[1]

SOME IMPORTANT NOTIONS OF GRÖBNER BASIS AND BUCHBERGER'S ALGORITHM

SHIV DATT KUMAR

Mathematics Department
Motilal Nehru National Institute Of Technology
(Deemed University)
Allahabad (U.P.), India
Email: sdt@mnnit.ac.in

June 4, 2006

Abstract. Buchberger's Algorithm for Gröbner basis furnishes the engine for computations in different areas of mathematics. Theory of Gröbner basis is the basis of many mathematical computer softwares like Singular, CoCoA, and many functions of Mathematica, Mapple, Macauley etc. In this article we describe some of the important and elementary crucial ideas of Gröbner basis theory through examples and we also discuss some basic algorithms viewing it from different angles and give some interesting examples of applications of Gröbner basis.

Key words : Gröbner Basis and Buchberger's Algorithm, Polynomial rings, Ideal.

Introduction

The theory of Gröbner bases was invented by Bruno Buchberger ([3], [4]) in 1965 when he constructed an algorithm to answer questions on the structure of ideals of polynomial rings. Gröbner bases and the Buchbergers algorithm are fundamental notions in Algebra. The algorithm for computing Gröbner bases is known as Buchbergers Algorithm. Gröbner bases is attractive because it easy to understand and explain. Many problems of different areas can be reduced to the problem of computing Gröbner bases. Gröbner bases provide a uniform approach to solve problems expressed in terms of multivariate polynomials. The determination of a Gröbner basis is roughly analogous to
(i) computing an orthonormal basis from a set of basis vectors
(ii) generalization of Gaussian elimination (for solving a system of linear equations)
(iii) the Euclidean Algorithm (for computing GCD of univariate polynomials over a field)
(iv) Simplex Algorithm for linear programming.

[1] AMS Classification: 13P10, 13F20

The application of Gröbner bases include Algebraic Geometry, Commutative and non-commutative algebra, coding theory, integer programming, partial differential equations, hyper geometric functions, system theory etc. Software Singular, CoCoA, Macauley2, Mathematicas functions Solve, Algebraic Rules, Eliminate and related functions and symbolic algorithms for manipulating polynomials in several variables are based on Gröbner basis theory. These functions take sets of equations as arguments. Gröbner bases are pervasive in the construction of symbolic algebra algorithms, and with respect to lexicographic order, this is very useful for solving equations and for elimination of variables. In this article we try to give an elementary introduction of the Gröbner bases theory via two applications: solving systems of polynomial equations, eliminating parameters from polynomial equations. Some good references of text books developing the theory of Gröbner bases and their applications to problems in algebra and geometry include (See [1], [2], [5]).

Solutions of Systems of Polynomial Equations

Gröbner basis is very useful for solving system of polynomial equations. A Gröbner basis G for a system of finite set of polynomials F is an equivalence system that generates the same ideal in $K[x_1, \ldots, x_n]$ and possesses useful properties. Furthermore, the set of polynomials in a Gröbner basis have the same collection of roots as the original polynomials. The advantage of G is that it reveals geometric properties that are not visible for F. For linear functions in any number of variables, a Gröbner basis is equivalent to Gaussian elimination. Solving systems of polynomial equations provides a good introduction to the subject. The solution technique underlying to the solve functions may be viewed as an extension of the standard method of solving systems of linear equations, reduction to triangular form. For example the pair of equations

$4x + 7y = 1$

$2x + 5y = 5 \qquad (1)$

is reduced to the equivalent pair of equations

$4x + 7y = 1$

$-3y = -9$

by multiplying the second equation by 2 and subtracting the result from the first equation. The new second equation gives $y = 3$ and substituting this value for y into the first equation gives the value for $x = -5$. The matrix formulation of this process is known as reduction to triangular form. Again a pair of polynomial equations:

$x - y^2 + 1 = 0$

$x^2 - y^2 + 2 = 0 \qquad (2)$

may be reduced to the equivalent pair

$x - y^2 + 2 = 0$

$y^4 - 5y^2 + 3 = 0.$

This is a triangular form in the sense that the second equation involves only one variable. The four values of y obtained from the second equations may be substituted into the first to obtain the corresponding values of x. In this example, the reduction may be accomplished by successively multiplying the first equation by x, y^2 and -1 and subtracting the results from the second equation. This process may be viewed as a form of long division. We know the long division algorithm for numbers and for polynomials of a single variable. The process of division of $2x^2 - 3x + 4$ by $x - 2$ consists of multiplying the divisor by the appropriate monomial to eliminate the leading term of the dividend, subtracting, and repeating the process. We observe that this is happening above in both the examples, the important point is that we need to identify the leading terms.

Notion of Term Orders

For a polynomial $p(x)$ in a single variable, the leading term is the term containing the highest power of x. When more than one variable is involved we need a rule to decide which of two given terms is larger. We use the words *term* and *monomial* interchangeably. In a term such as $-3x^2yz^2$, the coefficient is -3 and the power product is x^2yz^2. Now, what is the leading term of $x^2 - y^2 - 1$? Use the rule that says, given two power products of the form x^ay^b , the larger is the one with the larger exponent a. If the exponent a is same in both the terms, use the exponent b to break the tie. To make the rule apply in all cases, we use zero exponents $y^3 = x^0y^3$. We define the leading term of a polynomial to be the term that contains the largest power product under this rule. (The zero polynomial has no term and hence no leading term.) Now, the elimination process in examples (1) and (2) above may be described as multiply the first equation by a monomial and subtract it from the second equation in order to eliminate the leading term, just as in long division. The rule for choosing leading terms is an example of a *term order.* It might be described as first x, then y. Another term order that can be used is first y, then x. If this ordering is used in the example (2) above, a triangular system is obtained in one step. The second and third arguments to the *solve* and *eliminate* functions give the user some control over the ordering used. The lexicographic, or *lex*, ordering on a set of variables $x_1, x_2, \dots, x_n$ is first x_1, then x_2, then x_3, and so on. Lexicographic orders are used in solving systems of polynomial equations, but other orderings are used for other purposes. Another common ordering is the *degree-lexicographic ordering*, or *deglex* for short. With *deglex*, terms are ordered first by total degree (e.g. x^2y^3z has total degree 6) and ties are broken using lex.

Definition: A term order on $K[x_1, ..., x_n]$ is a total order $\prec$ on a set of all monomials $x^a = {x_1}^{a_1} \dots {x_n}^{a_n}$, which has the following two properties:

(i)It is multiplicative; i.e. $x^a \prec x^b$ implies $x^{a+c} \prec x^{b+c}$, for all $a, b, c \in N^n$.
(ii)The constant monomial is the smallest; i.e. $1 \prec x^a$, for all $a \in N^n - \{0\}$.

An example of term order on $K[x_1, ..., x_n]$ (for $n = 2$), is the *degree lexicographic order* $1 \prec x_1 \prec x_2 \prec x_1 \prec\prec x_1x_2 \prec\prec {x_2}^2 \prec \ldots$ If we fix a term order $\prec$, then every polynomial f has unique initial term $in_\prec(f) = x^a$. This is the largest monomial x^a which occurs with non-zero coefficient in the expansion of f with respect to the term order $\prec$. Given a fix ideal I in $K[x_1, ..., x_n]$ and a term order $\prec$, *Initial ideal* is the ideal generated by initial terms and is denoted as $in_\prec(I) = \{in_\prec(f)|f \in I\}$. A monomial $x^a = {x_1}^{a_1} \ldots {x_n}^{a_n}$ is called *Standard* if it not in the initial ideal $in_\prec(I)$.

Example: For $n = 1$, let $f \in K[x]$ be a polynomial of degree r. Then standard monomials are $1, x, x^2, \ldots, x^{r-1}$.

Remark: Note that standard monomials are a K-vector space for the residue ring $K[x_1, \ldots, x_n]/I$. The image of a polynomial f modulo I may be expressed uniquely as K-linear combination of standard monomials. This expression is the normal form of f. The process of computing the normal form is the division algorithm.

Now suppose $K \subset C$ (Complex numbers) and F is a finite set of polynomials in $K[x_1, \ldots, x_n]$. Then the variety of F is the set of all common complex zeros $= V(F) = \{(z_1, \ldots, z_n) \in C^n | f(z_1, \ldots, z_n) = 0$, for all $f \in F\}$. The variety does not change if we replace F by another set of polynomials G that generates the same ideal in $K[x_1, \ldots, x_n]$. The answer of the question that whether $V(F)$ is empty or not is given by the following fundamental result:

Hilbert Nullstellensatz : The variety $V(F)$ is empty iff $G = \{1\}$.

Remark: Note that the variety $V(I)$ is finite iff set of standard monomials is finite. In fact number of zeros (counted with multiplicity) is equal to the number of standard monomials.

Not every ordering of power products will do for a term ordering. It is crucial that when multiplying polynomials, the leading term of the product is the product of the leading terms of the factors and that constant terms are always last.

Polynomial Rings and Ideals

Consider the polynomial ring $R[x, y]$ in the variables x and y with *real* coefficients. An ideal in a polynomial ring is a sub-collection of polynomials that is not enlarged by multiplying any member of the sub collection by any other polynomial in the ring or by adding two members of the sub collection. An example is the collection

I =$\{f(x, y) \in R[x, y]| f(a, b) = 0\}$, whenever the point (a, b) lies on the unit circle in the xy-plane. Note that if g(x,y) is any polynomial and f is in I, then $g(a, b)f(a, b) = g(a, b).0 = 0$ and so $g(x, y)f(x, y)$ is already in the sub collection. The sub collection I is not enlarged by multiplying a member by any other polynomial in the ring. The sum condition is checked similarly. A particular polynomial in this ideal is $f(x, y) = x^2 + y^2 - 1$. In fact, every polynomial in the ideal is divisible by this polynomial. Let us see how long division can be used to check this claim. Suppose that $q(x, y)$ is in the ideal. Using lex with x first, we can divide g by f and get $g(x, y) = t(x, y)f(x, y) + xh(y) + r(y)$ for some single-variable polynomials h and r and some polynomial $t(x, y)$. Now, if (a, b) is a point on the unit circle, then $(-a, b)$ is also on the unit circle. Since there is such a point with $a \neq 0$, it follows that $h(b) = r(b) = 0$. Since there are an infinite number of such points, the single-variable polynomials f and g have an infinite number of roots. Thus, $h = r = 0$. This ideal has infinite collections of polynomials and we need a finite representation for computational purposes. The Hilbert Basis theorem states that every ideal in a polynomial ring has a finite basis, that is, there exist a finite set of polynomials $f_1, f_2, \ldots, f_r$ such that every polynomial g in the ideal can be written as

$$g = a_1f_1 + a_2f_2 + \ldots + a_rf_r \qquad (3)$$

for some polynomials $a_1, a_2, \ldots, a_r$. For example, the single polynomial $x^2 + y^2 - 1$ is a basis for the ideal of all polynomials that vanish on the unit circle. Any set of polynomials $f_1, f_2, \ldots, f_r$ is a basis for the ideal of all polynomials g defined by equation (3), as the a_i vary arbitrarily in the polynomial ring. Now consider the system of equations (2) above. Let $f_1 = x - y^2 + 1$and $f_2 = x^2 - y^2 + 2$. Let I be the ideal with basis $\{f_1, f_2\}$ in the ring $R[x, y]$. Then every polynomial $q(x, y)$ of I vanishes on the set points at which both f_1 and f_2 vanish. The solutions of the system. The reason the triangular system has exactly the same solutions as the original system is that the polynomials $x - y^2 + 2$ and $y^4 - 5y^2 + 3$ are also a basis of the ideal I. The second system is triangular because
(i) the corresponding polynomials are a Gröbner basis
(ii) a lexicographic ordering has been used.

A Gröbner basis of an ideal is defined to be a basis with the property that the leading term of every polynomial in the ideal is divisible by the leading term of one of the basis polynomials. This condition turns out to be equivalent to the requirement that in equation (3) above, the a_i may be chosen so that none of the leading terms of the products a_if_i is larger than the leading term of g, that is, no larger leading terms are cancelled off in the sum. Well-known Buchberger's algorithm, computes a Gröbner basis with respect to any term order.

Now, return to the question of solving a system of polynomial equations. Suppose that the system has solutions, but only a finite number. We include complex number solutions and allow polynomials with complex coefficients. Rewrite the equations so that the right-hand sides are zero and let I be the ideal in the polynomial ring with basis consisting of the left-hand sides. To simplify notation, suppose that the ring is

$Q[x, y, z]$. Since there are only a finite number of solutions, I must contain a polynomial $p(x)$ that is free of the variable y and z. Then the ideal I must also contain single-variable polynomials $q(y)$ and $r(z)$. To see this, suppose there are, for example, two solutions $(l, 2, 3)$ and $(4, 5, 6)$. Then $p(x, y, z) = p(x) = (x-1)(x-4)$ vanishes on both these points. Does $p(x)$ lie in the ideal I ? The answer is no. A fundamental result Hilbert Nullstellensatz, states that a power of p must lie in I and $p(x)^m$ is a polynomial in one variable. Now we know that I contains single-variable polynomials in each of the variables. It follows that a Gröbner basis of I with respect to lex must also contain at least one single-variable polynomial. Suppose we take lex with z first, then y, then x, then some element of the Gröbner basis must have a leading term dividing $p(x)$ and so have a leading term of the form x^m. But under lex, a polynomial with leading term must be free of y and z. Similarly, one may argue that the basis contains a polynomial $p(x, y)$ that is free of z, and so on, giving a triangular system. In general, it is not obvious whether or not a given set of polynomials forms a Gröbner basis, but there are two special cases :
(i) a single polynomial is always a Gröbner basis of the ideal it generates.
(ii) if the leading power products of each pair of polynomials are coprime to each other, then the set of polynomials is a Gröbner basis.

Polynomials in a single variable are a very special case. Given a set of polynomials in $Q[x]$, a Gröbner basis of the ideal they generate is any greatest common divisor of the set. In particular, any ideal of $Q[x]$ consists of all multiples of a single polynomial. Generally a basis is not a Gröbner basis. Consider the example : let $f = x$ and $g = 1 + y^2$ and let I be generated by f and g. It is easy to see that the set $\{f, g\}$ is a Gröbner basis of I. Now let $f' = xy$. Then the set $\{f', g\}$ is again a basis of I (indeed $f' = yf$ and $f = -yf' + xg$) but $\{f', g\}$ is not a Gröbner basis of I for x in I can not be reduced modulo $\{f', g\}$.

Gröbner bases for an ideal depend upon the term order used and are not even unique for a given term order. But if the condition that no polynomial in the basis has any term divisible by a leading term of one of the other basis polynomials, then the basis is unique (up to constant multiples). Such bases are called *interreduced.* For systems of linear equations, Gröbner bases correspond to equivalent triangular systems and the interreduced Gröbner bases - assuming that the leading coefficients are normalized to 1 -correspond to what is generally called the *Gauss-Jordan form* of the systems. This form is *unique* if the order of the variables is fixed.

Division and Normal Forms

A number a is a root of a polynomial $f(x) \in Q[x]$ if and only if $f(x)$ is divisible by $x - a$. A similar statement holds for polynomials in several variables. The single-variable statement follows by long division. If we divide $p(x)$ by $x - a$ by long division we get a quotient $q(x)$ and a remainder r, a constant. By substituting a for x in the equation $f(x) = q(x)(x - a) + r$. we see that $r = f(a)$ and so $f(a) = 0$ if and only if $f(x)$ is divisible by $x - a$. Now suppose that $f(x, y)$ is a polynomial in $Q[x, y]$ and consider the question of when $f(a, b) = 0$?. Imitating the single-variable case, divide $f(x, y)$ by $x - a$, considering y to be a constant. The result has the form $f(x, y) = q(x, y)(x - a) + r(y)$. Next, divide $r(y)$ by $y - b$, obtaining a quotient $t(y)$ and a constant remainder s. Substituting for $r(y)$ in the expression above for $f(x, y)$ gives $f(x, y) = q(x, y)(x - a) + t(y)(y - b) + s$ and substituting a for x and b for y shows that $f(a, b) = 0$ if and only if $f(x, y)$ lies in the ideal with basis $\{x - a, y - b\}$. There are several things to note about the division process as it applies to polynomials in several variables. If we first divide by $y - b$ and then by $x - a$ the final equation would be of the form $f(x, y) = h(x)(x - a) + g(x, y)(y - b) + s$

The remainder is the same $f(a, b)$ but the 'quotients', the coefficients of $x - a$ and $y - b$ are different. The reason that the remainder is always the same is a peculiar property of the set $\{x - a, y - b\}$. These polynomials are a Gröbner basis of the ideal no matter what term order is used (the leading terms, x and y have no common factors). For the general situation, start with a polynomial p, an ideal I, a term order, and a Gröbner basis $f_1, f_2, ..., f_n$ of I with respect to the term order. Then there is a division algorithm that produces quotients $q_1, q_2, ..., q_n$ and a remainder r such that $p = q_1 f_1 + ... + q_n f_n + r$ and the leading term of r is smaller than any leading term in the ideal I. The remainder r may vary with the term order and the quotients are not unique even for a fixed term order. In Mathematica, by division algorithm remainder may be computed using the AlgebraicRules function, but not the quotients. The AlgebraicRules function takes a set of equations, computes a Gröbner basis of the corresponding polynomial ideal, and returns an algebraic rules object, basis may be read directly from the displayed rules (Change $a \to b$ to $a - b$). The result is the remainder r above. (The term order is lex with the order of the variables determined by the user). As an example, begin with the polynomials $y - 2$ and $x^2 + y^2 - 1$. These polynomials form a Gröbner basis if we take x before y because the leading terms are relatively prime. Note that AlgebraicRules requires equations rather than polynomials. Consider an example:
In[1] = AlgebraicRules $[\{y - 2 = 0, x^2 + y^2 - 1 = 0\}, \{x, y\}]$
Out[1] = $\{y - 2, x^2 - 3\}$

The output shows that the interreduced Gröbner basis is $\{y - 2, x^2 + 3\}$. The remainder produced by the division algorithm is:
In[2] = $x^3 + y^3 /.AR\{y - 2, x^2 - 3\}$
Out[2] = $8 + 3x$

Note that this is not the result produced by the ordinary replacement rules:
In[3] $= x^3 + y^3/.\{y-2, x^2-3\}$
out[3] $= 8 + x^3$

Two polynomials p and q in a polynomial ring are congruent modulo the ideal I if $p-q$ is a polynomial in the ideal I. If we fix a Gröbner basis G of the ideal with respect to some term order, then p and q are congruent modulo I if and only if they have the same remainder under the division algorithm. This remainder is called the *normal form* of a polynomial with respect to the basis G. The normal form of p with respect to an ideal I and the given term order has the smallest leading term among all the polynomials congruent p modulo I. There is an important *geometric meaning* to congruence modulo I in the case that I is the ideal of polynomials vanishing on a set of points V. In this case, two polynomials are congruent modulo I if and only if they define the same function when restricted to V. For example, the ideal of polynomials in $Q[x,y]$ that vanish on the unit circle in the xy-plane is the ideal with basis consisting of the single polynomial x^2+y^2-1. Since there is only one polynomial in this basis, it will be a Gröbner basis of the ideal for any choice of term order. Thus, two polynomials $f(x,y)$ and $g(x,y)$ will have $f(a,b) = g(a,b)$ for every point (a,b) on the unit circle if and only if they have the same remainder when divided by x^2+y^2-1. The normal form computation gives a criterion for deciding whether a given polynomial p belongs to a given ideal, provided we have a Gröbner basis of the ideal. The polynomial belongs to the ideal if and only if its normal form with respect to the Gröbner basis is zero. Note that this does not depend upon using a special type of term order. In particular, *lex* need not be used. This is important because there are term orders that are computationally more efficient than lex. The package *Groebner.m* in Mathematica, contains three functions related to normal forms. They all need a Gröbner basis for one of their arguments. The function *Normal Form* returns the remainder r above. The function *Extended Normal Form* returns r and a set of quotients $q_1, q_2, \ldots, q_n$. The third function *Membership*, returns True when f is a member of the ideal; it is faster than Normal Form. All three accept arbitrary *term order* as arguments. Using the package, we can repeat the computation that was done above using the Algebraic Rules function and find a set of quotients as well.
In[4] $= \{q, r\} =$ ExtendedNormalForm $[\{y-2, x^2+y^2-1\}$, $\{x,y\}$, lex $][x^3+y^3]$
Out[4] $= \{\{4-2x+2y-xy+y^2-1, x\}, 8-3x\}$

The first element of the result is the list of quotients and the second is the remainder:
In[5] $=$ Expand[q.$\{y-2, x^2+y^2-1\}+r]$
Out[5] $= x^3+y^3$

General strategy of the Gröbner bases approach

Given a set F of a polynomials in $K[x_1, \ldots, x_n]$, by Buchberger's algorithm transform F into another set G of polynomials (Gröbner basis) such that F and G generate the same ideal. By certain nice properties of a Gröbner basis G, many problems that are difficult for an arbitrary F become simple for G. To understand Gröbner basis, we need to understand reduction (division) of multivariate polynomials. For a given set F of polynomials and a polynomial g, many reductions are possible. First we fix a term order on $K[x_1, \ldots, x_n]$, The basic idea behind the algorithm is : when we divide f by $f_1, f_2, \ldots, f_s$, we want to cancel terms of f using the leading terms of $f_i's$ (so the new terms which are introduced are smaller than the cancelled terms) and continue this process until it can not be done anymore.

Multivariate Division Algorithm

```
Input: $f, f_1, f_2, \ldots, f_s \in K[x_1, , x_n]$ with $f_i \neq 0, (1 \leq i \leq s)$
Output: $u_1, u_2, \ldots, u_s, r$ such that $f = u_1 f_1 + u_2 f_2 + \ldots + u_s f_s + r$
and $r$ is reduced with respect to $\{f_1, f_2, \ldots, f_s\}$ and
$max(lp(u_1)lp(f_1), \ldots, lp(u_s)lp(f_s), lp(r)) = lp(f)$.
Initialization: $u_1 := 0, u_2 := 0, \ldots, u_s := 0, h := f$
While $h \neq 0$ Do
IF there exists $i$ such that $lp(f_i)$ divides $lp(h)$ THEN
Choose $i$ least such that $lp(f_i)$ divides $lp(h)$
$u_i := u_i + \frac{lt(h)}{lt(f_i)}$
$h := h - (\frac{lt(h)}{lt(f_i)}) f_i$
ELSE
$r := r + lt(h)$
$h := h - lt(h)$
```

Notion of S-Polynomials: Notion of S-polynomials is very important part of Gröbner bases theory but the notion of Gröbner bases is independent of the notion of S-polynomials. Let f, g be non-zero polynomials in $K[x_1, \ldots, x_n]$. Let $L = lcm(lp(f), lp(g))$. Then the polynomial

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

is called the S-polynomial of f and g.

Example: Let $f = 2yx - y, g = 3y^2 - x^2 \in Q[x, y]$, with deglex term order with $y \succ x$. Then $L = y^2 x$ and

$S(f, g) = (\frac{y^2 x}{2yx)})f - (\frac{y^2 x}{3y^2})g = -(1/2)y^2 + (1/3)x^2$

Question : How can we check whether a given set of polynomial G is a Gröbner basis or not ?

Consider any two polynomials f_1 and $f_2 \in G$, form their S-polynomial $u_2 f_1 - u_1 f_2$. Here u_1 and u_2 are monomials of smallest possible degree such that $u_2 f_1 = u_1 f_2$. The S-polynomial $u_2 f_1 - u_1 f_2$ lies in the ideal G. We apply division algorithm with respect to the tentative

Gröbner basis G to $u_2 f_1 - u_1 f_2$. The resulting normal form is a K-linear combination of monomials, none of which is divisible by initial monomials from G. A necessary condition for G to be Gröbner basis is $normalform_G(u_2 f_1 - u_1 f_2) = 0$, for all $f_1,\ f_2 \in G$. Buchbergers Criterion states that this necessary condition for G to be a Gröbner basis is sufficient: A set G of polynomials is a Gröbner basis iff all its S-polynomials have normal form zero. From this criteria, one derives Buchbergers Algorithm for computing the reduced Gröbner basis G from any given input set F. For a subset S of $K[x_1, \ldots, x_n]$, define the leading term ideal of S to be the ideal

$Lt(S) = \{lt(s) | s \in S\}$.

Definition: Gröbner basis is a set of polynomials whose corresponding reduction is unique.

Facts :

(i) For any g and F, there are no infinite chains of reduction steps modulo F starting from g.

(ii) There is an algorithm RF that produces Reduced Form w.r.t. F, for any given polynomial g i.e. $\forall$, g and F, $g \rightarrow_F RF(F, g)F$.

(iii) Given g and F, there may exist h and k, such that $h_F \leftarrow_F g \rightarrow_F k_F$ but $h \neq k$.

Characterization of the Gröbner basis :

Theorem: Let I be a non-zero ideal of $K[x_1, \ldots, x_n]$. Then the following statements are equivalent for a set of non-zero polynomials

$G =: \{g_1, g, \ldots, g_s\} \subset I$.

(i) G is a Gröbner basis for I.

(ii) $f \in I$ iff $f \longrightarrow_+ 0$.

(iii) $f \in I$ iff $f = h_1 g_1 + h_2 g_2 + \ldots + h_s g_s$ with

$lp(f) = max(lp(h_1)lp(g_1), \ldots, lp(h_s)lp(g_s))$

(iv) $Lt(G) = Lt(I)$.

Construction of a Gröbner basis: Given any initial finite basis $F = \{f_1, f_2, ..., f_k\}$ of the ideal I, one can construct a Gröbner basis G starting from it and using the Buchberger's algorithm, which consists of the following steps :

```
Start with $G := F$.
For any pair of polynomials $f_1, f_2 \in G$ :
Compute the $S$-polynomial of $f_1, f_2$
Reduce it to a reduced form $h$ w.r.t. $G$.
If $h = 0$, consider the next pair.
If $h \neq 0$, add $h$ to $G$ and iterate
```

Now we state main result of Gröbner bases theory on which correctness of algorithm is based. Power of the Gröbner bases method lies on this theorem. Proof of this theorem is non-trivial. In the following theorem RF denotes the reduced form.

Theorem (Buchberger): *G is a Gröbner bases iff for every $f_1, f_2 \in G$, $RF[G, S - polynomial[f_1, f_2]] = 0$.*

Mathematica's Gröbner basis function takes a list of polynomials and returns an interreduced Gröbner basis. The term order is always *lex* and the second argument to the function specifies which variable comes first, which is second, and so on. For example, Gröbner basis which is a triangular system. Switching the order of the variables gives a different triangular system: The corresponding function in the package Gröbner.m is called *Grobner* and allows a third argument specifying the term order. Suppose a set of polynomials $f_1, f_2, \ldots, f_n$ is processed by a Gröbner basis algorithm producing $g_1, g_2, \ldots, g_n$. Since the $g_j's$ are in the ideal generated by the f_j, there must be polynomials t_{ij} such that $g_i = \sum t_{ij} f_j$, for each index i.

The t_{ij} are useful in some computations. The package *Gröbner.m* contains a function Extended Gröbner that returns the t_{ij} as well as the g_i.

Parameter Elimination and Projection For the second example, consider the parametric equations

$x = f(t) = t(t-1)(t-2)$

$y = g(t) = (t-1)(t-2)(t-3)$.

These are parametric equations for a curve in the plane. To obtain an equation for this curve in the form $p(x, y) = 0$, we need to eliminate the parameter t. Now the plane curve $(f(t), g(t))$ is the projection of the space curve $(f(t), g(t), t)$ on the xy-plane. The ideal of $Q[x, y, t]$ with basis $\{b_1 = x - f(t), b_2 = y - g(t)\}$ consists of the polynomials that vanish on the space curve. (The verification is similar to the argument above involving the unit circle). Take *lex* with x first, then y, then t. Now, given an arbitrary polynomial $p(x, y, z)$, divide first by $x - f(t)$ and divide the remainder by $y - g(t)$. Then we get an equation

$h(x, y, z) = h_1(x, y, t)(x - f(t)) + h_2(y, t)(y - g(t)) + h_3(t)$.

Now, if this ideal contains a polynomial of the form $p(x, y)$, then, because the variable t is missing, $p(x, y)$ must vanish on the entire surface consisting of all the vertical lines in xyt-space that intersect the projection of the space curve on the xy-plane. Thus, $p(x, y)$, considered as polynomial in $Q[x, y]$ must vanish on the plane curve. To find a polynomial of the form $p(x, y)$ in the ideal with basis $\{b_1, b_2\}$, choose a lex ordering with t first and compute a Gröbner basis of the ideal. If the ideal contains polynomials of the form $p(x, y)$, then so does the Gröbner basis. This is because with t first, any polynomial containing t must have t in its leading term and so this leading term can divide leading terms only of other polynomials containing t. But the leading term of some Gröbner basis element must divide the leading term of every polynomial in the ideal. The computation is

In [6]= GröbnerBasis $[\{x - t(t-1)(t-2), y - (t-1)(t-2)(t-3)\}, \{t, x, y\}]$;

Out [6]= $\{-6x^2 + x^3 15xy - 3x^2y - 6y^2 + 3xy^2y^3, 6x - x^2 - 6y + 9ty$ $+2xyy^2, -21x + 9tx - x^2 - 6y + 2xy - y^2, 69t + 3t^2 - x + y\}$.

The first polynomial of this output provides an equation for the curve. This is the Gröbner basis approach to elimination theory. The computation of geometric projections can be somewhat subtle (see [7]). Although the lex ordering works for elimination problems, it is not the most efficient. All that is needed in the example above is an ordering that puts t first. Ties could be broken by, for example, using *deglex* in x and y. Such orderings are generally more efficient than lex. Mathematica function *Eliminate* uses more efficient orderings internally([1], [2]).

Applications

Buchberger Algorithm for Gröbner basis furnishes the engine for computations in commutative and non-commutative algebra, algebraic geometry for example computing cohomology, resolving singularities etc. Gröbner basis is being used by researchers in coding theory, robotics, statistics, and control theory. Softwares based on the Gröbner bases technique are Singular, CoCoA, Macaulay2. Software Maple and Mathematica are also very useful for computations of Gröbner basis.

An Example From Robotics

The study of the inverse kinematics of the ROMIN manipulator ([10]) shall be used to give an idea how helpful Gröbner bases are for this kind of work. The system of equations is as follows:

$-sin\theta_1(l_1cos\theta_2 + l_2cos\theta_3) - x = 0$

$cos\theta_1(l_1cos\theta_2 + l_2cos\theta_3) - y = 0$

$l_1sin(\theta_2) + l_2sin\theta_3 - z = 0$

where l_1 and l_2 denote the length of the first and second arm of the robot and $\theta_1, \theta_2, \theta_3$ represent rotation angles around the base and the robot arms. With these equations, the angles should be computed given a position (x, y, z) of the tip of the robot. Actually we are satisfied if we can find the cosines or sines of these angles. There are two ways of converting the equations into polynomial form.

A rational parameterization of trigonometric functions is used:

$cos\theta_i = \frac{1-t_i{}^2}{1+t_i{}^2}$, $sin\theta_i = \frac{2t_i}{1+t_i{}^2}$, for $i = 1, 2, 3$.

When we use these rational expressions make sure that we multiply the equations with products of $(1 + t_1{}^2), (1 + t_2{}^2)$, and $(1 + t_3{}^2)$ so that polynomial equations arise. In our case, we get three polynomials in $l_1, l_2, x, y, z, t_1, t_2, t_3$ from which we could solve t_1, t_2 and t_3, and by computing the decomposed Gröbner basis with respect to lexicographic ordering $x \succ y \succ z \succ t_3 \succ t_2 \succ t_1$. Drawback of this method is that joint angles of 180 degrees are not possible in this parameterization and joint angles close to 180 degrees give awkwardly large numerical values.

The cosines and sines are considered as variables and trigonometric relations are added in the format of polynomial equations. For the ROMIN manipulator we get:

$-s_1(l_1c_2 + l_2c_3) - x = 0$

$c_1(l_1c_2 + l_2c_3) - y = 0$
$(l_1c_2 + l_2c_3) - z = 0$
${c_1}^2 + {s_1}^2 - 1 = 0$
${c_2}^2 + {s_2}^2 - 1 = 0$
${c_3}^2 + {s_3}^2 - 1 = 0$

where $s_i = sin\theta_i$, $c_i = cos\theta_i$, for $i = 1, 2, 3$. The set of defining polynomials can now be converted into a Gröbner basis with respect to the pure lexicographic ordering $s_1 \succ c_1 \succ s_2 \succ c_2 \succ s_3 \succ c_3$. We consider l_1, l_2, x, y, z as parameters .

polys $:= [-s[1] * (l[1] * c[2] + l[2] * c[3]) - x,$
$c[1] * (l[1] * c[2] + l[2] * c[3]) - y,$
$l[1] * s[2] + l[2] * s[3] - z,$
$c[1]^2 + s[1]^2 - 1, c[2]^2 + s[2]^2 - 1$
$c[3]^2 + s[3]^2 - 1];$

polys $:[-s_1(l_1c_2+l_2c_3)-x$, $c_1(l_1c_2+l_2c_3)-y$, $(l_1c_2+l_2c_3)-z$, ${c_1}^2+{s_1}^2-1$, ${c_2}^2 + {s_2}^2 - 1$, ${c_3}^2 + {s_3}^2 - 1]$

gbasis(polys, $[c[3], s[3], c[2], s[2], c[1], s[1]], plex)$;

$[2l_2xc_3 + 2zl_1s_2s_1 + (x^2 + y^2 + {l_2}^2 - z^2 - {l_1}^2)s_1, l_1s_2 + l_2s_3 - z, -2zl_1s_2s_1 + 2l_1xc_2 + (-{l_2}^2 + z^2 + x^2 + y^2 + {l_1}^2)s_1, (4{l_1}^2 + 4{l_1}^2y^2 + 4{l_1}^2z^2){s_2}^2 - 2{l_1}^2x^2 - 2{l_1}^2y^2 + {l_1}^4 + {l_2}^4 + z^4 - 2{l_2}^2y^2 + 2z^2y^2 + x^4 + y^4 - 2x^2{l_2}^2 + x^2z^2 + 2x^2y^2 + 2{l_1}^2z^2 - 2{l_2}^2z^2 - 2{l_2}^2{l_1}^2 + (4l_1z{l_2}^2 - 4l_1z^3 - 4zl_1x^2 - 4zl_1y^2 - 4z{l_1}^3)s_2, ys_1 + xc_1, -x^2 + (x^2 + y^2){s_1}^2]$

The Gröbner basis is in triangular form. So, in principle the inverse kinematics problem is solved. However, the key problem is whether for numerical values of the parameters the above basis stays a Gröbner basis. If so, everything is OK. In the example we are considering, if we choose $l_1 \neq 0, l_2 \neq 0, x^2 + y^2 \neq 0$, then the above set is still a Gröbner basis. This specialization problem can be avoided by using so-called comprehensive Gröbner bases ([11]).

Counting of Finite Solutions

Suppose that the system of polynomial equations has a finite number of solutions. The number of solutions (counted with multiplicities and solutions at infinity) is equal to the cardinality of the set of monomials that are no multiples of the leading monomials of the polynomials in the Gröbner basis (any term ordering may be chosen). We apply this criterion on the previous example, with considered as a parameter. First we compute the leading monomials in the Gröbner basis with respect to the total degree inverse lexicographic ordering for which

polys $:= [c * x + x * y^2 + x * z^2 - 1, c * y + y * x^2 + y * z^2 - 1,$
$c * z + z * x^2 + z * y^2 - 1]$:
gbasis $(polys, [x, y, z], tdeg)$:
map$(f \mapsto op(2, leadmon(f, [x, y, z], plex)),$");
$[x, y^2, yz^7, z^{14}]$

So, the set of monomials that are no multiples of these leading monomials equals $\{1, z, \ldots, z^{13}, y, yz, \ldots, yz^6\}$ and has cardinality 21. So, according to the above criterion there are 21 finite solutions. If we would use the *solve* command in Maple to find all solutions of this system of polynomial equations we could easily verify that this is indeed the correct number of solutions.

Invertibility of Polynomial Mappings

The Jacobian conjecture states that a polynomial mapping has an inverse which is itself a polynomial mapping if and only if the determinant of the Jacobian of the mapping is nonzero. In an attempt of proving the conjecture the following criterion of invertibility has been found ([13]): Let $f_1, f_2, \ldots, f_n$ be the coordinate functions of a polynomial mapping in the variables $x_1, x_2, \ldots, x_n$. Let $y_1, y_2, \ldots, y_n$ be new indeterminates and let $\succ$ be an admissible ordering such that $y_1 \succ y_2 \ldots \succ y_n \succ x_1 \succ x_2 \ldots \succ x_n$. Then the mapping is invertible if and only if the Gröbnerbasis of $y_1 - f_1, y_2 - f_2, \ldots, y_n - f_n$ has the form $x_1 - g_1, x_2 - g_2, \ldots, x_n - g_n$, where $g_1, g_2, \ldots, g_n$ are the coordinate functions of the inverse mapping. Consider the example (See [13]):

$(x, y, z) \longmapsto (x^4 + 2(y + z)x^3 + (y + z)^2x^2 + (y + 1)x + y^2 + yz, x^3 + (y + z)x^2 + y, x + y + z)$

$F := [x^4 + 2 * (y + z) * x^3 + (y + z)^2 * x^2 + (y + 1) * x + y^2 + y * z, x^3 + (y + z) * x^2 + y, x + y + z]$

$F := [x^4 + 2 * (y + z) * x^3 + (y + z)^2 * x^2 + (y + 1) * x + y^2 + y * z, x^3 + (y + z) * x^2 + y, x + y + z];$

$gbasis([X - F[1], Y - F[2], Z - F[3]], [x, y, z, X, Y, Z], plex);$

$[x - X + ZY, y + ZX^2 - Y + Z^3Y^2 - 2Z^2YX, Y - ZY - Z^3Y^2 + 2Z^2YX + X - ZX^2 - Z + z]$

So, the mapping has inverse $(X, Y, Z) \longmapsto (X - ZY, -ZX^2 + Y - Z^3Y^2 + 2Z^2YX, -Y + ZY + Z^3Y^2 - 2Z^2YX - X + ZX^2 + Z)$

It turns out that verification of the result by composition of mappings takes more time then the Gröbner basis computation of the inverse mapping.

Acknowledgment

This work has been conducted during the special semester on Gröbner bases, February 1 to July 31, 2006 organized by Johann Radon Institute for Computational and Applied Mathematics(RICAM), Austrian Academy of Sciences, and RISC, Johannes Kepler University, Linz, Austria. The author thanks Professor Bruno Buchberger for the invitation and RICAM for the hospitality and excellent research facilities.

References

[1] Adams W., and P. Loustaunau : An introduction to Gröbner bases, *Providence: American Mathematical Society*, 1994.

[2] Becker Thomas, and Volker Weispfenning: Gröbner bases: A computational approach to commutative algebra, New York, *Springer-Verlag*, 1993.

[3] Buchberger B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Ph.D. thesis, University of Innsbruck, Austria, 1965(in English Journal of Symbolic Computation, 2005).

[4] Buchberger B.: ÖEin algorithmisches Kriterium fr die Lsbarkeit eines algebraischen Gleichungssystems, *Aequationes Mathematicae*, Vol. 4, Fasc. 3, 1970.

[5] Buchberger B.: Gröbner bases: An algorithmic method in polynomial ideal theory, N.K. Bose (Editor): In Recent trends in multidimensional systems theory, Pages 14-232, Dordrecht: D. Reidel , 1985.

[6] Buchberger B. : Gröbner Bases: A Short Introduction to for System Theorists, *Proceedings of EUROCAST* 2001.

[7] Cox David, John Little, and Donal O'Shea : Ideals, varieties, and algorithms, New York, Springer Verlag, 1992.

[8] Helzer, Garry : Gröbner Bases, Mathematica Journal, Miller Freeman Publication, 1995.

[9] Bernd Sturmfels : What is a Gröbner basis, *Notices AMS*, Vol. 52, Number 10.

[10] M. J. GonzÄ, lez-LÄpez and T. Recio: The ROMIN inverse geometric model and the dynamic evaluation method, A.M. Cohen, editor, Computer Algebra for Industry: Problem Solving in Practice, pages 117-141. John Wiley and Sons, 1993.

[11] V. Weispfenning : Comprehensive Gröbner Bases, *J. Symbolic Computation*, 14(1): pages 1-29, 1993.

[12] A. V. D. Essen : Polynomial Maps and the Jacobian Conjecture, *Computational Aspects of Lie Groups and Related Topics*, A. M. Cohen, Editor, CWI Tract 84, pages 29-44, 1991.

[13] A. J. P. Heck : Introduction to Maple, 2nd edition, *Springer Verlag*, 1996.