 as in follows.

$$U(\sqrt{30}, 0, 0) = 4\sqrt{30}^2 + 3\sqrt{30} \cdot 0^2 + 5 \cdot 0 \cdot 0 = 120.$$

There have been many other applications of Grobner bases, for example, integer programming, geometrical theorem proving, and integration of rational functions (BF 29). There is an interesting lecture note "Grobner Bases and Integer Programming" by Hosten and Thomas. It shows how the reduced Grobner bases of ideal are test sets for the integer programming. Also, another lecture note by Michael Moller, discusses the polynomial interpolation problem, which has a given set of distinct points, ask to find all polynomials satisfying some conditions, with Grobner bases techniques. We have seen that Grobner bases are very useful.

Bibliography

[AB] Abbott, J., Bigatti, A., Kreuzer, M., Robbiano, L., 2000. Computing ideals points. Journal of Symbolic Computation. 30, 341-356.

[AK] Abbott, J., Kreuzer, M., Robbiano, L., 2005. Computing zero-dimensional schemes. Journal of Symbolic Computation. 39, 31-38.

[BW] Buchberger, B.,Winkler, F., 1998, "Grobner Bases and Applications.", Cambridge University Press.

[C] Cox, D.,1998. Introduction to Grobner Bases. Proceedings of Symposia

in Applied Mathematics. 53, 1-24.

[DF] Dummit, D., Foote, M., "Abstract Algebra.". 3rd Edition. Wiley.

[KR] Kreuzer,M.,Robbiano,L.,2000."Computational Commutative Algebra 1.", Springer.