Computational Algebraic Geometry

Yvan Grinspan

July 7 2020

Contents

1 Introduction

In the ring of univariate polynomials, $k[x]$, we can find a unique, principal representation for any ideal. The procedure for finding this simplified form of an ideal with multiple generators is a generalization of Euler's algorithm for finding the greatest common divisor of two integers. Using polynomial division, we can repeatedly divide the largest generator by a smaller one and replace it with the resulting remainder in the generating set. This will always yield the greatest common factor of the generators, which generates the same ideal as the original generating set.

However, this concept of a unique, convenient representation of an ideal breaks down when we look at polynomials in multiple variables. First, not every ideal in $k[x_1, \ldots, x_n]$ is principal (take (x, y) as a simple example). Also, our algorithm for reducing a generating

set no longer works because it relies on degree in order to determine which polynomial is greatest and should be reduced through division.

Gröbner bases offer a solution to these issues by providing a single canonical basis for any multivariate polynomial ideal, and in general, they facilitate many aspects of the study of ideals in $k[x_1, \ldots, x_n]$. For example, they can be used to determine equivalencies of polynomial ideals and to decide whether a polynomial is in a given ideal. They are also useful when manipulating and solving systems of polynomial equations. However, before we discuss Gröbner bases, we must find a way to compare the "complexity" of polynomials, and in turn bases in multiple variables.

2 Monomial Orderings

In order to form a concept of a more or less simple basis for an ideal, we need a system that is analogous to degree in $k[x]$ to determine which of two given monomials we should define as "greater" than the other. A monomial ordering provides this consistent order of monomials in a polynomial, which is necessary when comparing, dividing, and reducing polynomials.

Definition 2.1. *A **monomial ordering** on $k[x_1, \ldots, x_n]$ is a relation $>$ on the set of monomials $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$, where $0 \leq \alpha_i$ (which we abbreviate as α) satisfying the following properties:*

1. *For any monomials α and β, exactly one of the three statements $\alpha > \beta$, $\alpha < \beta$, and $\alpha = \beta$ is true.*
2. *$>$ is transitive. That is, for any monomials α, β, and γ, if $\alpha > \beta$ and $\beta > \gamma$, then $\alpha > \gamma$.*
3. *If $\alpha > \beta$ and γ is a monomial, then $\alpha + \gamma > \beta + \gamma$ and $\alpha\gamma > \beta\gamma$.*
4. *Every set S of monomials has a smallest element, that is, an element α such that $\beta > \alpha$ for every $\beta \in S \setminus \alpha$.*

The definition above does not seem very useful, since the properties are intuitive given the term "ordering," but it is still very important to keep these basic properties in mind. Most algorithms and definitions related to Gröbner bases rely on the choice of ordering, and so does whether a given basis is a Gröbner basis at all. Here are three examples of monomial orderings (in the following definitions, α_i denotes the power of x_i in monomial α):

Definition 2.2. ***Lexicographic** or **lex** order is the monomial ordering described by the following. Let α and β be monomials. For the smallest value i such that $\alpha_i \neq \beta_i$, $\alpha >_{lex} \beta$ if $\alpha_m > \beta_m$.*

Example: $x_1^2 x_2^4 x_3^3 >_{lex} x_1^2 x_2^3 x_3^7$ because $2 = 2$ and $4 > 3$

Lex ordering is the most intuitive because it is a similar system to alphabetical order, but it is actually the most difficult ordering of the three to use in anything but simple

computation. However, it is still very useful because it is an elimination order, meaning it allows for elimination, which will be discussed later.

Definition 2.3. ***Graded Lexicographic*** *or* ***grlex*** *order is the monomial ordering described by the following. Let α and β be monomials. $\alpha >_{grlex} \beta$ if $\sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i$. If these two quantities are equal, then $\alpha >_{grlex} \beta$ if $\alpha >_{lex} \beta$.*

Examples:

- $x_1^2x_2^4x_3^3 <_{grlex} x_1^2x_2^3x_3^7$ because $2+4+3 < 2+3+7$
- $x_1^7x_2^2x_3^3 >_{grlex} x_1^3x_2^4x_3^5$ because $7+2+3 = 3+4+5$ and $7 > 2$

Grlex ordering has the nice property that any monomial has a finite number of monomials that are less than it. However, it is the least common of three because it is more difficult to compute with than the next ordering despite being fairly similar.

Definition 2.4. ***Graded Reverse Lexicographic*** *or* ***grevlex*** *order is the monomial ordering described by the following. Let α and β be monomials. Then $\alpha >_{grevlex} \beta$ if $\sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i$. If these two quantities are equal, $\alpha >_{grevlex} \beta$ if, for the greatest value i such that $\alpha_i \neq \beta_i$, $\alpha_i < \beta_i$.*

Examples:

- $x_1^2x_2^4x_3^3 <_{grevlex} x_1^2x_2^3x_3^7$ because $2+4+3 < 2+3+7$
- $x_1^7x_2^2x_3^3x_4^2 >_{grevlex} x_1^3x_2^4x_3^5x_4^2$ because $7+2+3 = 3+4+5$ and $3 < 5$

Grevlex ordering seems counter-intuitive at first because the tie-breaking comparison gives the opposite result from what seems natural. One way to think about why it is defined this way is that if two monomials have the same total degree, the one with the lower exponent in the rightmost variables must have higher exponents in the more leftward, "important" variables, and therefore is chosen as the greater monomial.

3 Reduction

Now that we have the tools to keep a consistent order of terms in a multivariate polynomial we can move on to finding ways to manipulate bases of ideals according to this order, but first, we define a simple piece of notation that will be used frequently.

Definition 3.1. ***LT(f)****, where $f \in k[x_1, \ldots, x_n]$, is the leading term of f, or the greatest monomial in f following the chosen ordering. LT(S), where S is a set of polynomials, is the set of LT(p) for all $p \in S$.*

Now, we can define a generalization of Euler's algorithm in multiple variables. This new algorithm removes from a polynomial f multiples of polynomials in a set $\{p_1, \ldots, p_s\}$, leaving

the reduction, or remainder, r. In other words, given f and a set P, this algorithm finds $q_1, \ldots, q_s \in k[x_1, \ldots, x_n]$ such that $f = q_1p_1 + q_2p_2 + \ldots + q_sp_s + r$ and returns r.

Definition 3.2. *The **reduction** r of $f \in k[x_1, \ldots, x_n]$ by a set $P = \{p_1, \ldots, p_n\} \subset k[x_1, \ldots, x_n]$ using a chosen monomial ordering can be constructed using the following algorithm:*

1. *Let $g = f$ and $r = 0$.*
2. *Searching in order from p_1 to p_n, let p_i be the first polynomial such that $LT(p_i)|LT(g)$. Subtract $\frac{LT(g)}{LT(p_i)}p_i$ from the value of g.*
3. *Repeat step 2 until there is no possible p_i.*
4. *Subtract the leading term from g and add it to r.*
5. *If $g \neq 0$, then return to step 2. Otherwise, the algorithm is finished and r is the reduction of f by P.*

Notice that this algorithm is quite similar to polynomial long division, except for a few key differences. These differences come from the fact that, in more than one variable, a monomial that is smaller than another monomial according to a chosen ordering does not necessarily divide the larger monomial. In a single variable, $x^a|x^b$ as long as $a < b$, or equivalently, $x^a < x^b$. In grevlex order, though, if we let $x > y$, then $x^2 > xy$ but $xy \nmid x^2$, as an example.

The part of the algorithm that stands out as most different from long division is step 4, where $LT(g)$ is removed and added to r. This step is necessary because even if nothing in $LT(P)$ divides $LT(g)$, there could still be multiples of elements of P remaining in g. For example, let $g = x^2 + xy$ and $LT(p_a) = xy$ for some a, and assume $\beta \nmid x^2$ for any $\beta \in LT(P)$. If step 4 wasn't included and we proceeded like in normal division, $x^2 + xy$ would be considered the reduction of f, but once the leading term x^2 is removed, we are able to subtract xy from g and therefore reduce it further, calculating a residue of x^2 instead.

It is tempting to say that this algorithm is equivalent to finding a canonical form of f in $k[x_1, \ldots, x_n]/(P)$, since it involves repeatedly subtracting elements of P from f. However, there is an important caveat to this statement: the algorithm often yields a different result based on the order of the polynomials in P. For example, let $f = x^2y + xy^2 + 1$ and $P = \{xy - 1, x + 1\}$. The following reduction process yields y:

$$f - xp_1 = xy^2 + x + 1 \to xy^2 + x + 1 - yp_1 = x + y + 1 \to x + y + 1 - p_2 = y.$$

On the other hand, if we reduce f by $P' = \{x + 1, xy - 1\}$, we have:

$$f - xyp'_1 = xy^2 - xy + 1 \to xy^2 - xy + 1 - y^2p'_1 = -xy + y^2 + 1 \to -xy + y^2 + 1 - (-y)p'_1 = y^2 + y + 1.$$

From this example, we see that the reduction of a polynomial by a set is not unique, so it is not a suitable method for finding a canonical form of a polynomial in $k[x_1, \ldots, x_n]/(P)$. Reduction is more helpful when the set of polynomials has certain special properties, which lead to the study of Gröbner bases.

4 Gröbner Bases

So far, we have considered the reduction set P to be an arbitrary set of polynomials, but we can also think of it as a basis for an ideal in $k[x_1, \ldots, x_n]$. This is the first step to finding a canonical basis for a polynomial ideal, which we will eventually do through Gröbner bases.

Definition 4.1. *A* ***Gröbner basis*** $G = \{g_1, \ldots, g_n\}$ *of an ideal* $I \subset k[x_1, \ldots, x_n]$ *is a subset of* I *such that* $(LT(G)) = (LT(I))$.

Although the term strongly suggests the following result, it is not immediately obvious to be true based on the definition.

Theorem 4.1. *Any Gröbner basis* G *of an ideal* I *is a basis of* I.

Proof. Let $G = \{g_1, \ldots, g_n\}$ be a Gröbner basis of an ideal I. By definition, $(LT(G)) = (LT(I))$. We are aiming to prove that $I = (G)$. One direction of inclusion, $(G) \subset I$, is obvious because $G \subset I$.

To prove the other direction, let $f \in I$. If we reduce f by G in the order above, we get a polynomial r where no term of r is divisible by a leading term in $LT(G)$. Assume $r \neq 0$. Since r is the result of subtracting multiples of elements of G from f, and $G \in I$, it must be true that $r \in I$. However, this implies that $LT(r) \in (LT(I))$, and as we have previously stated, this is equivalent to $LT(r) \in (LT(G))$. Then $LT(r)$ must be a multiple of $LT(g_i)$ for some i, which contradicts the definition of reduction. Therefore, we can trace the reduction process to express f as a sum of multiples of elements of G, so $f \in (G)$. f is an arbitrary polynomial in I, so $I = (G)$. □

The following theorem is another fundamental result in the theory of Gröbner bases.

Theorem 4.2. *Every ideal* I *has a Gröbner basis.*

Proof. $(LT(I))$ is generated by all the leading monomials in I, and all monomial ideals are finitely generated (the proof is left out for conciseness). Therefore, $(LT(I))$ can also be generated by a finite set of leading monomials $LT(P)$ in I. For any such set, P is a Gröbner basis. □

We can now define an algorithm to derive a Gröbner basis from an arbitrary basis of an ideal. Buchberger's algorithm does so by exclusively adding polynomials to a basis until it satisfies the definition of a Gröbner basis.

Theorem 4.3 (Buchberger's Algorithm)**.** *For any polynomial ideal* $I \subset k[x_1, \ldots, x_n]$*, a the following algorithm terminates and produces a Gröbner basis of* I *from a basis* $P = \{p_1, \ldots, p_s\}$.

1. *Let* $Q = P$.

2. *Choose two different elements f and g in Q. Let α be the lowest common multiple of LT(f) and LT(g) (that is, the monomial whose x_a-degree is the maximum of the x_a-degree of LT(f) and the x_a-degree of LT(g) for all $1 \leq \alpha \leq n$). Let f' and g' be f and g respectively multiplied by monomials so that $LT(f') = LT(g') = \alpha$. Let $s = f' - g'$, so that the α terms cancel out.*
3. *Reduce s by Q, and if the result is non-zero, add the reduction to Q.*
4. *Repeat steps 2-3 for every pair of polynomials f and g in Q.*
5. *Repeat steps 2-4 until there is no pair of polynomials in Q that result in a new element. Q is now a Gröbner basis of I.*

Proof. However, we can prove that the algorithm terminates. For any single iteration of steps 2-3, let Q' be the basis before any polynomial is added, and let Q be the basis at the end of step 3, with the new polynomial included. It is clear that $(LT(Q')) \subseteq (LT(Q))$, since $Q' \subseteq Q$. However, the new polynomial r added is a result of a reduction by Q', so by definition, $LT(q_i') \nmid LT(r)$ for any i. Therefore, $LT(r) \notin (LT(Q'))$, so $(LT(Q'))$ is strictly smaller than $(LT(Q))$, so as the algorithm is repeated, all of the ideals $(LT(Q))$ form a strictly ascending chain. Since $k[x_1, \ldots, x_n]$ is noetherian, there is no infinite strictly ascending chain of ideals, so the chain of $(LT(Q))$'s must stabilize at some point. We have shown that it strictly grows as long as the algorithm continues and new polynomials are added, so the algorithm must terminate after a finite number of iterations.

Let $S(f, g)$ for $f, g \in k[x_1, \ldots, x_n]$ be the result h of step 2 described above. When the algorithm terminates, $S(q_i, q_j)$ for any i and j yields 0 when reduced by Q. Buchberger's Criterion states that this condition is true if and only if Q is a Gröbner basis, but the proof of this criterion is unfortunately beyond the scope of this paper. However, for some idea as to why Q might end up being a Gröbner basis, it makes sense that the ascending chain of $(LT(Q))$ ideals stabilizes at its largest possible value, $(LT(I))$, making Q a Gröbner basis when the algorithm terminates.

□

Although general Gröbner bases have some convenient properties, they are still not unique for a given ideal. However, once we have a Gröbner basis, we are very close to finally arriving at the unique, "canonical" representation of an ideal in $k[x_1, \ldots, x_n]$.

Definition 4.2. *A **reduced Gröbner basis** G of an ideal I is a Gröbner basis in which every element has a leading coefficient of 1 and no monomial in any element is a multiple of a leading monomial.*

As the name might suggest, a reduced Gröbner basis can be derived from a Gröbner basis G by reducing each element p by $G \setminus p$, then make each element monic by dividing it by its leading coefficient. This results in a reduced Gröbner basis because the reduction of p by $G \setminus p$ does not have any monomial that is a multiple of a leading term in $G \setminus p$, since such a monomial would be removed in the reduction process.

Theorem 4.4. *Every ideal $I \subset k[x_1, \ldots, x_n]$ has a unique reduced Gröbner basis.*

Proof. First, every ideal I must have a Gröbner basis, and a reduced Gröbner basis can be derived from any Gröbner basis, so every ideal has a reduced Gröbner basis.

As for proving uniqueness, assume we have two reduced Gröbner bases G and H for the same ideal I. $LT(G)$ and $LT(H)$ are both bases of $(LT(I))$ by the definition of a Gröbner basis. By the definition of a reduced Gröbner basis, every element of $LT(G)$ is unique and none of the elements divide another. The same property holds for H. This means that $LT(G)$ and $LT(H)$ are both minimal bases of the monomial ideal $(LT(I))$, meaning they must be equal.

Therefore, for every $g \in G$, there exists $h \in H$ such that $LT(g) = LT(h)$. Consider $g - h$. This is an element of I, and G is a basis of I, so $g - h$ reduced by G gives 0. However, when we take $g - h$, the leading terms cancel out, so $g - h$ is not divisible by $LT(g)$. The remaining terms are all monomials in g or h. Since G and H are reduced, this means that none of the terms in $g - h$ are divisible by any element of $LT(G) = LT(H)$. Therefore, $g - h$ is irreducible by G, and $g - h$ reduced by G is simply $g - h$. But we have previously shown that $g - h$ reduced by G is 0, so $g - h = 0$. Therefore, $g = h$ for all $g \in G$, so $G = H$, and the reduced Gröbner basis of an ideal is unique. □

5 Applications of Gröbner Bases

Now that we have defined several properties and algorithms related to Gröbner bases, we can explore how they apply to other parts of algebraic geometry, ring theory, and mathematics at large.

5.1 Ideal Membership, Ideal Equality, and Coordinate Rings

We can say that $f \in k[x_1, \ldots, x_n]$ is in an ideal I if its reduction by a basis B of I is 0. This is because the reduction process consists of subtracting multiples of elements of B, so if it results in 0, then f is a sum of multiples of elements of B, meaning it is in I. However, the converse is not necessarily true because the result of reduction depends on the order of the set by which the polynomial is reduced. As a simple example, $2x \in (x + y, x)$ clearly, but when we use that order of the two generators to reduce $2x$, we have $2x - 2(x + y) = -2y$, which cannot be reduced any further.

This problem goes away when we are specifically dealing with Gröbner bases.

Theorem 5.1. *A polynomial f is in an ideal I if and only if its reduction by a Gröbner basis G of I yields 0.*

Proof. The forwards direction is obvious because it is true for any basis, as stated before. The problem with the other direction when we use a non-Gröbner basis stems from the fact

that the value of a reduction depends on the order of the elements in the basis, so we try to prove that reduction over a Gröbner basis yields the same remainder no matter the order of the elements.

Reduction over G splits f into $f_1p_1+f_2p_2+\ldots+f_mp_m+r$, where $f_i \in k[x_1,\ldots,x_n]$, $p_i \in G$, and r does not have any term divisible by a leading term in G. Let $g = f_1p_1+f_2p_2+\ldots+f_mp_m$. Then we can also say that reduction expresses f as $g+r$, where $g \in G$. Suppose that there is another way to split f, which we call $g'+r'$, and we get this alternative when we order the terms in G differently. Then, assuming $r \neq r'$, we have $g+r = g'+r'$, so $r-r' = g'-g \in I$. By the definition of a Gröbner basis, this means that $LT(h)|r-r'$ for some $h \in G$. However, we assumed that no term of r or r' divides any leading term in G. Therefore, $r = r'$ and the result of reduction is unique.

If $f \in I$, then there is a way to express f as $f_1p_1+f_2p_2+\ldots+f_mp_m$ where $f_i \in k[x_1,\ldots,x_n]$ and $p_i \in G$, so the reduction of f is 0 for some ordering of elements of G. It follows that the reduction of f by G is 0 independently of the order. □

We can extend this idea of reduction by a Gröbner basis to coordinate rings. In order to more easily theorize about quotient rings of polynomial ideals, we often select a single polynomial to represent each coset in a quotient ring. For example, in $k[x,y,z]/(x)$, we can represent each element as a single polynomial in $k[y,z]$. As was suggested earlier, we can use reduction by a Gröbner basis to find such a canonical representative of a coset in coordinate rings. The problem with this before the introduction of Gröbner bases was that reduction over a general polynomial set is not unique. However, our proof of theorem 5.1 says that Gröbner bases solve this problem, and we can safely reduce polynomials by Gröbner bases in order to find canonical forms of polynomials in coordinate rings.

Another related use for Gröbner bases for analyzing ideals in $k[x_1,\ldots,x_n]$ is determining whether two sets of multivariate polynomials generate the same ideal or not. We can apply Buchberger's algorithm to both sets to form Gröbner bases, then reduce both of these bases to get reduced Gröbner bases. Because reduced Gröbner bases are unique, the two ideals generated by the sets are the same if and only if the resulting reduced Gröbner bases are identical. Although it is sometimes easier to tell that two generating sets are equivalent by inspection, this method can be very useful when dealing with sets of complicated, very different-looking polynomials in many variables.

5.2 Elimination Theory

One important application of Gröbner bases outside of ring theory is in solving, or eliminating variables from, systems of polynomial equations.

When we have a system of polynomial equations in $x_1,\ldots,x_n$ that we would like to solve, we can make a Gröbner basis from the system. There is often a subset of the Gröbner basis that only involves a certain number of smaller variables $x_{i+1},\ldots,x_n$, and the following theorem states that if it is possible to deduce a simpler set of equations in fewer variables

and eliminate $x_1, \ldots, x_i$ in this way, then the Gröbner basis of the system will contain such a set of polynomials.

However, this only works when we use a special type of ordering for the Gröbner basis called an elimination ordering. In an elimination ordering, the variables are divided into different blocks ($\{x_1, \ldots, x_i\}$ and $\{x_{i+1}, \ldots, x_n\}$, for example, would define an elimination ordering with 2 blocks). Two monomials are compared using a chosen ordering, often grevlex, with only their parts in the first block. If this causes a tie, then their second-block parts are compared, and so on. The Elimination Property allows for the elimination of the first k blocks for some k. The simplest elimination order is one with which we are already familiar, namely lex order, which has n blocks in the set of variables $\{x_1, \ldots, x_n\}$. Lex order therefore has the benefit that any set of variables $x_1, \ldots, x_i$ can be eliminated. Therefore, the version of the theorem below, which uses lex order, is more useful than the more general version using a general elimination order.

Theorem 5.2 (Elimination Property)**.** *Let G be a Gröbner basis of an ideal $I \subset k[x_1, \ldots, x_n]$ using lex order. For every $0 \leq i \leq n$, $G \cap k[x_{i+1}, \ldots, x_n]$ is a Gröbner basis of $I \cap k[x_{i+1}, \ldots, x_n]$.*

Proof. Fix i between 0 and n. Let $G_i = G \cap k[x_{i+1}, \ldots, x_n]$ and $I_i = I \cap k[x_{i+1}, \ldots, x_n]$. Because $G \subset I$, we have $G_i \subset I_i$, so we can prove the theorem by proving that $(LT(G_i)) = (LT(I_i))$. The forwards inclusion is obvious.

We now try to prove the reverse inclusion. First, notice that since $f \in I$, we have $LT(g)|LT(f)$ for some $g \in G$. Because $f \in I_i$, $LT(g)$ involves only $\{x_{i+1}, \ldots, x_n\}$. However, since we are working in lex order, any monomial involving a variable in $\{x_1, \ldots, x_i\}$ is greater than any monomial that does not. Since $LT(g)$ is the greatest monomial in g and it does not involve any of these larger variables, none of the other monomials in g does either. Therefore, $g \in G_i$. This means that for any $f \in I_i$, there exists $g \in G_i$ such that $LT(g)|LT(f)$. □

It is important to notice that even though the Elimination Property applies for any Gröbner basis, it is most likely to be useful with the reduced Gröbner basis because the process of reduction may remove certain variables completely from some polynomials.