GRÖBNER BASES

ISHAN LEVY

1. Hilbert Basis Theorem & Monomial Orderings

Gröbner bases are a great way to do computations in polynomial rings $R[x_1, \ldots, x_n]$ which is quite useful in algebraic geometry, where such rings are viewed as the ring of functions on an affine space. They allow you to answer questions like:

- Given two ideals I, J, how can you compute $I \cap J$?
- Given an ideal I, how can you make computations in the quotient $K[x_1, \ldots, x_n]/I$?
- Given two ideals I, J, how can you tell if they are the same?
- How can you tell if an element is in the radical of an ideal?
- How can you compute the saturation of an ideal with respect to a polynomial?
- How can we find solutions to systems of polynomial equations (when there are finitely many)?
- How can we compute the ideal quotient $(I : J) = \{r | rJ \subset I\}$

These will all be answered here.

The fundamental idea of the Gröbner basis is seen in the proof of the Hilbert Basis Theorem:

Theorem 1.1 (Hilbert Basis Theorem)**.** *If R is Noetherian, then $R[x]$ is too.*

Proof. Fix an ideal of $R[x]$, I. Let L_n be the ideal in R of leading coefficients of terms with x^n as the leading term in I. L_n stabilizes as $n \to \infty$ as R is Noetherian. Thus by choosing polynomials whose leading terms generate L_n up till the point of stabilization we get a finite set of generators for I. □

As a corollary, $R[x_1, \ldots, x_n]$ is Noetherian (induction), but note that this inductive argument implicitly orders x_1 to x_n. The ideas of ordering and looking at leading terms generating an ideal give rise to Gröbner bases.

Definition 1.2. *A **monomial ordering** is a well ordering on monomials satisfying $a \leq b \implies ac \leq bc$ (a,b,c are monomials in $R[x_1, ..., x_n]$).*

Here are three important examples:

- **(lex)** We can lexicographically order monomials with $x_1 > \cdots > x_n$.
- **(grlex)** We can "grade" the lexicographical ordering by ordering monomials by total degree, and if they are the same degree, then by lex.
- **(grevlex)** We can first grade monomials by degree, and if they are the same degree, we can start from x_n going to x_1, saying that $m > n$ if m has a lower exponent on x_n.

Note in all of these orderings we have $x_1 > \cdots > x_n$.

As an example consider these three orderings of the same set of monomials:

- (lex) $x^3y, x^3y^2, x^2y^2z, x^2yz^2, x^2z^2, x^2z, x^2, xy^2z$
- (grlex) $x^3z^2, x^2y^2z, x^2yz^2, x^3y, x^2z^2, xy^2z, x^2z, x^2$
- (grevlex) $x^2y^2z, x^3z^2, x^2yz^2, x^3y, xy^2z, x^2z^2, x^2z, x^2$

2. Division Algorithms and Gröbner Bases

Whenever we have a monomial ordering, we have a notion of leading coefficient, namely the highest nonzero term according to the ordering. Given an ideal $(f_1, \dots f_n)$, we would like to run the following division algorithm: Take a polynomial g, and compare leading coefficients with each f_i. If the leading coefficient of f_i divides one of g's terms, subtract the corresponding multiple of f_i from g. If you are not capable of doing this with any of the f_i, then set the leading term aside as a remainder, and continue with the rest of the polynomial. As the monomial ordering is well-ordered, this will stop eventually, ie. none of the leading terms of the f_i will divide any of what is left of g. We would like this process to yield a unique remainder for any two members of the same coset of the ideal so we can do computations in the quotient. Given arbitrary generators of an ideal, this may not always work unfortunately.

For example, consider $(x+y, x^2+xy+y^2)$ with the lexicographical order $x > y$. We can try to reduce the polynomial x^2+xy in two ways. First we can subtract $x(x+y)$ from it to get 0, after which we are done. Or we can subtract $1(x^2+xy+y^2)$ from it to get $-y^2$, after which we are done. Note that we got different remainders, which is not what we'd like. To fix this, we should choose a different set of generators for the ideal that also generate the ideal of leading coefficients, for example $(y^2, x+y)$. If we were to run the algorithm on this set of generators, we would get 0 both times. This is because $(y^2, x+y)$ is a Gröbner basis.

Definition 2.1. *If f is a polynomial, $LT(f)$ denotes its leading term (with the coefficient). If I is an ideal $LT(I)$ is the ideal of leading terms. A **Gröbner basis** G of I is a nonempty subset of I whose leading terms generate $LT(I)$.*

Proposition 2.2. *If G is a Gröbner basis of I, then the division algorithm yields a unique representative for each coset of $R[x_1, \dots, x_n]/I$. In particular, it is 0 iff the element is in the ideal, so G generates I.*

Proof. Suppose we have two remainders of elements from the same coset, r_1, r_2 and we subtract them. We'll get something in I but if it is nonzero, we can apply the algorithm to it as G is a Gröbner basis. But any term we remove must have come from either r_1 or r_2, which is a contradiction, as it means the division algorithm was not yet complete on r_1 or r_2. If r_1 is in the ideal, it must be 0 or else the algorithm again is not complete. □

By Proposition 2.2 and the proof of the Hilbert Basis Theorem (except now we are working with arbitrary monomial orderings) we get that every ideal has a Gröbner basis. How can we actually compute it? The Buchberger Criterion gives a way to do this. From now on, we will work over a field K.

To motivate this, consider the example before with $(x+y, x^2+xy+y^2)$. We can look at the leading terms, x and x^2, and take the LCM, x^2. We can then add in the extra term $x(x+y) - 1(x^2+xy+y^2) = -y^2$. Adding this in to our list of generators, we do get a Gröbner basis. The Buchberger Criterion says this strategy will always work.

First we will set up some notation. Fix a set of generators of I, G. We say $f \mapsto r$ to mean that applying the algorithm to f with G yields r as the remainder. If f, g are polynomials,

then we let $LCM = LCM(LT(f), LT(g))$ denote the monic that is the LCM of the leading terms of f and g. We define $S(f,g) = \frac{LCM}{LT(f)}f - \frac{LCM}{LT(g)}g$. We would like to say that any missing generators to make a Gröbner basis will be produced by repeatedly adding the $S(f,g)$ until they are no longer needed.

Before we prove the Buchberger Criterion, a simple lemma:

Lemma 2.3. *Suppose that $f_1 \dots f_n$ are polynomials of the same leading monomial. Then if $h = \sum_1^n s_i f_i, s_i \in K$ has leading term smaller than the f_i, then $h = \sum_1^{n-1} r_i S(f_i, f_{i+1}), r_i \in K$.*

Proof. WLOG assume the f_i are monic. Note $S(f_i, f_{i+1})$ is just $f_i - f_{i+1}$. Then write $\sum_1^n s_i f_i$ as $\sum_1^{n-1} \left(\sum_1^i s_i\right)(f_i - f_{i+1}) + \left(\sum_1^n s_i\right) f_n$. Each of the terms in the first sum has leading term smaller than the f_i, so $\left(\sum_1^n s_i\right) f_n = 0$, and we get that $h = \sum_1^n s_i f_i = \sum_1^{n-1} \left(\sum_1^i s_i\right) S(f_i, f_{i+1})$. □

Theorem 2.4 (Buchberger Criterion)**.** *$G = \{f_1 \dots f_n\} \subset I$ is a Gröbner basis iff each $S(f_i, f_j) \mapsto 0$ and if G generates I.*

Proof. The only if follows from Proposition 2.2. Now suppose each $S(f_i, f_j) \mapsto 0$ and G generates I. Take any $f \in I$, and apply the division algorithm to get a remainder f'. Choose a representation $f' = \sum_1^n g_i f_i$ such that the maximal leading term of each summand is minimal, say α. Suppose $f' \neq 0$, so that $\alpha > LT(f)$. We will try to find a smaller representation using the fact that $S(f_i, f_j) \mapsto 0$.

We have:

$$\begin{aligned} f' &= \sum_1^n g_i f_i \\ &= \sum_{LT(g_i f_i) = \alpha} LT(g_i) f_i + \sum_{LT(g_i f_i) = \alpha} (g_i - LT(g_i)) f_i + \sum_{LT(g_i f_i) < \alpha} g_i f_i \\ &= \sum s_i S(LT(g_i) f_i, LT(g_j) f_j) + \sum_{LT(g_i f_i) = \alpha} (g_i - LT(g_i)) f_i + \sum_{LT(g_i f_i) < \alpha} g_i f_i \end{aligned}$$

The second two sums have all their terms smaller than α so Lemma 2.3 applies to the first sum, which is what has been done in the last step.

However now we have a contradiction as $S(LT(g_i) f_i, LT(g_j) f_j)$ is a monomial multiplied with $S(f_i, f_j)$ so we have $S(LT(g_i) f_i, LT(g_j) f_j) \mapsto 0$ so it can be written as a linear combination of the f_i with degrees of each term at most that of $S(LT(g_i) f_i, LT(g_j) f_j)$, which in particular is smaller than α. This contradicts minimality of α. □

Buchberger's Criterion allows us to produce Gröbner bases. In particular, given a set of generators $\{f_1 \dots f_n\}$ we can compute the $S(f_i, f_j)$, and reduce them. If they are all zero, we have a Gröbner basis, otherwise we add the remainder to the list and repeat until the criterion is satisfied. Now that we can find Gröbner bases, we can compute in quotient rings, and make nontrivial statements about the ideals that we are working with. In particular, this gives an effective Nullstellensatz, as an ideal is trivial iff 1 is in a Gröbner basis of it.

3. Reduced Gröbner bases and Applications

Let's work this out for $(x+y, x^2+xy+y^2)$, $x > y$ as before. We saw $S(x+y, x^2+xy+y^2) = -y^2$ so we can add y^2 to our list of generators. $S(x+y, y^2) = y^2(x+y) - xy^2 = y^3 \mapsto 0$ and $S(x^2+xy+y^2, y^2) = y^2(x^2+xy+y^2) - x^2y^2 = xy^3+y^4 \mapsto 0$, so we see $(x+y, x^2+xy+y^2, y^2)$ is a Gröbner basis. Note however that the leading term of x^2+xy+y^2 has the leading term of $x+y$ as a divisor. This means it can be removed by Proposition 2.2. We are left with $(x+y, y^2)$. This is a minimal Gröbner basis as no more terms can be removed.

Definition 3.1. *A **minimal Gröbner basis** is one with a minimal number of elements.*

Proposition 3.2. *We can always get a minimal Gröbner basis from a Gröbner basis as above, by removing redundant terms. The leading coefficients and number of terms of a minimal Gröbner basis for a fixed ideal I is unique.*

Proof. This follows from the observation that for an ideal generated by monomials, there is a unique minimal monic generating set of monomials. □

Note that minimal Gröbner bases are not unique even though their size and leading coefficients are. For example, $(x+y, y^2)$ and $(x+y+y^2, y^2)$ are both Gröbner bases of the same ideal. To get true uniqueness we need a slightly stronger condition.

Definition 3.3. *A **reduced Gröbner basis** is one in which none of the leading terms of any element divide any of the terms of the others and the leading terms are monic.*

A reduced Gröbner basis is in particular a minimal Gröbner basis. For example, $(x+y, y^2)$ is an example, and $(x+y+y^2, y^2)$ is a non-example. We can always make a Gröbner basis reduced by performing the division algorithm on a term with the rest of the terms until it is reduced. For example, performing it on $(x+y+y^2, y^2)$, we get $x+y+y^2-1(y^2) = x+y$ as the result for $x+y$, and y^2 stays as it is. In particular we get back $(x+y, y^2)$. Here is the reason we introduced reduced Gröbner bases:

Proposition 3.4. *Every ideal has a unique reduced Gröbner basis.*

Proof. By Proposition 3 we know the leading coefficients and number of elements are unique. So given two reduced Gröbner bases $\{f_1, \ldots, f_n\}, \{g_1, \ldots, g_n\}$ we can subtract terms with the same leading coefficient and apply the division algorithm to see that we must get 0 or else one of the Gröbner bases isn't reduced. □

This yields a way to check if two ideals are equal, namely computing their reduced Gröbner bases. For example, the ideals (xy^2+y^3+x+y, y^2) and $(x+y, x^2+xy+y^2)$ have the same reduced Gröbner basis, $(x+y, y^2)$ so are the same.

We can also use Gröbner bases to try to solve systems of polynomial equations, similarly to the Gauss-Jordan elimination that is used to solve systems of linear equations. This is the beginning of elimination theory, something developed by Emmy Noether and her students. To do this, we must choose a lexicographical ordering, which will specify in which order we eliminate variables. Then we have:

Proposition 3.5 (Elimination)**.** *Suppose our ordering is (lex) $x_1 > \cdots > x_n$. Then if G is a Gröbner basis for I, then $G \cap K[x_2, ..., x_n]$ is a Gröbner basis of $I \cap K[x_2, \ldots, x_n]$.*

Proof. Consider using the division algorithm of G on $f \in I \cap K[x_2, \ldots, x_n]$. As $x_1 > x_2$ we will never use any elements of G with x_1, but will still get to 0 as G is a Gröbner basis. Then in the division algorithm we must be using only elements of $G \cap K[x_2, \ldots, x_n]$ so by Proposition 2.2 we are done. □

This allows us to solve systems of equations when there are finitely many solutions. For example, consider the ellipse $2x^2 + 2xy + y^2 - 2x - 2y$ and the circle $x^2 + y^2 - 1$. We can find their points of intersection via elimination. In particular, we would like to find zeros of the ideal $2x^2 + 2xy + y^2 - 2x - 2y, x^2 + y^2 - 1$. To do this, we compute its Gröbner basis under the ordering $x > y$, giving $(2x + y^2 + 5y^3 - 2, 5y^4 - 4y^3)$. Then we eliminate x and solve $5y^4 - 4y^3 = 0$, which gives $y = 0, \frac{4}{5}$. We then substitute this in for y to find the corresponding solutions in x, giving us $(1, 0), (-\frac{3}{5}, \frac{4}{5})$ as our two points of intersection.

Elimination can also be used to compute intersections of ideals (sums and products are easy). In order to do so, we introduce an auxiliary variable t and eliminate it. In particular, $I \cap J = K[x_1, \ldots, x_n] \cap (tI + (1 - t)J)$, and we can compute the right hand side using elimination. To see the equality above, note that something of the form $tf + (1-t)g$ doesn't involve t iff $f = g$.

Here is an example of computing $I \cap J$ using elimination. Suppose we want to find $(y^2, xy, x^2) \cap (x)$. We consider $(ty^2, txy, +tx^2, -tx + x)$ and find a Gröbner basis with the ordering $t > x > y$. We get $(tx - x, ty^2, x^2, xy)$ as our reduced Gröbner basis, so (xy, y^2) is the intersection.

Elimination has other computational applications as well. For example, one may want to saturate an ideal I with respect to a polynomial f. This can be done by considering the ideal $I + (1 - tf)$ and eliminating t. The reason this works is because by adding in $1 - tf$ we are sending I to the ideal it corresponds to in the localization, and by eliminating t we are intersecting it with our original ring, and by the correspondence of ideals for localization, this yields the saturation.

We can use this idea of localization to also tell if $f \in \sqrt{I}$. In particular, $f \in \sqrt{I}$ iff $I + (1 - tf) = (1)$ and this condition can be computed by looking at the Gröbner basis of $I + (1 - tf)$.

Finally we can compute ideal quotients $(I : J)$ using elimination. First note that it suffices to consider J principle as $(I : (f_1, \ldots, f_n)) = \cap_1^n (I : (f_i))$. Then note that if $G \subset I \cap (f_i)$ is a generating set of $I \cap (f_i)$, then $\frac{G}{f_i} := \{\frac{g}{f_i} | g \in G\}$ generates $(I : (f_i))$. Thus we can compute this using Gröbner bases.

Some final remarks: This is just the beginning of what Gröbner bases are good for. For example, they can compute radicals of general ideals, although this is more complicated (first reduce to 0-dimensional case, then treat perfect and non-perfect fields separately). They can also compute the primary decomposition of an ideal. The theory of Gröbner bases also extends to rings other than finitely generated K-algebras, for example there is an analogous theory for polynomial rings over principle ideal rings.