ELEMENTARY GRÖBNER BASIS THEORY

Jeffrey Clark

Introduction. Most of us have a sense as to how to solve a polynomial equation in one variable: factoring, rational roots, Newton's method, bisection, etc. However, when it comes to polynomial equations in several variables, unless there is an immediate way to solve and substitute or to cancel terms, we get stuck.

This paper is about one such method, Gröbner bases. A Gröbner basis is a particular system of polynomials, found from a given set of polynomials, that can be used to describe all equations that are derivable from the original system.

Order. We will be working with long division with multivariable polynomials. With one variable, it is clear what we mean by quotient and remainder: if we divide x^3+1 by x^2+1, we have $x^3+1=(x^2+1)(x)+(-x+1)$, where the quotient is x and the remainder $-x+1$ is required to be "smaller" than x^2+1, in the sense that its degree is smaller than that of x^2+1.

What if we have two variables x and y? What does it mean to divide x^3+y^3 by x^2+y^2? Do we want $x^3+y^3=(x^2+y^2)(x)+(-xy^2+y^3)$ or $x^3+y^3=(x^2+y^2)(y)+(x^3-x^2y)$?

The key is deciding how we want the remainder to be "smaller" than the divisor. This implies some sort of ordering of the polynomials. We will start by ordering the terms, so that each polynomial will have a leading term. We can then define $p<q$ to mean that the leading coefficient of $q-p$ is positive.

Ordering the terms comes down to ordering the monomials $x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}$; once we have done so, then we can worry as to whether or not the coefficient of the term is positive or negative.

Since we are dealing with polynomials, we need an order that respects not only addition but also multiplication. Therefore, we define a *monomial ordering* on the monomials to be a well-ordering $<$ such that if m_1, m_2, and m_3 are any monomials, $m_1<m_2$ implies that $m_1m_3<m_2m_3$.

One of the simplest monomial orderings is lexicographic:
$x_1^{e_1}\cdots x_n^{e_n}>x_1^{f_1}\cdots x_n^{f_n}$ if and only if there is a j between 1 and n such that $e_i=f_i$ for $i<j$ and $e_j>f_j$. This ordering is completely determined by how we order the variables themselves.

Once we have a monomial order defined, we have a well-ordering on the set of polynomials. In performing long division, we will always require that the remainder be smaller than the divisor in the sense of this order. Thus, if we use a lexicographic ordering on our variables with $x>y$, we have that $x^3+y^3=(x^2+y^2)(x)+(-xy^2+y^3)$. The remainder $-xy^2+y^3$ is smaller than our divisor x^2+y^2 since the leading term of $-xy^2+y^3-(x^2+y^2)$ is $-x^2$, and the leading coefficient is negative.

Rewriting. We can think of going from a polynomial to its remainder as a form of rewriting. For example, if we know that $x^2 + 1 = 0$, then on the one hand we can take any polynomial $p(x) = (x^2 + 1)q(x) + r(x) = r(x)$ and reduce it to a remainder of degree less than 2. On the other hand we can replace the leading term x^2 everywhere that it appears in $p(x)$ by -1. We will write this substitution as a rewriting rule $x^2 \to -1$; we will also use an arrow wherever we employ it, i.e., $p(x) \to r(x)$. For example $x^3 \to -x$.

In the area of solving systems of polynomial equations, we would like to be able to use one equation to simplify another in this fashion. The process of applying rewriting rules to polynomials is known as reduction since we are replacing the leading term by a combination of smaller terms.

In this setting, we would like to reduce a given equation by all of the other equations, and therein lies the rub. It is possible that reducing a polynomial by different equations will yield different results.

For example, suppose we know that $x^2 - y = 0$ and that $xy - y^3 = 0$, where we order the terms lexicographically with $x > y$. Then how can we use these equations to reduce x^2y? If we divide out by the first polynomial, we have $x^2y = (x^2 - y)(y) + y^2$, which we can write as $x^2y \to y^2$. If we divide out by the second polynomial we have $x^2y = (xy - y^3)(x + y^2) + y^5$, which we can write as $x^2y \to y^5$. Note that the results y^2 and y^5 differ and themselves can not be reduced any further.

This problem will only occur when we try and reduce a term that is divisible by both of the leading terms of our two rewriting rules.

Therefore, if we want to make sure that reduction by a set of polynomials leads to consistent results, we will need to make sure that the result of applying two rules to any common multiples of their leading terms will yield the same result.

For every pair of polynomials p and q we define their *syzygy* to be

$$S(p, q) = (\text{lcm } (p_L, q_L)/p_L)p - (\text{lcm } (p_L, q_L)/q_L)q,$$

where p_L and q_L are the respective leading terms. (The difference will always result in the leading terms of the products canceling out.) The syzygy measures how far apart is the reduction of lcm (p_L, q_L) by p or q. If we now set the syzygy to 0, we force the results of reductions by p and by q to be equal.

For example, $S(x^2 - y, xy - y^3) = (x^2y/x^2)(x^2 - y) - (x^2y/xy)(xy - y^3) = xy^3 - y^2$, which can be reduced to $y^5 - y^2$ by $xy \to y^3$.

Algorithm. When we look at all the possible combinations of a given set of polynomials, we are looking at an *ideal* generated by them. (In an arbitrary ring, an ideal is a subset that is closed under addition, subtraction, and scalar multiplication.)

A reduced Gröbner basis for a given polynomial ideal is a set of polynomials that will always produce the same result when applied as rewriting rules to any

polynomial. It is used in an analogous fashion to an orthonormal basis for a vector space: it can easily and unambiguously be used to reduce a polynomial.

By the above, one of the problems in constructing such a basis lies in making sure that all syzygies are accounted for.

The following algorithm, due to Buchberger, will take a set of polynomials and produce a reduced Gröbner basis for the ideal that they generate.

1. Let G be the set of polynomials, with a monomial ordering on them.
2. Let B be the reduced Gröbner basis. Start with $B = \{\}$.
3. While G is nonempty, let g be an element, and remove it from G.
4. Reduce g by all of the elements of B.
5. If $g = 0$, return to Step 3.
6. Otherwise, see if any of the elements b of B can be reduced by g. If so, remove b from B and add it to G if it is nonzero.
7. Add $S(g, b)$ to G for all of the remaining elements of B.
8. Add g to B.
9. Return to 3.

It can be shown that this algorithm will always terminate in a finite number of steps. At any point we may remove any constant factors.

For example, let $x > y$ be a lexicographic ordering on polynomials in those three variables. We will find a Gröbner basis for the polynomials $x^3 - 2$ and $x^2 - y$. The leading term will always be written at the front of the polynomial.

1. We start with $B = \{\}$ and $G = \{x^3 - 2, x^2 - y\}$. Take $g = x^3 - 2$ from G. Since B is empty, it cannot be reduced any further by division by elements of B, and likewise none of the elements of B can be reduced. There are no syzygies to compute, and we add g to B.
2. $B = \{x^3 - 2\}$ and $G = \{x^2 - y\}$. Take $g = x^2 - y$ from G. It cannot be reduced by the only element of B, but it can be used to reduce $x^3 - 2$ to $xy - 2$, which we add to G. There are now no syzygies to compute with g since B is empty. We add g to B.
3. $B = \{x^2 - y\}$ and $G = \{xy - 2\}$. Take $g = xy - 2$ from G. It cannot be reduced by the only element of B, nor can it reduce that element. We add the syzygy $S(xy - 2, x^2 - y) = -2x + y^2$ to G and g to B.
4. $B = \{x^2 - y, xy - 2\}$ and $G = \{-2x + y^2\}$. Take $g = -2x + y^2$ from G. Both elements of B can be reduced as follows: $x^2 - y \to y^4/4 - y$, $xy - 2 \to y^3/2 - 2$. We add $y^4 - 4y$ and $y^3 - 4$ to G. There are no syzygies to compute, so we add g to B.
5. $B = \{-2x + y^2\}$ and $G = \{y^4 - 4y, y^3 - 4\}$. Take $g = y^4 - 4y$ from G. It cannot be reduced by the only element of B, nor can g reduce that element.

We compute the syzygy $S(y^4 - 4y, -2x + y^2) = 8xy - y^6$ and add it to G, and we add g to B.

6. $B = \{-2x + y^2, y^4 - 4y\}$ and $G = \{y^3 - 4, 8xy - y^6\}$. Take $g = y^3 - 4$ from G. It cannot be reduced by the elements of B but it reduces $y^4 - 4y$ to 0. We compute the syzygy $S(y^3 - 4, -2x + y^2) = 8x - y^5$ and add it to G, and we add g to B.
7. $B = \{-2x+y^2, y^3-4\}$ and $G = \{8xy-y^6, 8x-y^5\}$. Both of the elements of G reduce to 0, and we are done: the reduced Gröbner basis is $\{-2x+y^2, y^3-4\}$.

This process is almost always too lengthy to be done by hand; fortunately both *Maple* and *Mathematica* have commands for it. In *Maple* the command is `groebner[gbasis],` and in *Mathematica* it is `GroebnerBasis[listofpolys,variableorder].`

Solving a System of Polynomial Equations. If it is possible to eliminate a variable from a system of polynomial equations, then a properly chosen Gröbner basis for that system will contain a polynomial free of that variable.

The same is true for eliminating several variables, so if it is possible to solve a system for a finite number of solutions, then it is possible to find a Gröbner basis for the system that eliminates all but one of the variables. The roots of that univariate polynomial can be substituted back in to recursively solve for the values of the other variables.

Suppose we start with the following system of equations:

$$x^3 + xy + y^3 = 4$$

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

If we use these equations to generate a Gröbner basis with a lexicographic order, then if it is possible to combine these equations to eliminate a variable, it will show up as the smallest generator in the basis. The smaller of the two variables will be the one eliminated.

Using *Mathematica,* we write the equations as polynomials in a list, and the lexicographic order as a second list of variables.

With $x > y$:

$$\text{In[1]} := \text{GroebnerBasis}[\{x^3 + x * y + y^3 - 4,\ x * y^2 + x^3 - y^4 - 5\},\ \{x,\ y\}]$$

$$\begin{aligned}\text{Out[1]} = \{&-1 - 8y^3 + 11y^4 - 13y^5 + y^6 - 8y^7 + y^8 - 3y^9 - 3y^{10} - 3y^{11} \\ &- y^{12},\ -8 - 9x - 8y + 55y^2 - 117y^3 + 88y^4 - 25y^5 + 55y^6 \\ &- 18y^7 + 17y^8 + 20y^9 + 23y^{10} + 8y^{11}\}.\end{aligned}$$

The first generator is a twelfth-degree polynomial in a single variable. Generally such an equation will not be solvable in terms of radicals, etc., but the system can then be "solved" in terms of the root.

Eliminating a Parameter. If we are given polynomial or even rational parametric equations, we can use them to solve for a Gröbner basis that contains at least one generator that does not contain the parameter(s), i.e., an implicit equation connecting other variables.

Let $x = t/(t^2 - 1)$ and $y = t^2/(t^3 + 1)$. We will try to eliminate t and produce an equation connecting x and y.

As written, x and y are not polynomial functions, but we can introduce two auxiliary variables u and v to be the reciprocals of the denominators:

$$x - tu = 0$$

$$y - t^2 v = 0$$

$$u(t^2 - 1) - 1 = 0$$

$$v(t^3 + 1) - 1 = 0.$$

If we order the variables $u > v > t > x > y$, then the least polynomial in the Gröbner basis will eliminate u, v, and t if at all possible.

Using *Mathematica* on this system, we find that one of the generators is our answer:

$$x^3 - xy - x^2 y - 2x^3 y + y^2 + 3x^2 y^2 = 0.$$

Conclusion. Gröbner bases are a very powerful tool for working with multivariable polynomials. I have only touched on some of the more elementary uses in this paper; there are far deeper results involving algebraic geometry.

The algorithm itself is intuitive but the computation itself is usually beyond the scope of paper and pencil. Fortunately the algorithm is available in the most popular Computer Algebra Systems on the market.

References

1. F. Baader and T. Nipkow, *Term Rewriting and All That,* Cambridge University Press, Cambridge, MA, 1998.
2. T. Becker and V. Weispfenning, *Gröbner Bases,* Springer-Verlag, New York, NY, 1993.
3. D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms,* Springer-Verlag, New York, NY, 1992.
4. D. Cox, J. Little, and D. O'Shea, *Using Algebraic Geometry,* Springer-Verlag, New York, NY, 1998.
5. J. H. Davenport, Y. Siret, and E. Tournier, *Computer Algebra,* Academic Press, San Diego, CA, 1988.
6. D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry,* Springer-Verlag, New York, NY, 1995.

Jeffrey Clark
Department of Mathematics
2122 Campus Box
Elon University
Elon, NC 27244
email: clarkj@elon.edu