

PROJECTIONS AND GRÖBNER BASES

Greg Henry

Mississippi State University

email: glh1@ra.msstate.edu

Faculty advisor: Vivien G. Miller

Department of Mathematics and Statistics, Mississippi State University,
Drawer MA, Mississippi State, MS, 39762.

email: vivien@math.msstate.edu

ABSTRACT. We consider the system of equations $f_1(x_1, \dots, x_n) = 0, \dots, f_m(x_1, \dots, x_n) = 0$ where f_1, \dots, f_m are polynomials. We discuss an ordering of these polynomials and define the Gröbner basis of an ideal. These ideas are applied to a system of equations corresponding to the projection of a three dimensional surface onto a plane.

Introduction. Systems of equations are ubiquitous, and the development of efficient methods for solution is a goal that has influenced computational as well as "pure" mathematics. As a particularly successful example, we mention the problem of finding solutions of systems of linear equations. The theory of linear algebra is rooted in this problem and computational methods of solution have been optimized. Using Gaussian elimination, the system

$$\begin{cases} 3x - 6y - 2z = 0 \\ 2x - 4y = 0 \\ x - 2y - z = 0 \end{cases}$$

is equivalent to

$$\begin{cases} x - 2y = 0 \\ z = 0 \end{cases}$$

One interpretation of this is that the span of the functions $f_1 = 3x - 6y - 2z, f_2 = 2x - 4y,$ and $f_3 = x - 2y - z$ is equal to the span of $g_1 = x - 2y$ and $g_2 = z$ and the zero-set of $\{g_1, g_2\}$ is easily determined.

In this paper, we consider solutions of systems of polynomials in several variables. While searching for analogies to the linear span of functions, we are led to rings of polynomials, and the variety of an ideal of polynomials. Analogous to Gaussian elimination is Buchberger's algorithm for the construction of a Gröbner basis for an ideal of polynomials, that is, a simple set of polynomials $\{g_1, \dots, g_m\}$ that generate the same zero-set as a given collection $\{f_1, \dots, f_n\}$.

Ideals of polynomials. Let k be a field such as the rationals or the reals, then $k[x_1, \dots, x_n]$ will represent the set of all polynomials in n variables with coefficients in k . Thus $k[x_1, \dots, x_n]$ consists of sums of terms of the form $ax_1^{\beta_1}x_2^{\beta_2}\dots, x_n^{\beta_n}$ where $a \in k$ and $\beta_1, \beta_2, \dots, \beta_n \in \mathbb{N}_0 = \{0, 1, 2, \dots\}$. It is easy to see the $k[x_1, \dots, x_n]$ is a commutative ring under polynomial addition and multiplication. (For an introduction to ring theory, see [3])

Let $f_1, \dots, f_m \in k[x_1, \dots, x_n]$. The variety defined by f is denoted $V(f_1, \dots, f_m)$ and it is the set of solutions of the system of equations $f_1 = 0, f_2 = 0, \dots, f_m = 0$. Thus in the example above we are looking for $V(f_1, f_2, f_3)$ where $f_1 = 3x - 6y - 2z, f_2 = 2x - 4y,$ and $f_3 = x - 2y - z$. If we let $f_4 = z$ and $f_5 = x - 2y$ clearly, $V(f_1, f_2, f_3) = V(f_4, f_5)$ and of course, $V(f_4, f_5)$ is much easier to find.

The ideal generated by f_1, \dots, f_m denoted $\langle f_1, \dots, f_m \rangle$ is

$$\langle f_1, \dots, f_m \rangle := \left\{ \sum_{i=1}^m u_i f_i : u_i \in k[x_1, \dots, x_n] \text{ for } i = 1, \dots, m \right\}.$$

If we let $I = \langle f_1, \dots, f_m \rangle$ we see that I is clearly an ideal, since $f + g \in I$ for all $f, g \in I$ and $h \cdot f \in I$ for all $h \in k[x_1, \dots, x_n]$. The set f_1, \dots, f_m is called the generating set of the ideal I . Many sets can generate the same ideal, but some sets are easier to work with than others. As an example, let us consider $k[x]$, the set of all polynomials in one variable. Suppose $\{f_1, \dots, f_m\} \in k[x]$. A greatest common divisor of $\{f_1, \dots, f_m\}$, denoted $GCD(f_1, \dots, f_m)$, is a polynomial h such that h divides f_1, f_2, \dots, f_m and if p is another polynomial that divides f_1, \dots, f_m , then p divides h . The $GCD(f_1, \dots, f_m)$ is unique up to a constant multiple. If we let g be the $GCD(f_1, \dots, f_m)$ with leading coefficient 1, then g is a generator of the ideal $\langle f_1, \dots, f_m \rangle$ and is the reduced Gröbner basis of $\langle f_1, \dots, f_m \rangle$. We will define a Gröbner basis in the next section. For example, the $GCD(x^3 - 3x + 2, x^4 - 1, x^6 - 1) = x - 1$. This is obtained by polynomial division as seen below.

$$\begin{aligned} x^6 - 1 &= x^2(x^4 - 1) + (x^2 - 1) \\ x^4 - 1 &= (x^2 + 1)(x^2 - 1) + 0 \end{aligned}$$

Thus $GCD(x^4 - 1, x^6 - 1) = x^2 - 1$. Since

$$\begin{aligned} x^3 - 3x + 2 &= x(x^2 - 1) + (-2x + 2) \\ x^2 - 1 &= (-2x + 2)\left(-\frac{x}{2} - \frac{1}{2}\right) + 0 \end{aligned}$$

the $GCD(x^3 - 3x + 2, x^4 - 1, x^6 - 1) = x - 1$. Thus solutions of

$$\begin{cases} x^3 - 3x + 2 = 0 \\ x^4 - 1 = 0 \\ x^6 - 1 = 0 \end{cases}$$

are the same as solutions of $x - 1 = 0$ which is just $x = 1$.

Gröbner Basis. Now suppose $f_1, f_2, \dots, f_m \in k[x_1, x_2, \dots, x_n]$. How do we go about determining a Gröbner basis? First we have to put an ordering on the monomials that make up the polynomials. There are several different orderings that one can use, but for the purposes of this paper we will use the lexicographical ordering. This is also the ordering that is used in most computer algebra systems. Let $M_n = \{x_1^{\beta_1}, x_2^{\beta_2} \cdots, x_n^{\beta_n} \mid \beta_1, \beta_2, \dots, \beta_n \in \mathbb{N}_0\}$. We define the lexicographical order on M_n with respect to $x_1 > x_2 > \cdots > x_n$ as follows: For $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}_0^n$

and $x = (x_1, \dots, x_n)$, we define $x^\alpha < x^\beta$ if and only if the first coordinates α_i and β_i in α and β from the left which are different satisfy $\alpha_i < \beta_i$. For example, the lexicographical order on $k[x, y, z]$ with respect to $x > y > z$ is $1 < z < z^2 < \dots < y < yz < yz^2 \dots < y^2 < y^2z < y^2z^2 \dots < x < xz < xz^2 < \dots < xy < xyz < xyz^2 < \dots < xy^2 < xy^2z < xy^2z^2 < x^2 < x^2z < x^2z^2 < \dots$. Under the lexicographical ordering each $f \in k[x_1, \dots, x_n]$ has a unique leading term denoted $LT(f)$. Using the lexicographical order with respect to $x > y > z$ mentioned above the leading term of $4xy^2 + 4z^2 - 5x^3 + 7x^2z^2$ is $-5x^3$.

Suppose $0 \neq I$ is an ideal in $k[x_1, \dots, x_n]$ with some given monomial ordering. We denote by $LT(I)$ the set of leading terms of the elements of I , and by $\langle LT(I) \rangle$ the ideal generated by $LT(I)$. It's natural to ask whether the leading terms of a generating set for I generates $LT(I)$; that is, does $LT(I) = \langle LT(f_1), \dots, LT(f_n) \rangle$ whenever $I = \langle f_1, \dots, f_n \rangle$? The answer is generally not, as the following example shows. Give $k[x, y]$ the lexicographical order with respect to $x > y$, and consider the ideal $I = \langle f_1, f_2 \rangle$ where $f_1 = x^3 - 2xy$ and $f_2 = x^2y + x - 2y^2$. Since $x^2 = x(yx^2 - 2y^2 + x) - y(x^3 - 2xy)$ we see that $x^2 \in I$. Thus $x^2 = LT(x^2) \in \langle LT(I) \rangle$. However, x^2 is not divisible by $LT(f_1) = x^3$ or $LT(f_2) = x^2y$. Thus $x^2 \notin \langle LT(f_1), LT(f_2) \rangle$ and so $LT(I) \neq \langle LT(f_1), LT(f_2) \rangle$. If however for some generating set G of I equality obtains, then G is said to be a Gröbner basis for I .

Definition. Let $0 \neq I \subset k[x_1, \dots, x_n]$. Fix a monomial ordering on I . A finite subset $G = \{g_1, \dots, g_m\}$ of I is said to be a Gröbner basis for I if $\langle LT(g_1), \dots, LT(g_m) \rangle = \langle LT(I) \rangle$.

Equivalently, a set $\{g_1, \dots, g_m\} \subset I$ is a Gröbner basis of I if and only if the leading term of any element of I is divisible by one of the $LT(g_i), i = 1, \dots, m$. A consequence of the Hilbert Basis Theorem (Theorem 2.5.4 and Corollary 2.5.6 of [2]) is that every nonzero ideal has a Gröbner basis and that it is a basis for the ideal. In fact, there may be many Gröbner bases for a given ideal. A reduced Gröbner basis for an ideal I is a Gröbner basis G for I such that the leading coefficient of each polynomial $p \in G$ is 1 and such that for all $p \in G$ no monomial of p lies in $\langle LT(G - \{p\}) \rangle$. The importance of the reduced Gröbner basis is that for every nonzero ideal I with a given monomial ordering there exists a unique reduced Gröbner basis. (Proposition 2.7.6 of [2]).

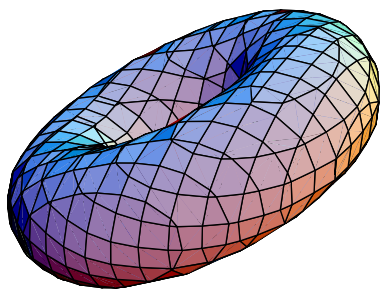
Suppose $0 \neq f, g \in k[x_1, \dots, x_n]$, the least common multiple of f and g denoted $LCM(f, g)$ is the polynomial h such that f and g both divide h and if f and g both divide p then h divides p . The S-polynomial of f and g , denoted $S(f, g)$ is defined as follows:

$$S(f, g) = \frac{LCM(LT(f), LT(g))}{LT(f)}f - \frac{LCM(LT(f), LT(g))}{LT(g)}g.$$

Here is an example of how to calculate a reduced Gröbner basis. We are using what is commonly called Buchberger's algorithm. (See section 1.7 of [1]). Let $f_1 = -x^3 + z$ and $f_2 = -x^2 + y$. Consider $I = \langle f_1, f_2 \rangle$. We wish to find a reduced Gröbner basis for I . First compute $S(f_1, f_2) = \frac{x^3}{-x^3}(-x^3 + z) - \frac{x^3}{-x^2}(-x^2 + y) = xy - z$. Check to see if either $LT(f_1)$ or $LT(f_2)$ divides $LT(xy - z)$. If so, then we do not have to add it to our set; but if neither $LT(f_1)$ or $LT(f_2)$ divide $LT(xy - z)$ we must add it to the set and we let $f_3 = xy - z$. Also, since the $LT(f_2)$ divides the $LT(f_1)$ we can throw out f_1 . Now computing gives $S(f_2, f_3) = xz - y^2$. Since $LT(f_2)$ and $LT(f_3)$ do not divide $LT(xz - y^2)$ we add it to the set as f_4 . Expand and check to see if $LT(f_2, f_4) = -x^2yz - x^2y^2z$ is divisible by at least one of the $LT(f_2), LT(f_3), LT(f_4)$. Since it is, we get $S(f_3, f_4) = y^3 - z^2$ by computing. Since $LT(f_2), LT(f_3)$ and $LT(f_4)$ do not divide the $LT(y^3 - z^2)$, we add this to the set as f_5 and, after checking that the leading terms of $S(f_2, f_5), S(f_3, f_5), S(f_4, f_5)$ are all divisible by one of the leading terms of f_2, f_3, f_4, f_5 , we see that a Gröbner basis for I is $\{-x^2 + y, xy - z, xz - y^2, y^3 - z^2\}$. The reduced Gröbner basis for I is just $\{y^3 - z^2\}$. Note that if we consider the surface formed by the intersection of $f_1 = 0$ and $f_2 = 0$, the projection of this surface into the yz -plane is just $y^3 - z^2 = 0$. Note that we have eliminated the variable x from the original equations.

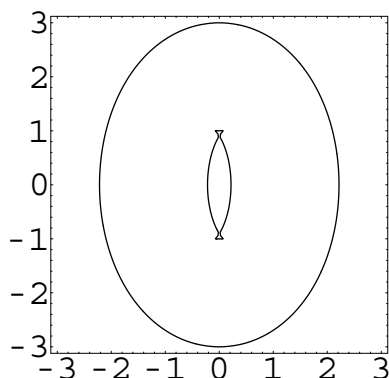
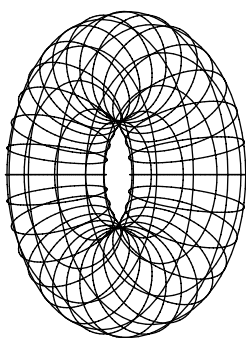
Projections. Now suppose we have a surface S in 3-space with coordinates (x, y, z) and our viewpoint is from above on the z -axis. For example, the tilted torus shown below.

Here $\theta = \frac{\pi}{6}$ is the angle measured upward from the xy -plane.

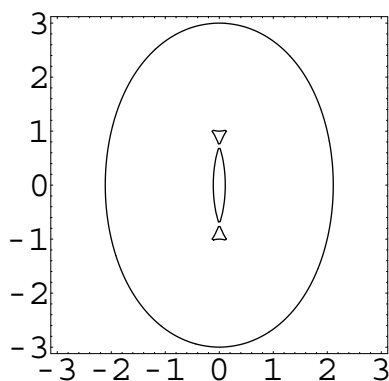
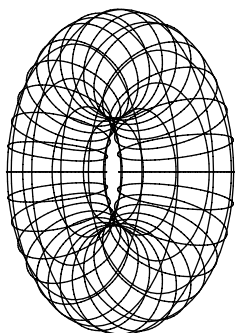


If we were to draw a 2-dimensional line drawing of the torus projected onto the xy -plane, certain

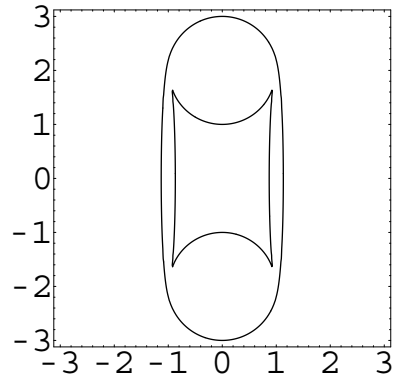
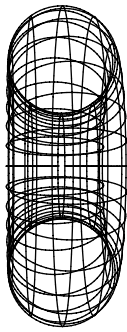
points of the torus show up in this profile while others do not. The points that are projected are exactly the points where the tangent plane to the torus is parallel to the z -axis. This is called the z -profile of the surface. Since a normal vector to a point P on the surface $F(x, y, z) = 0$ is just the gradient vector (F_x, F_y, F_z) of F evaluated at P we quickly see that we have to find solutions of the system of equations $F(x, y, z) = 0$ and $F_z(x, y, z) = 0$. We have already seen above that what we need is the reduced Gröbner basis for the ideal generated by F and F_z . Since this is a much more complicated example than the one we worked earlier, we have used Mathematica to compute the reduced Gröbner basis. Using this basis we have Mathematica graph pictures of the torus and its projections for the torus tilted at 4 different angles.



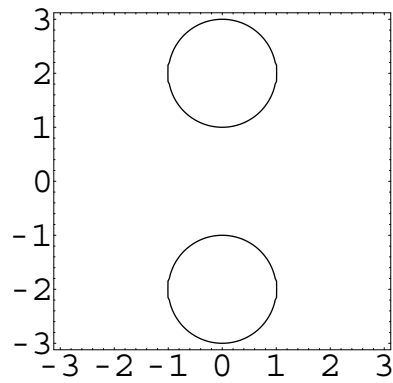
$$\theta = \frac{5}{16}\pi$$



$$\theta = \frac{\pi}{3}$$



$$\theta = \frac{23}{48}\pi$$



$$\theta = \frac{\pi}{2}$$

REFERENCES

1. W.W. Adams and P. Loustau, *An Introduction to Gröbner Bases*, AMS, Providence, RI.
2. D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer Verlag, New York, NY.
3. I. N. Herstein, *Topics in Algebra*, John Wiley and Sons, Inc., New York, NY.