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.