Groebner Bases and Applications

Robert Hines

December 16, 2014

1 Groebner Bases

In this section we define Groebner Bases and discuss some of their basic properties, following the exposition in chapter 2 of [2].

1.1 Monomial Orders and the Division Algorithm

Our goal is this section is to extend the familiar division algorithm from $k[x]$ to $k[x_1, \ldots, x_n]$. For a polynomial ring in one variable over a field, we have the

Theorem 1 (Division Algorithm)**.** *Given $f, g \in k[x]$ with $g \neq 0$, there exists unique $q, r \in k[x]$ with $r = 0$ or $deg(r) < deg(g)$ such that*

$$f = gq + r.$$

We can use the division algorithm to find the greatest common divisor of two polynomials via the

Theorem 2 (Euclidean Algorithm)**.** *For $f, g \in k[x]$, $g \neq 0$, $(f, g) = (r_n)$ where r_n is the last non-zero remainder in the sequence of divisions*

$$\begin{aligned} f &= gq_1 + r_1 \\ g &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\cdots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1} + 0 \end{aligned}$$

Furthermore, $r_n = af + bg$ for explicitly computable $a, b \in k[x]$ (solving the equations above).

We can use these algorithms to decide things such like ideal membership (when is $f \in (f_1, \ldots, f_m)$) and equality (when does $(f_1, \ldots, f_m) = (g_1, \ldots, g_l)$).

In the above, we used the degree of a polynomial as a measure of the size of a polynomial and the algorithms eventually terminate by producing polynomials of lesser degree at each step. To extend these ideas to polynomials in several variables we need a notion of size for polynomials (with nice properties).

Definition 1 (Monomial Order)**.** *A* **monomial order** *on $\mathbb{Z}^n_{\geq 0}$ is a well-ordering $\leq$ such that if $\alpha \leq \beta$, then $\alpha + \gamma \leq \beta + \gamma$.*

We use a monomial order (as the name suggests) to order monomials of $k[x_1, \ldots, x_n]$ by $ax^\alpha \leq bx^\beta$ if $\alpha \leq \beta$ (using the notation $x^\alpha = x_1^{\alpha_1} \cdot \cdots \cdot x_n^{\alpha_n}$ where $\alpha = (\alpha_1, \ldots, \alpha_n)$). Here are two basic examples.

- (lexicographic order) $\alpha > \beta$ if the left-most non-zero entry of $\alpha - \beta$ is positive,
- (graded lexicographic order) $\alpha > \beta$ if $|\alpha| > |\beta|$ or if $|\alpha| = |\beta|$ the left-most non-zero entry of $\alpha - \beta$ is positive (here $|\gamma| = \sum_i \gamma_i$). Any monomial order for which $\alpha > \beta$ if $|\alpha| > |\beta|$ will be refered to as a graded order.

For a given monomial order and a non-zero polynomial $f = \sum_\alpha a_\alpha x^\alpha$, we define the **leading term** of f to be $LT(f) := a_\beta x^\beta$ where β is the largest exponent among α such that $a_\alpha \neq 0$, the **degree** of f to be $\deg(f) := \beta$, the **leading coefficient** $LC(f) := a_\beta$, and the **leading monomial** $LM(F) := x^\beta$.

Given a monomial order we have the following

Theorem 3 (Multivariate Division Algorithm)**.** *Given non-zero $f, f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$, there exist $r, a_i \in k[x_1, \ldots, x_n]$ with*

$$f = \sum_i a_i f_i + r,$$

where r is a sum of monomials none of which is divisible by any of the $LT(f_i)$. Furthermore, either $a_i f_i = 0$ or $deg(a_i f_i) < deg(f)$.

Proof. Here is some pseudocode:

```
INPUT f, f_i
a_i = 0, r = 0
WHILE (f ≠ 0) DO
    i = 1
    division_occurred=FALSE
    WHILE (i ≤ m and division_occurred==FALSE) DO
        IF LT(f_i)|LT(f) THEN
            a_i = a_i + LT(f)/LT(f_i)
            f = f − LT(f)/LT(f_i)
            division_occured=TRUE
        ELSE
            i = i + 1
    IF division_occurred==FALSE THEN
        r = r + LT(f)
        f = f − LT(f)
OUTPUT a_i, r
```

□

As the following examples show, r and a_i depend on the order of the f_i, and while $r = 0$ clearly implies that $f \in I = (f_1, \ldots, f_n)$, the converse does not hold. We use lexicographic order, with $x > y$.

Example 1. Let $f = x^2y + xy^2 + y^2$, $f_1 = y^2 - 1, f_2 = xy - 1$. We get $a_1 = x + 1, a_2 = x$, and $r = 2x + 1$. If we switch the order and let $f_1 = xy - 1, f_2 = y^2 - 1$, we get $a_1 = x + y, a_2 = 1$, and $r = x + y + 1$.

Example 2. Let $f = xy^2 - x$ and $f_1 = xy + 1, f_2 = y^2 - 1$. We get $a_1 = y, a_2 = 0$, and $r = -x - y$. If we switch the order and let $f_1 = y^2 - 1, f_2 = xy + 1$, we get $a_1 = x, a_2 = 0$, and $r = 0$.

These deficiencies are the motivation for the definition of Groebner basis that follows.

1.2 Definition, Existence, and Basic Properties of Groebner Bases

For motivation, (even though we've implicitly assumed finite generation of ideals thus far), we recall the Hilbert basis theorem - more importantly, its proof.

Definition 2. *A* **monomial ideal** $I \subseteq k[x_1, \ldots, x_n]$ *is an ideal generated by a set of monomials* $\{x^\alpha : \alpha \in A\}$ *for some* $A \subseteq \mathbb{Z}^n_{\geq 0}$.

We have a preliminary version of the Hilbert basis theorem,

Theorem 4 (Dickson's Lemma)**.** *If* $I = (x^\alpha : \alpha \in A)$ *is a monomial ideal, there exist* $\alpha^{(1)}, \ldots, \alpha^{(t)} \in A$ *such that* $I = \left(x^{\alpha^{(1)}}, \ldots, x^{\alpha^{(t)}}\right)$.

Proof. See theorem 5 of chapter 2, section 4 of [2]. □

And of the course, the famous

Theorem 5 (Hilbert Basis Theorem)**.** *Every ideal of* $k[x_1, \ldots, x_n]$ *is finitely generated.*

Proof. Fix a monomial order and let I be a non-zero ideal of $k[x_1, \ldots, x_n]$. By Dickson's lemma, there are $g_1, \ldots, g_t \in I$ such that $(LT(I)) = (LT(g_1), \ldots, LT(g_t))$. Clearly $(g_1, \ldots, g_t) \subseteq I$. Conversely, let $f \in I$ and divide by $(g_1, \ldots, g_t)$ to get

$$f = \sum_i a_i g_i + r$$

where no term of the remainder is divisible by any of $LT(g_i)$. If $r \neq 0$, then $LT(r) \in (LT(I)) = (LT(g_i))$, which is impossible (else $LT(g_i) | LT(r)$ for some i). Hence $I = (g_1, \ldots, g_t)$. □

Isolating the property $(LT(I)) = (LT(g_1), \ldots, LT(g_t))$ for $I = (g_1, \ldots, g_t)$ used in the Hilbert basis theorem gives us the following

Definition 3. *A* **Groebner basis** *for an ideal* $I = (f_1, \ldots, f_m) \subseteq k[x_1, \ldots, x_n]$ *(with respect to a given monomial order) is a collection* $g_1, \ldots, g_l \in I$ *such that* $(LT(I)) = (LT(g_i))$*, in which case we have* $I = (g_i)$.

The proof of the Hilbert basis theorem above gives us an important

Corollary 1. *Every ideal of* $k[x_1, \ldots, x_n]$ *has a Groebner basis.*

The frist property of Groebner bases we prove is

Theorem 6 (Uniqueness of Remainder)**.** *If* $(g_1, \ldots, g_m) = I$ *is Groebner basis, then the remainder* r *defined in the division algorithm is independent of the ordering of the* g_i.

Proof. Suppose $f = g + r = g' + r' \in k[x_1, \ldots, x_n]$ with $g, g' \in I$, r, r' such that $LT(g_i)$ does not divide any term of r, r' for any i. Then $LT(r - r') \in (LT(I)) = (LT(g_i))$ and $LT(g_i)|LT(r - r')$ for some i. However, this is impossible as the terms of r, r' are not divisible by $LT(g_i)$. □

Corollary 2. *If $(g_1, \ldots, g_m) = I$ is a Groebner basis, then $f \in I$ if and only if the remainder r in the division algorithm is zero.*

Although the remainder is unique, the a_i in the division algorithm still depend on the order of the g_i as the following example shows.

Example 3. Accepting that $(x + z, y - z) = I$ is a Groebner basis of $I \subseteq k[x, y, z]$ with respect to the lexicographic order and $x > y > z$, we divide $f = xy$ in both orders to get

$$f = y(x + z) - z(y - z) - z^2, f = x(y - z) + z(x + z) - z^2,$$

with unique remainder $r = -z^2$ but different coefficients.

1.3 Checking and Producing Groebner Bases - Buchberger's Criterion and Algorithm

We now consider whether or not a given basis is a Groebner basis (Buchberger's criterion) and how to produce a Groebner basis from a given basis (Buchberger's algorithm).

Definition 4. *The* **S-polynomial** *(with respect to a monomial order) of two non-zero polynomials $f, g \in k[x_1, \ldots, x_n]$ is*

$$S(f, g) = \frac{x^\gamma}{LT(f)} f - \frac{x^\gamma}{LT(g)} g$$

where $\gamma_i = \max\{\alpha_i, \beta_i\}$ and $deg(f) = \alpha, deg(g) = \beta$ (i.e. x^γ is the least common multiple of x^α, x^β).

Clearly the leading term of the S-polynomial is a potential obstruction to $(LT(I)) = (LT(f_1), \ldots, LT(f_m))$ for an ideal $I = (f_1, \ldots, f_m)$, but it turns out that it is the only obstruction.

Theorem 7 (Buchberger's Criterion)**.** *The basis $(g_1 \ldots, g_m) = I$ is a Groebner basis if and only if for all i, j, $S(g_i, g_j)$ has remainder zero after division by I (in some/every order of the g_k).*

Proof. See theorem 6 of chapter 2, section 6 of [2]. □

Example 4. With lexicographic order and $y > z > x$, $(y - x^2, z - x^3)$ is a Groebner basis for the twisted cubic (t, t^2, t^3) since

$$S(y - x^2, z - x^3) = yx^3 - zx^2 = x^3(y - x^2) - x^2(z - x^3) + 0.$$

However, with lexicographic order and $x > y > z$, $(-x^2 + y, -x^3 + z)$ is *not* a Groebner basis since

$$S(-x^2 + y, -x^3 + z) = -xy + z = r \neq 0,$$

(neither $-xy$ nor z is divisible by the leading terms $-x^2, -x^3$ of the generators of I).

Finally, we present an algorithm for producing a Groebner basis $(g_1, \ldots, g_l)$ for an ideal $I = (f_1, \ldots, f_m)$ by adding in successive remainders of division of S-polynomials.

Theorem 8 (Buchberger's Algorithm)**.** *There is an algorithm to produce a Groebner basis for* $I = (f_1, \ldots, f_m)$.

Proof. The following (non-optimized) algorithm produces a Groebner basis $(g_1 \ldots, g_l)$ for an ideal $I = (f_1, \ldots, f_m)$.

INPUT $F = \{f_1, \ldots, f_m\}$
$G = F$
DO
    $G' = G$
    FOR (all pairs $p, q \in G', p \neq q$)
        $S = S(p, q)\%G'$ (the remainder of $S(p, q)$ after division by G')
        IF $S \neq 0$ THEN $G = G \cup \{S\}$
WHILE $(G' \neq G)$
OUTPUT $G = \{g_1, \ldots, g_l\}$

It is clear that $I = (F) \subseteq (G) \subseteq I$ at each step of the algorithm and that the result is a Groebner basis by Buchberger's criterion. The process terminates since $k[x_1, \ldots, x_n]$ is Noetherian and $(LT(G')) \subsetneq (LT(G))$ because $LT(S(p, q)\%G') \notin (LT(G'))$ if it is non-zero. □

Example 5. Consider $I = (x^3 - 2xy, x^2y - 2y^2 + x) \subseteq k[x, y]$ with the graded lexicographic order and $x > y$. The algorithm above produces the Groebner basis

$$I = (x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x).$$

The Groebner basis produced by the algorithm above can be large and redundant. We can eliminate/modify a Groebner basis to produce a *unique* Groebner basis for an ideal I (with respect to a monomial order), analogous to the reduced row echelon form of a system of linear equations.

Definition 5. *A* **reduced Groebner basis** G *for an ideal* $I \subseteq k[x_1, \ldots, x_n]$ *is a Groebner basis such that*

- $LC(g) = 1$ *for all* $g \in G$ *(*G *consists of monic polynomials),*
- *for every* $g \in G$*, no term of* g *is an element of* $(LT(G \backslash \{g\}))$.

Theorem 9. *Every ideal* $I \subseteq k[x_1, \ldots, x_n]$ *has a unique reduced Groebner basis.*

Proof. See proposition 6, chapter 2, section 7 of [2]. □

Example 6. The reduced Groebner basis for the previous example (graded lexicographic, $x > y$, $I = (x^3 - 2xy, x^2y - 2y^2 + x)$) is

$$I = (x^2, xy, y^2 - x/2).$$

Having covered the "Groebner basics", we move on to a brief overview of some applications.

2 Applications

There are many, many applications of Groebner bases to computational algebraic geometry; here we offer a few (with most details omitted).

2.1 Dimension

One can use Groeber bases to compute the dimension of an affine variety $V = V(I)$, $I = (f_1, \ldots, f_m) \subseteq k[x_1, \ldots, x_n]$ by considering an appropriate "linearization". We first discuss the case where $I = (m_1, \ldots, m_t)$ is a monomial ideal.

The variety defined by a monomial ideal is a finite union of coordinate subspaces of k^n (i.e. linear subspaces defined by the simultaneous vanishing of coordinate functions),

$$V = V\left(\left\{m_j = x^{\alpha^{(j)}}\right\}_j\right) = \bigcap_j \bigcup_i V\left(x_i^{\alpha_i^{(j)}}\right) = \bigcap_j \bigcup_{\substack{i \text{ s.t.} \\ \alpha_i^{(j)} > 0}} V(x_i),$$

and its dimension is the maximum dimension of its components. If we define

$$M_j = \{k \in [1,n] : x_k | m_j\},\ \mathcal{M} = \{J \subseteq [1,n] : J \cap M_j \neq \text{ for all } j\},$$

a little thought shows that the dimension of V is $n - \min\{|J| : J \in \mathcal{M}\}$. The key to computing dimension for arbitrary I is the following

Theorem 10. *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal and $\geq$ a graded monomial order. Then the monomial ideal $(LT(I))$ has the same Hilbert function as I.*

Proof. See proposition 4 of chapter 9, section 3 in [2]. □

So to find the dimension of the variety defined by $I = (f_1, \ldots, f_m)$, first compute a Groebner basis $I = (g_1, \ldots, g_k)$ with respect to a graded monomial order, then determine the dimension of the variety defined by $(LT(I)) = (LT(g_i))$ (equality because we're using a Groebner basis).

2.2 Projective Closure

Given an affine variety $V_a = V(I)$, $I = (f_1, \ldots, f_m) \subseteq k[x_1, \ldots, x_n]$, we can consider its projectivization, $V_p = V(I^h)$ where $I^h = (f^h : f \in I)$ is the homogenization of I, and

$$f^h = x_0^{|\deg(f)|} f(x_1/x_0, \ldots, x_n/x_0) \in k[x_0, \ldots, x_n]$$

the homogenization of f ($\deg(f)$ taken with respect to a graded order). To obtain generators for I^h, one may naively from the ideal

$$J = (f_1^h, \ldots, f_m^h) \subseteq I^h,$$

but this is generally strictly smaller than I^h as the next example shows.

Example 7. Consider the twisted cubic, $I = (f_1, f_2) = (x_2 - x_1^2, x_3 - x_1^3)$. We have $J = (f_1^h, f_2^h) = (x_0x_2 - x_1^2, x_0^2x_3 - x_1^3)$, but the polynomial $f_3 = f_2 - x_1f_1 = x_3 - x_1x_2 \in I$ has homogenization $f_3^h = x_0x_3 - x_1x_2 \in I^h \backslash J$.

However, if we start with a Groebner basis $I = (g_1, \ldots, g_k)$ with respect to a graded monomial order, we have the following

Theorem 11. *If $I = (g_1, \ldots, g_k)$ is a Groebner basis with respect to a graded monomial order $\geq$, then $I^h = (g_1^h, \ldots, g_k^h)$. Moreover, $I^h = (g_1^h, \ldots, g_k^h)$ is a Groebner basis with respect to the monomial order $\geq_h$ given by $x^\alpha x_0^d >_h x^\beta x_0^e$ if $\alpha > \beta$ or $\alpha = \beta$ and $d > e$.*

Proof. See theorem 4 of chapter 8, section 4 in [2]. □

2.3 Elimination

This section concerns using Groebner bases to solve systems of polynomial equations by eliminating variables. See chapter 3 of [2] for more applications of elimination.

Definition 6. *The* l**-th elimination ideal** *of an ideal* $I \subseteq k[x_1, \ldots, x_n]$ *is the ideal of* $k[x_{l+1}, \ldots, x_n]$ *given by*

$$I_l = I \cap k[x_{l+1}, \ldots, x_n].$$

With this definition, we have the

Theorem 12 (Elimination Theorem)**.** *Let* $G = \{g_i\} \subseteq k[x_1, \ldots, x_n]$ *be a Groebner basis of an ideal* I *with respect to the lexicographic order,* $x_1 > \cdots > x_n$*. The for all* l*,*

$$G_l = G \cap k[x_{l+1}, \ldots, x_n]$$

is a Groebner basis for the l*-th elimination ideal* I_l*.*

Proof. Clearly, $G_l \subseteq I_l$ and $(LT(G_l)) \subseteq (LT(I_l))$, so let $f \in I_l$. Since $f \in I$ and G is a Groebner basis, there is a $g \in G$ such that $LT(g)|LT(f)$. Hence $LT(g) \in k[x_{l+1}, \ldots, x_n]$, and because we are using lexicographic order with $x_1 > \cdots > x_n$, if $LT(g) \in k[x_{l+1}, \ldots, x_n]$, then $g \in k[x_{l+1}, \ldots, x_n]$. Hence $(LT(I_l)) \subseteq (LT(G_l))$ and G_l is a Groebner basis for I_l. □

Example 8. Consider the system of equations

$$\begin{aligned} x^2 + y + z &= 1 \\ x + y^2 + z &= 1 \\ x^2 + y + z^2 &= 1. \end{aligned}$$

The ideal they generate has Groebner basis (with respect to the lexicographic order, $x > y > z$)

$$\begin{aligned} g_1 &= x + y + z^2 - 1 \\ g_2 &= y^2 - y - z^2 + z \\ g_3 &= 2yz^2 + z^4 - z^2 \\ g_4 &= z^6 - 4z^4 + 4z^3 - z^2 = z^2(z-1)^2(z^2 + 2z - 1). \end{aligned}$$

Working backwards from the last generator to the first, we find the solutions

$$(1,0,0), (0,1,0), (0,0,1), (-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}), (-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2}).$$

References

[1] Thomas Becker, Volker Weispfenning, *Gröbner Bases*, Graduate Texts in Mathematics vol. 141, Springer-Verlag, 1993

[2] Cox, Little, O'Shea, *Ideals, Varieties, and Algorithms*, Third Edition, Undergraduate Texts in Mathematics, Springer, 2007