Groebner Bases

October 24, 2016

1 Introduction

The previous introductory chapter shed light on the connections between the algebra behind the polynomial ring $F[x_1, \cdots, x_n]$ and the geometry behind affine algebraic varieties. In this chapter, we'll go over the method of Groebner bases, which will allow us to solve many problems about polynomial ideals algorithmically. Specifically, we'll spend this chapter focusing on the following four problems:

1. Ideal description problem: Does every polynomial ideal $I \subset F[x_1, \cdots, x_n]$ have a finite generating set, so that we can write $I = \langle f_1, \cdots, f_s \rangle$ for some $f_1, \cdots, f_s \in F[x_1, \cdots, x_n]$?
   In the last chapter, we solved this problem for $n = 1$ by showing that every ideal $I \subset F[x]$ can be written $I = \langle g \rangle$ for some $f \in F[x]$.

2. Ideal membership problem: Given a polynomial $f \in F[x_1, \cdots, x_n]$ and ideal $I = \langle f_1, \cdots, f_s \rangle$, determine if $f \in I$. This is closely related to the problem of determining if $\mathbf{V}(f_1, \cdots, f_s) \subset \mathbf{V}(f)$.
   We also solved this problem for $n = 1$ in the last chapter, by showing that $f \in \langle g \rangle$ if and only if g divides f, which can be determined algorithmically from the polynomial division algorithm.

3. Polynomial equations: Find all solutions to the system of polynomial equations $f_1(x_1, \cdots, x_n) = \cdots = f_s(x_1, \cdots, x_n) = 0$, which is equivalent to finding an explicit description of $\mathbf{V}(f_1, \cdots, f_s)$.
   Linear algebra offers a solution to this problem when $\deg(f_i) = 1$ and $f_i \in F[x]$, for $1 \leq i \leq s$, since then the system of equations reduces to a system of linear equations which can be solved algorithmically with matrix algebra.

4. Implicitization problem: This problem is the inverse of the polynomial equations problem. Given the parametric representation of $V \in F^n$
   $$\begin{aligned} x_1 &= g_1(t_1, \cdots, t_m) \\ &\vdots \\ x_n &= g_n(t_1, \cdots, t_m) \end{aligned}$$
   for polynomials g_i, it follows that V is either an affine variety or part of an affine variety; find an implicit description (i.e. a system of polynomial equations) that determines this variety.

2 Orderings on Monomials

Many standard algorithmic techniques for solving the four main problems of this chapter, such as the division algorithm or matrix row reduction (for linear polynomials in one variable) rely on the notion of ordering monomials, usually by decreasing order of degree if the monomials are all in one variable. In this section, we'll try to find a good ordering for general monomials in many variables, by first defining some desirable properties the ordering should have and then by defining several examples of orderings that satisfy those properties.

Firstly, we require that the ordering $>$ be **total**, so that for any two monomials in $x^\alpha, x^\beta \in F[x_1, \cdots, x_n]$, either $x^\alpha > x^\beta, x^\beta > x^\alpha$, or $x^\alpha = x^\beta$. This property allows us to unambiguously arrange the terms of a polynomial in descending or ascending order, which is useful in many polynomial algorithmic contexts.
Next, we also require that the ordering be preserved by the standard arithmetic operations of addition and multiplication. Being invariant under addition isn't difficult to have seeing as we can simply rearrange like terms, but multiplication poses a problem since monomials with different degrees can be multiplied to produce a completely different monomial. To have multiplication preserve our ordering, we would like for the product of the largest monomial terms in two polynomials to be the largest monomial term in the product of the two polynomials, i.e. if x^α is the leading term of polynomial f and x^β is the leading term of polynomial g, then $x^\alpha x^\beta$ is the leading term of polynomial fg. To guarantee this, we require that $x^\alpha > x^\beta \to x^\alpha x^\gamma > x^\beta x^\gamma$.

Finally, we would also like the ordering to be a *well ordering*, so that it is, in some sense, complete. More precisely, the ordering is well-ordering if every non-empty subset of the ordered set has a least element under the ordering. The reason this is a desirable property is made clear by the following theorem.

(Theorem) Alternate formulation of well-ordering: *An order relation $>$ on $\mathbb{Z}_{\geq 0}^n$ is well-ordering if and only if every strictly decreasing sequence in $\mathbb{Z}_{\geq 0}^n$*

$$\alpha_1 > \alpha_2 > \cdots$$

eventually terminates.

• *Proof*: We prove the contrapositive; first assume that $>$ is not a well-ordering. We will prove that there exists an infinite strictly decreasing sequence. Since $>$ is not well-ordering, there's some non-empty subset $S \subset \mathbb{Z}_{\geq 0}^n$ which has no least element.

Pick an $\alpha_1 \in S$. Since α_1 is not the least element of S, $\exists \alpha_2 \in S$ such that $\alpha_1 > \alpha_2$. The same logic holds if we first pick α_2, so we can find an α_3 such that $\alpha_1 > \alpha_2 > \alpha_3$. We will never be able to find a least element of S, since it's not well-ordered, and so we may continue this forever. Thus, $\alpha_1 > \alpha_2 > \cdots$ is an infinite strictly decreasing sequence.

Conversely, suppose that there exists an infinite strictly decreasing sequence $\alpha_1 > \alpha_2 > \cdots$ in $\mathbb{Z}_{\geq 0}^n$ under $>$. Then the subset $\{\alpha_1, \alpha_2, \cdots\}$ is a non-empty subset with no least element, which shows that $>$ is not a well-ordering. □

The importance of the above theorem is that if our monomial ordering is a well-ordering, then it will allow us to prove that many of the algorithmic techniques we use to solve problems, like the ones above, terminate. This is because many algorithms we use, such as the division algorithm, iteratively reduce some term in a polynomial.

Moreover, because a monomial $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is completely determined by the exponents $(\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$, we can specify our orderings over integer tuples. These properties lead to the following definition.

(Definition) Monomial ordering: *A **monomial ordering** $>$ on $F[x_1, \cdots, x_n]$ is a relation on $\mathbb{Z}_{\geq 0}^n$ satisfying*

1. *$>$ is a total ordering.*
2. *If $\alpha > \beta$ then $\alpha + \gamma > \beta + \gamma$, for $\alpha, \beta, \gamma \in \mathbb{Z}_{\geq 0}^n$*
3. *$>$ is a well-ordering on $\mathbb{Z}$, i.e. every non-empty subset of $\mathbb{Z}_{\geq 0}^n$ has a least element under $>$.*

Let's now turn to some common examples of monomial orderings. The first one we look at is a very intuitive and familiar ordering, extensively used in the real world to order strings of symbols such as words and titles.

(Definition) Lexicographic order: *Let $\alpha = (\alpha_1, \cdots, \alpha_n), \beta = (\beta_1, \cdots, \beta_n)$ be elements of $\mathbb{Z}_{\geq 0}^n$. Then we define the **lexicographic order** by $>_{lex}$, where*

$$\alpha >_{lex} \beta \iff \exists i \in \{1, \cdots, n\} \text{ s.t. } \alpha_i > \beta_i \text{ and } \alpha_j = \beta_j, \forall j < i$$

The fact that the lexicographic ordering is a monomial ordering follows easily. Notice that there are many lexicographic orderings for monomials, depending on how we order the indeterminates $x_1, \cdots, x_n$.

One way that the lexicographic ordering breaks from the more intuitive or standard way of ordering monomials is that if doesn't take the monomials' degrees into account; a variable dominates any combination of smaller variables, regardless of degree. For example, we have $x >_{lex} y^{10} z^{15}$. To account for degree, we define the following monomial ordering, which extends lexicographic ordering.

(Definition) Graded lexicographic order: *Let $\alpha = (\alpha_1, \cdots, \alpha_n), \beta = (\beta_1, \cdots, \beta_n)$ be elements of $\mathbb{Z}_{\geq 0}^n$. Then we define the **graded lexicographic order** by $>_{grlex}$, where*

$$\alpha >_{grlex} \beta \iff |\alpha| > |\beta| \text{ or } |\alpha| = |\beta|, \alpha >_{lex} \beta$$

• *Motivation*: Graded lexicographic order first orders monomials by total degrees, and then breaks ties with lexicographic order. This is a good compromise between lexicgraphically ordering monomials and ordering monomials by degree.

Another less intuitive but algorithmically useful ordering is the graded reverse lexicographic order, denoted $>_{grevlex}$, which, like graded lexicographic order, first orders monomials by degree, and then applies reverse lexicographic order to break ties. Which order is used during an algorithmic computation of a problem is an important choice; most computer algebra systems support lexicographic order by default, but also allow for the choice of graded lexicographic order or graded reverse lexicographic order. Now that we have the necessary ideas to order the terms of a polynomial, we can extend some useful definitions from polynomials in one variable to polynomials in several variables.

(Definition) Multidegree: *The **multidegree** of a polynomial $f = \sum_\alpha a_\alpha x^\alpha \in F[x_1, \cdots, x_n]$ with respect to the monomial order $>$ is given by*

$$\text{multideg}(f) := \max\left\{\alpha \in \mathbb{Z}^n_{\geq 0} \text{ where } a_\alpha \neq 0\right\}$$

*We also define the **leading coefficient** of f with*

$$\text{LC}(f) := a_{\text{multidef(f)}}$$

*and the **leading monomial** of f with*

$$\text{LM}(f) := x^{\text{multidef}(f)}$$

*Putting the two together, we finally define the **leading term** of f with*

$$\text{LT}(f) := \text{LC}(f) \cdot \text{LM}(f)$$

3 Division Algorithm for Polynomials in Many Variables

We've seen that the division algorithm provides a means of solving the ideal membership problem for polynomials in one variable; in this section, we extend the division algorithm to polynomials in $F[x_1, \cdots, x_n]$. In the most general case, we wish to divide $f \in F[x_1, \cdots, x_n]$ by $f_1, \cdots, f_s \in F[x_1, \cdots x_n]$, which is to say, express

$$f = a_1 f_1 + \cdots + a_s f_s + r, a_1, \cdots, a_s, r \in F[x_1, \cdots, x_n]$$

where we'll use monomial orderings to characterize the remainder and extend the requirement that $\deg(r) < \deg(g)$ for $f = qr + g$ in $F[x]$.
The idea behind the extended division algorithm is the same as the original algorithm - to cancel the leading term of f by multiplying some f_i by the appropriate monomial and subtracting, then repeating. One difference from the single variable case is that in several variables, the algorithm no longer necessarily terminates when the leading terms of any of the divisors don't device the leading term of the current dividend; rather, we can move the terms of the dividend around until one of its terms is divisible by one of the leading terms of the divisors, putting the moved terms as part of the remainder. We now formalize this idea.

(Theorem) Division algorithm in several variables: *Let $>$ be a monomial order. For any $f_1, \cdots, f_s \in F[x_1, \cdots, x_n]$, and $f \in F[x_1, \cdots, x_n]$, we can write*

$$f = a_1 f_1 + \cdots + a_s f_s + r, a_i, r \in F[x_1, \cdots, x_n]$$

where either $r = 0$ or r is a linear combination of of monomials, none of which is divisible by any of $LT(f_1), \cdots LT(f_s)$. Moreover, if $a_i f_i \neq 0$, then we have multideg$(f) \geq$ multideg$(a_i f_i)$.

• *Proof*: We prove the theorem by outlining the division algorithm for polynomials in $F[x_1, \cdots, x_n]$ and proving its correctness.

procedure DIVISION$((f_1, \cdots, f_s), f)$
  $a_1 = \cdots = a_s = r = 0$
  $p \leftarrow f$
  while $p \neq 0$ **do**
    $i \leftarrow 1$
    done $\leftarrow$ **false**
    while $i \leq s$ **and** *done* $=$ **false do**
      if $\text{LT}(f_i)$ divides p **then**
        $a_i \leftarrow a_i + \frac{\text{LT}(p)}{\text{LT}(f_i)}$
        $p \leftarrow p - \frac{\text{LT}(p)}{\text{LT}(f_i)} f_i$
        done $\leftarrow$ **true**
      else
        $i \leftarrow i + 1$
      end if
    end while
    if *done* $=$ **false then**
      $r \leftarrow r + \text{LT}(p)$
      $p \leftarrow p - \text{LT}(p)$
    end if
  end while

return $(a_1, \cdots, a_s)$
end procedure

The intuition behind this algorithm is that at each iteration, p represents the *intermediate dividend*, while r represents the incrementally built remainder. Every time $p \neq 0$ and $\text{LT}(p)$ is not divisible by any of the leading terms of the divisors, we move $\text{LT}(p)$ to the remainder column by adding it to r, and continue to the new leading term of p, proceeding onwards as usual the same way as in one variable. The boolean flag *done* is used to identify when the leading term of the intermediate dividend should be transferred to the remainder. Since there are multiple divisors, if more than one has a leading term that divides $\text{LT}(p)$, the choice is arbitrary as to which to use.

To prove the correctness of the algorithm, we'll show that at each iteration, the statement

$$f = a_1 f_1 + \cdots + a_s f_s + p + r$$

holds true, and then that p must eventually become 0. Initially the statement trivially holds, since we have $a_i = r = 0, p = f$, so we can use a proof by induction to prove the statement in the loop. If the above statement holds and the next iteration of the loop is a division step, then $\text{LT}(f_i)|p$ for some i. Then the only variables whose values change are a_i and p, but from the identity

$$a_i f_i + p = \left(a_i + \frac{\text{LT}(p)}{\text{LT}(f_i)}\right) + \left(p - \frac{\text{LT}(p)}{\text{LT}(f_i)} f_i\right)$$

shows that the quantity $f = a_1 f_1 + \cdots + a_i f_i + \cdots + a_s f_s + p + r$ is unchanged. If, instead, the iteration is a remainder step, then the only variables changed are p and r, and the identity

$$p + r = (p - \text{LT}(p)) + (r + \text{LT}(p))$$

shows that the quantity above is again unchanged.

Finally, to show that the algorithm halts, we show that eventually $p = 0$. Notice that in each iteration of the loop, the multidegree of p drops, or p becomes 0, since we subtract off the leading term of p in each iteration. Thus, the loop iterations form a strictly decreasing sequence of numbers representing the multidegree of p, which must eventually hit 0. □

• Note that one key difference from the one variable case is that in many variables the remainder is not necessarily unique, and depends on the order of divisors.

Recall that the motivation for defining a division algorithm in $F[x_1, \cdots, x_n]$ was the fact that the division algorithm in $F[x]$ was instrumental in solving the ideal membership problem. It's clear that if polynomials $f_1, \cdots, f_s \in F[x_1, \cdots, x_n]$ divide $f \in F[x_1, \cdots, x_n]$, then $f \in \langle f_1, \cdots, f_s \rangle$ by definition. Thus, $r = 0$ in the division algorithm is a sufficient condition for ideal membership. However, it is not a necessary condition, since the remainder is not unique.

4 Monomial Ideals and Dickson's Lemma

In this section, we consider the ideal description problem in the special case of monomial ideals. First, some preliminary definitions.

(Definition) Monomial ideal: *An ideal $I \subset F[x_1, \cdots, x_n]$ is a **monomial ideal** if it's generated by monomials; that is, if there is a subset $A \subset \mathbb{Z}^n_{\geq 0}$ such that*

$$I = \left\{ \sum_{\alpha \in A} h_\alpha x^\alpha \text{ where } h_\alpha \in F[x_1, \cdots, x_n] \right\}$$

• *Notation*: Then we write $I = \langle x^\alpha, \alpha \in A \rangle$.

(Theorem) Monomial ideal membership for monomials: *Let $I = \langle x^\alpha, \alpha \in A$ by a monomial ideal. Then $x^\beta \in I$ if and only if $\exists \alpha \in A$ s.t. $x^\alpha | x^\beta$.*

• *Proof*: The necessary condition is trivial, since if x^α divides x^β for some $\alpha \in A$ then by the definition of an ideal, we have $x^\beta = \sum_{\alpha' \neq \alpha \in A} 0 \cdot x^{\alpha'} + g x^\alpha$ for monomial $g \in F[x_1, \cdots, x_n] \rightarrow x^\beta \in I$. Conversely, if $x^\beta \in I$, then $x^\beta = \sum_{i=1}^s h_i x^{\alpha_i}, \alpha_i \in A, h_i \in F[x_1, \cdots, x_n]$. If we expand h_i as a linear combination of monomials, then every term on the right side of the equation is divisible by some x^{α_i}, and therefore so is x^β. □

Monomial ideals have a useful and intuitive geometric description as well. Notice that x^β is divisible by x^α precisely when $x^\beta = x^\alpha x^\gamma$, which is to say, when $\exists \gamma \in \mathbb{Z}^n_{\geq 0}$ s.t. $\beta = \alpha + \gamma$. This means that the set

$$\alpha + \mathbb{Z}^n_{\geq 0} := \left\{ \alpha + \gamma, \gamma \in \mathbb{Z}^n_{\geq 0} \right\}$$

consists of the exponents of the monomials (which fully determines the monomial) divisible by x^α. It follows that

$$\langle x^\alpha, \alpha \in A\rangle = \bigcup_{\alpha\in A} \left(\alpha + \mathbb{Z}^n_{\geq 0}\right)$$

where $x^\alpha = x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ as usual.
$\alpha + \mathbb{Z}^n_{\geq 0}$ can be geometrically visualized as the lattice of positive integer points in n-dimensional space, with the origin translated to α; $\langle x^\alpha, \alpha \in A\rangle$, then, is the union of each translated lattice of positive integer points.
We've seen that, unsurprisingly, the ideal membership problem for monomial ideals is trivial when considering monomials, but we can also solve the ideal membership problem of determining if a polynomial is in a monomial ideal by analyzing the polynomials monomials.

(Theorem) Monomial ideal membership for polynomials: *Let I be a monomial ideal and $f \in F[x_1, \cdots, x_n]$. Then the following statements are equivalent.*

1. $f \in I$
2. *Every term of f lies in I.*
3. *f is a k-linear combination of monomials in I.*

• *Proof*: The fact that (3) implies (2) follows by definition of an ideal generated by monomials, as does (2) implies (1). (1) implies (3) also follows by definition. □
It follows as a corollary that two monomial ideals are the same if and only if they contain the same monomials.

We now have the machinery to prove the main result of this section, that all monomial ideals are finitely generated.

(Theorem) Dickson's lemma: *Let $I = \langle x^\alpha, \alpha \in A\rangle \subset F[x_1, \cdots, x_n]$ be a monomial ideal. Then $\exists \alpha_1, \cdots, \alpha_n \in A$ s.t. $I = \langle x^{\alpha_1}, \cdots, x^{\alpha_s}\rangle$, i.e. I has a finite basis.*

• *Proof*: We prove the theorem by induction on n. The base case is simple - if I is a monomial ideal over $F[x]$, then $I = \langle x_1^\alpha, \alpha \in A\rangle$. Let $\beta := \min(A)$. Then $x_1^\beta | x_1^\alpha$, and so $I = \langle x_1^\beta\rangle$.

Now suppose the theorem is true for $F[x_1, \cdots, x_{n-1}]$ and consider $F[x_1, \cdots, x_{n-1}, y]$. We can write polynomials in $F[x_1, \cdots, x_{n-1}, y]$ as $x^\alpha y^m, \alpha \in \mathbb{Z}^{n-1}_{\geq 0}, m \in \mathbb{Z}_{\geq 0}$. Now let $I \subset F[x_1, \cdots, x_{n-1}, y]$ be a monomial ideal, so we wish to show that I is finitely generated. First we introduce the notion of a "projection" of I into $F[x_1, \cdots, x_{n-1}]$: let J be the ideal over $F[x_1, \cdots, x_{n-1}]$ generated by all the monomials x^α such that $x^\alpha y^m \in I$, for some $m \in \mathbb{Z}_{\geq 0}$. By the inductive hypothesis, J is finitely generated, so $J = \langle x^{\alpha(1)}, \cdots, x^{\alpha(n-1)}\rangle$, and by definition of J, $x^{\alpha_i} y^{m_i} \in I$.

Let $m := \max_i m_i$, and define for $1 \leq k < m$ the ideal $J_k \subset F[x_1, \cdots, x_{n-1}]$ generated by $x^\beta y^k$ for any β; intuitively, J_k is the "slice" of I that's generated only by monomials divisible by y^k. Again, by the inductive hypothesis, J_k is finitely generated: $J_k = \langle x^{\alpha_k(1), \cdots, \alpha_k(s_k)}\rangle$. We have now constructed the projection of I down into $n-1$ variables as well as the slices of I iteratively increasing from 1 to the maximum power of y for which y is in I. We wish to show that J taken together with the J_k's completely determine I, based on the intuition that given that I is a monomial ideal in n variables, J is a subset of I which "takes care" of determining all monomials only in $n-1$ variables, and to "take care" of the remaining monomials in n variables we can iteratively use $J_k \subset I$ to account for precisely those monomials in n variables which consist of monomials in $n-1$ variables (i.e. in J) with an extra factor of the n^{th} variable, y^k, all the way up to the maximum power of y. In this fashion, we can inductively "create" I by re-using the monomial ideal from $n-1$ variables and taking care of the final case of n variables by iterating through all possible powers of the n^{th} variable.

To formally prove this, we must show that I is generated by the following monomials:

$$\begin{aligned}
x^{\alpha(1)}y^m, \cdots, x^{\alpha(s)}y^m &\text{ (from } J\text{)}\\
x^{\alpha_0(1)}, \cdots, x^{\alpha_0(s_0)} &\text{ (from } J_0\text{)}\\
x^{\alpha_1(1)}y, \cdots, x^{\alpha_1(s_1)} &\text{ (from } J_1\text{)}\\
&\vdots\\
x^{\alpha_{m-1}(1)}y^{m-1}, \cdots, x^{\alpha_{m-1}(s_{m-1})}y^{m-1} &\text{ (from } J_{m-1}\text{)}
\end{aligned}$$

First, notice that for $x^\alpha y^p \in I$, $p \geq m$ implies that some monomial in J, due to the way we constructed J divides $x^\alpha y^p$. If instead $p \leq m$ then by the way we constructed J_p, there's some monomial in J_p which divides $x^\alpha y^p$. By monomial ideal membership for monomials, this means that every element of I lies in the ideal generated by the above monomials, which means I is equivalent to the ideal generated by the above monomials, which implies that I is finitely generated. □

5 Hilbert Basis Theorem and Groebner Bases

In this section, we will find a full solution to the ideal description problem. This will involve defining a canonical basis for an ideal, which is guaranteed to have certain "good" properties relative to the division algorithm. This will rely on the key idea that every $f \in F[x_1, \cdots, x_n]$ has a unique leading term with respect to some monomial ordering. With that in mind, we can make the following useful definition.

(Definition) Ideal of leading terms: *Let $I \neq \{0\}$ be a polynomial ideal over $F[x_1, \cdots, x_n]$. Then we define the* ***set of leading terms*** *of I with*

$$\text{LT}(I) := \{\text{LT}(f), f \in I\} = \{cx^\alpha \text{ where } \exists f \in I \text{ s.t. } \text{LT}(f) = cx^\alpha\}$$

Moreover, we define the ***ideal of leading terms*** *of I, denoted $\langle LT(I)\rangle$, as the ideal generated by $LT(I)$.*

It's necessary to note one subtlety here. Given $I = \langle f_1, \cdots, f_s\rangle$, the fact that $\text{LT}(f_i) \in \text{LT}(I) \subseteq \langle \text{LT}(I)\rangle$ implies that $\langle \text{LT}(f_1), \cdots, \text{LT}(f_s)\rangle \subseteq \langle \text{LT}(I)\rangle$. However, it's not always the case that $\langle \text{LT}(f_1), \cdots, \text{LT}(f_s)\rangle = \langle \text{LT}(I)\rangle$; in general, the latter might be strictly larger.
Next, we will connect this section to the previous one by showing that $\langle \text{LT}(I)\rangle$ is a monomial ideal.

(Theorem) Ideal of leading terms is monomial: *Let $I \subset F[x_1, \cdots, x_n]$ be an ideal. Then $\langle LT(I)\rangle$ is a monomial ideal, and $\exists g_1, \cdots, g_t \in I$ s.t. $\langle LT(I)\rangle = \langle LT(g_1), \cdots, LT(g_t)\rangle$.*

• *Proof*: Proving that $\langle \text{LT}(I)\rangle$ is a monomial ideal is trivial. Consider the set $\{\text{LM}(g), g \in I - \{0\}\}$. This set generates the ideal $\langle \text{LM}(g), g \in I - \{0\}\rangle$, but since $\text{LM}(g)$ and $\text{LT}(g)$ differ only by a constant factor, it follows that $\langle \text{LM}(g), g \in I - \{0\}\rangle = \langle \text{LT}(g), g \in I - \{0\}\rangle$, which shows that $\langle \text{LT}(I)\rangle$ is a monomial ideal, generated by the leading monomials of the elements of I. The fact that $\langle \text{LT}(I)\rangle$ is finitely generated follows from Dickson's lemma. □

In investigating Dickson's lemma and the polynomial division algorithm, we made significant progress towards the ideal description and ideal membership problems. We now have the machinery to prove one of the most central results in this section - that every ideal, not just monomial ideals, are finitely generated.

(Theorem) Hilbert basis theorem: *Every ideal $I \subset F[x_1, \cdots, x_n]$ has a finite generating set, so $I = \langle g_1, \cdots, g_t\rangle$ for some $g_1, \cdots, g_t \in I$.*

• *Proof*: The proof is quite elegant and natural. Given an ideal $I \neq \{0\}$, we'll construct a finite basis for I by showing that $I = \langle g_1, \cdots, g_t\rangle$, where $\langle \text{LT}(I)\rangle = \langle \text{LT}(g_1), \cdots, \text{LT}(g_t)\rangle$, as guaranteed by the above theorem.

Obviously, $\langle \text{LT}(g_1), \cdots, \text{LT}(g_t)\rangle \subset I$, so let's prove the other direction. If $f \in I$, then we can apply the polynomial division algorithm to divide f by $g_1, \cdots, g_t$, obtaining

$$f = a_1 g_1 + \cdots + a_t g_t + r$$

for some $a_i \in I$ and where no term of r is divisible by any of $\text{LT}(g_i)$. We'll show that $r = 0$, proving that $f \in \langle g_1, \cdots, g_t\rangle$, which shows that $I \subset \langle g_1, \cdots, g_t\rangle$, which in turn proves the theorem.

To see why $r = 0$, simply note that $f, \sum_{i=1}^n a_i g_i \in I \rightarrow r \in I$, which means $\text{LT}(r) \in \langle \text{LT}(I)\rangle = \langle \text{LT}(g_i)\rangle \rightarrow \text{LT}(r)$ is divisible by some $\text{LT}(g_j)$, which violates the division algorithm above. Thus, we must have $r = 0$, which proves the theorem. □

As the proof of the above theorem demonstrates, bases $\{g_1, \cdots, g_t\}$ which have the property that $\langle \text{LT}(I)\rangle = \langle \text{LT}(g_1), \cdots, \text{LT}(g_t)\rangle$ play particularly important roles in the study of polynomial ideals and affine varieties. With that motivation in mind, we present the following definition.

(Definition) Groebner basis: *A finite generating set $G := \{g_1, \cdots, g_t\}$ of polynomial ideal $I = \langle G\rangle$ is a* ***Groebner basis****, or a* ***standard basis****, with respect to some monomial ordering if*

$$\langle \text{LT}(g_1), \cdots, \text{LT}(g_t)\rangle = \langle \text{LT}(I)\rangle$$

• An equivalent formulation of this definition is that G is a Groebner basis of I if the leading term of every element of I is divisible by some $\text{LT}(g_i)$.

• It follows as a corollary that every ideal other than $\{0\}$ has a Groebner basis, and that Groebner bases are, naturally, bases for I.

We conclude this section with two applications of the Hilbert basis theorem. The first is an algebraic statement about ideals in $F[x_1, \cdots, x_n]$, and concerns ascending chains of ideals, which are nested sequences of ideals I_i of the form

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

Namely, we can show that infinitely ascending chains of ideals eventually "converge" or stabilize.

(Theorem) Ascending chain condition: *Let $I_1 \subset I_2 \subset I_3 \subset \cdots$ be an ascending chain of ideals in $F[x_1, \cdots, x_n]$. Then $\exists N$ s.t.*

$$I_N = I_{N+1} = \cdots$$

which is to say, the ascending chain of ideals stabilizes.

• *Proof*: Consider the set

$$I := \bigcup_{i=1}^{\infty} I_i$$

First note that I is an ideal, since

1. $0 \in I_i, \forall i \rightarrow 0 \in I$
2. $f, g \in I \rightarrow \exists i, j$ s.t. $f \in I_i, g \in I_j \rightarrow f, g \in I_j$, where we label such that $i \leq j$ which implies $I_i \subset I_j$, which shows that $f + g \in I_j$, which shows that $f + g \in I$
3. $f \in I, g \in F[x_1, \cdots, x_n] \rightarrow \exists i$ s.t. $f \in I_i \rightarrow gf \in I_i \rightarrow gf \in I$

Then by the Hilbert basis theorem, I is finitely generated, and since each of the generators are contained in some I_i, we can take N to be the maximum index of an ideal which contains a generator of I, which shows that

$$I \subset I_N \subset I_{N+1} \subset \cdots$$

which implies that $I = I_N = I_{N+1} = \cdots$. □

• It can also be shown that the ascending chain condition implies the Hilbert basis theorem, which means that the two are equivalent to each other. The ascending chain condition will be crucial in designing Buchberger's algorithm for finding Groebner bases, discussed in a later section.

Because all polynomial ideals are finitely generated, we can now formally make the following natural definition of the affine variety defined by an ideal (previously we defined the ideal of an affine variety).

(Definition) Affine variety defined by an ideal: *Let $I \subset F[x_1, \cdots, x_n]$ be a polynomial ideal. Then we define the **affine variety defined by the ideal** I, denoted $\mathbf{V}(I)$, as the set*

$$\mathbf{V}(I) := \{(a_1, \cdots, a_n) \in F^n \text{ where } \forall f \in I : f(a_1, \cdots, a_n) = 0\}$$

• *Proof that $\mathbf{V}(I)$ is an affine variety*: We prove the stronger statement that, in particular,

$$\mathbf{V}(I) = \mathbf{V}(f_1, \cdots, f_s) \text{ where } I = \langle f_1, \cdots, f_s \rangle$$

Note that the above formulation is valid for all polynomial ideals I, since I is guaranteed to have a finite generating set by the Hilbert basis theorem.

First, note that $\mathbf{V}(I) \subset \mathbf{V}(f_1, \cdots, f_s)$ since $(a_1, \cdots, a_n) \in \mathbf{V}(I) \rightarrow f(a_1, \cdots, f_s) = 0, \forall f \in I \rightarrow f_i(a_1, \cdots, a_n) = 0, \forall i$. Conversely, $\mathbf{V}(f_1, \cdots, f_s) \subset \mathbf{V}(I)$ since $(a_1, \cdots, a_n) \in \mathbf{V}(f_1, \cdots, f_s) \rightarrow f_i(a_1, \cdots, a_n) = 0, \forall i \rightarrow \forall f \in I : f(a_1, \cdots, a_n) = 0$ since we can write $f = h_1 f_1 + \cdots + h_s f_s$ which implies $f(a_1, \cdots, a_n) = h_1(a_1, \cdots, a_n) f_1(a_1, \cdots, a_n) + h_s(a_1, \cdots, a_n) f_s(a_1, \cdots, a_n) = h_1(a_1, \cdots, a_n) \cdot 0 + \cdots + h_s(a_1, \cdots, a_n) \cdot 0 = 0$.

It follows that $\mathbf{V}(I) = \mathbf{V}(f_1, \cdots, f_s)$ and thus is an affine variety. □

The main consequence of the above proof is the important idea that varieties are determined by ideals; polynomial ideals are deeply connected to affine varieties, and in fact lie at the heart of affine varieties.

6 Properties of Groebner Bases

Building off the last section, where we saw that all polynomial ideals have a Groebner basis, in this section we'll study the properties of Groebner bases and how to detect if a basis is a Groebner basis. Groebner bases are significant because they are in many ways "nice" bases that are well-behaved. We begin by giving an example of this by showing that Groebner bases are amicable to work with in the polynomial division algorithm.

(Theorem) Uniqueness when dividing by Groebner bases: *Let $G = \{g_1, \cdots, g_t\}$ be a Groebner basis for ideal $I \subset F[x_1, \cdots, x_n]$ with respect to some monomial order. Then for any $f \in F[x_1, \cdots, x_n]$, the remainder of the division of f*

by G is unique.

• *Proof*: Applying the division algorithm, we find $a_i, r \in F[x_1, \cdots, x_n]$ such that

$$f = a_1 g_1 + \cdots + a_t g_t + r$$

where no term of r is divisible by any of $\mathrm{LT}(g_i)$. Suppose that

$$f = g + r = g' + r'$$

where $g = a_1 g_1 + \cdots + a_t g_t$ and (g', r') are another solution to f divided by G. Then $r - r' = g - g' \in I$ which means that $r \neq r' \rightarrow \mathrm{LT}(r - r') \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_t) \rangle$ which means $\mathrm{LT}(r - r')$ is divisible by some $\mathrm{LT}(g_i)$, which means $\mathrm{LT}(r), \mathrm{LT}(r')$ are divisible by $\mathrm{LT}(g_i)$, which contradicts the division algorithm. Hence, $r = r'$, which proves uniqueness. □

• As a corollary which also obtain another solution to the ideal membership problem - if G is a Groebner basis for polynomial ideal $I \subset F[x_1, \cdots, x_n]$ then $\forall f \in F[x_1, \cdots, x_n] : f \in I \iff$ remainder on division of f by G is zero.

The corollary to the above theorem essentially reduces the ideal membership problem to the problem of finding Groebner bases; if we can algorithmically compute Groebner bases, then we can algorithmically solve the ideal membership problem, since we can then apply the division algorithm to the polynomial in question and the Groebner basis. In upcoming sections we study how to find Groebner bases, but for the remainder of this section, we discuss the problem of determining if a given basis is a Groebner basis.

Notice that the only thing stopping a set $\{g_1, \cdots, g_t\}$ from being a Groebner basis is the possibility that some linear combination of the g_i's yields a polynomial whose leading term isn't in $\langle \mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_t) \rangle$ (because it's always true that $\langle \mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_t) \rangle \subset \langle \mathrm{LT}(I) \rangle$). The only way this could happen is if the leading terms of the linear combination of the g_i's somehow cancel and leave behind terms that are all smaller in degree than any of $\mathrm{LT}(g_i)$. To further study this cancellation, we make the following useful definitions.

(Definition) Least common multiple of monomials: *Let $f, g \in F[x_1, \cdots, x_n]$ with $\alpha :=$ multideg$(f), \beta :=$ multideg(g). Then the **least common multiple** of LM(f) and LM(g) is*

$$\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g)) := x^\gamma, \gamma = (\gamma_1, \cdots, \gamma_n) \text{ where } \gamma_i = \max(\alpha_i, \beta_i) \text{ for } 1 \leq i \leq n$$

*Moreover, we define the **S-polynomial** of f and g as*

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

• *Motivation*: The definition of the least common multiple follows naturally from the definition of the greatest common divisor, defined earlier. We could have defined the precise analog for the least common multiple of two polynomials, but instead defined the special case with monomials because it's much simpler to compute and directly relevant to the definition of S-polynomials. The "S" in S-polynomials stands for "subtraction", as the S-polynomial is specifically designed so as to eliminate the leading terms of the two polynomials f, g. The S-polynomial "forces" the leading terms of the two terms being subtracted to become $\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$ so in the subtraction the resulting polynomial has the leading terms eliminated. In accordance with the intuition design of the S-polynomial, it actually turns out that in some sense every cancellation of leading terms in polynomial addition is due to S-polynomials:

(Theorem) Cancellation of leading terms is due to S-polynomials: *Given polynomials $f_i \in F[x_1, \cdots, x_n], 1 \leq i \leq s$, with $\forall i :$ multideg$(f_i) = \delta$, let $L := \sum_i c_i f_i, c_i \in F$ be a linear combination of the polynomials. If multideg$(L) < \delta$, then L is a linear combination of S-polynomials $S(f_j, f_k), 1 \leq j, k \leq s$.*

• *Proof*: With some clever definitions and algebraic manipulation, we can transform the sum $L = \sum_i c_i f_i$ into a linear combination of $S(f_j, f_k)$. Let $d_i := \mathrm{LC}(f_i), p_i = d_i^{-1} f_i$, so that $f_i = d_i p_i$. Next, note that

$$\mathrm{multideg}(f_i) = \delta \rightarrow \mathrm{LCM}(\mathrm{LM}(f_j), \mathrm{LM}(f_k)) = x^\delta \rightarrow S(f_j, f_k) = \frac{x^\delta}{\mathrm{LT}(f_j)} f_j - \frac{x^\delta}{\mathrm{LT}(f_k)} f_k = \frac{x^\delta}{d_j x^\delta} f_j - \frac{x^\delta}{d_k x^\delta} f_k = p_j - p_k$$

We are now in a position to write L as a linear combination of S-polynomials, once we transform the summation defining L into a telescoping series as follows.

$$L = \sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i d_i p_i = \sum_{i=1}^{s} \left((p_{i-1} - p_i) \sum_{j=1}^{i-1} c_j d_j \right) + p_s \sum_{j=1}^{s} c_j d_j$$

We can prove the above identity by induction on s. Let $L_s = \sum_{i=1}^{s} c_i f_i$ and assume the identity above as the inductive hypothesis. Then

$$\begin{aligned}
L_{s+1} &= \sum_{i=1}^{s+1} c_i d_i p_i = L_s + p_{s+1} c_{s+1} d_{s+1} = \sum_{i=1}^{s} \left((p_{i-1} - p_i) \sum_{j=1}^{i-1} c_j d_j \right) + p_s \sum_{j=1}^{s} c_j d_j + p_{s+1} c_{s+1} d_{s+1} \\
&= \sum_{i=1}^{s} \left((p_{i-1} - p_i) \sum_{j=1}^{i-1} c_j d_j \right) + p_s \sum_{j=1}^{s} c_j d_j + \left(p_{s+1} \sum_{i=1}^{s} c_i d_i - p_{s+1} \sum_{i=1}^{s} c_i d_i \right) + p_{s+1} c_{s+1} d_{s+1} \\
&= \sum_{i=1}^{s} \left((p_{i-1} - p_i) \sum_{j=1}^{i-1} c_j d_j \right) + (p_s - p_{s+1}) \sum_{j=1}^{s} c_j d_j + p_{s+1} \sum_{j=1}^{s} c_j d_j + p_{s+1} c_{s+1} d_{s+1} \\
&= \sum_{i=1}^{s+1} \left((p_{i-1} - p_i) \sum_{j=1}^{i-1} c_j d_j \right) + p_{s+1} \sum_{j=1}^{s+1} c_j d_j
\end{aligned}$$

Moreover, because $c_i f_i$ all have multidegree δ but their sum has multidegree strictly smaller than δ, all the leading terms in the summation must cancel out, so that $\sum_{i=1}^{s} c_i d_i = 0$. Thus, from the above telescoping series and the formulation of $S(f_j, f_k)$ in terms of p_j, p_k, it follows that

$$L = \sum_{i=1}^{s} \left((p_{i-1} - p_i) \sum_{j=1}^{i-1} c_j d_j \right) + p_s \sum_{j=1}^{s} c_j d_j = \sum_{i=1}^{s} \left(S(f_{i-1}, f_i) \sum_{j=1}^{i-1} c_j d_j \right) + p_{s+1} \cdot 0 = \sum_{i=1}^{s} a_{i-1} S(f_{i-1}, f_i)$$

where $a_i := \sum_{j=1}^{i} c_i d_i$, proving that L is a linear combination of S-polynomials. $\square$

Because the linear combination of polynomials, each with multidegree δ, can be written as a linear combination of S-polynomials, each with multidegree strictly less than δ, the S-polynomials account for the cancellation. As we will now see, this cancellation property of S-polynomials is useful in determining if a basis is a Groebner basis or not.

(Theorem) Buchberger's criterion: *Let I be a polynomial ideal and $G = \{g_1, \cdots, g_t\}$ be a basis for I. G is a Groebner basis for I if and only if*

$$\forall i \neq j : G \text{ divides } S(g_i, g_j) \text{ with respect to some monomial ordering of } G$$

where "divides" refers to zero remainder upon applying the division algorithm.

• *Proof*: We want to show that for any $f \in I$, $\mathrm{LT}(f) \in L := \langle \mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_t) \rangle$. Since G is a basis for I, we can find $h_1, \cdots, h_t \in F[x_1, \cdots, x_n]$ such that

$$f = h_1 g_1 + \cdots + h_t g_t$$

Let $\delta := \max_i \mathrm{multideg}(h_i g_i)$, chosen so that δ is minimal over all possible monomial orderings of $h_i g_i$; then $\mathrm{multideg}(f) \leq \delta$. If we have equality, then we're done, since then, for some k, $\mathrm{multideg}(h_k g_k) = \mathrm{multideg}(f) = \deg(\mathrm{LT}(f))$ which means g_k divides $\mathrm{LT}(f)$.

Otherwise, $\mathrm{multideg}(f) < \delta$. We'll show that this leads to a contradiction. First, split the linear combination by multidegree:

$$f = \sum_{\mathrm{multideg}(h_i g_i) = \delta} h_i g_i + \sum_{\mathrm{multideg}(h_i g_i) < \delta} h_i g_i = \sum_{\mathrm{multideg}(h_i g_i) = \delta} \mathrm{LT}(h_i) g_i + \sum_{\mathrm{multideg}(h_i g_i) = \delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{\mathrm{multideg}(h_i g_i) < \delta} h_i g_i$$

The second and third terms above have multidegree below δ, as does f by assumption, so the first summation must involve some cancellation, which means we can rewrite it as a linear combination of S-polynomials.

$$\sum_{\mathrm{multideg}(h_i g_i) = \delta} \mathrm{LT}(h_i) g_i = \sum_{j,k} a_{j,k} S(\mathrm{LT}(h_j) g_j, \mathrm{LT}(h_k) g_k) = \sum_{j,k} a_{j,k} x^{\delta - \gamma_{j,k}} S(g_j, g_k)$$

where $\gamma_{j,k} := \mathrm{LCM}(\mathrm{LM}(g_j), \mathrm{LM}(g_k))$ and because, letting $\mathrm{LT}(h_i) = c_i x^{\alpha_i}$,

$$S(c_j x^{\alpha_j} g_j, c_k x^{\alpha_k} g_k) = \frac{x^\delta}{x^{\alpha_j} \mathrm{LT}(g_j)} x^{\alpha_j} g_j - \frac{x^\delta}{x^{\alpha_k} \mathrm{LT}(g_k)} x^{\alpha_k} g_k = x^{\delta - \gamma_{j,k}} S(g_j, g_k)$$

Applying the division algorithm, we find that due to our assumption that the S-polynomials have no remainder,

$$S(g_j, g_k) = \sum_{i=1}^{t} h'_{i,j,k} g_i, h'_i \in F[x_1, \cdots, x_n] \text{ and where } \mathrm{multideg}(h'_{i,j,k} g_i) \leq \mathrm{multideg}(S(g_j, g_k))$$

where the division algorithm implies $\text{multideg}(x^{\delta-\gamma_{j,k}}a_{i,j,k}) \leq \text{multideg}(x^{\delta-\gamma_{j,k}}S(g_j,g_k)) < \delta$.

$$\rightarrow x^{\delta-\gamma_{j,k}}S(g_j,g_k) = \sum_{i=1}^{t} x^{\delta-\gamma_{j,k}}h'_{i,j,k}g_i \rightarrow \sum_{\text{multideg}(\text{LT}(h_i)g_i)=\delta} h_ig_i = \sum_{j,k} a_{j,k}\sum_{i=1}^{t} x^{\delta-\gamma_{j,k}}h'_{i,j,k}g_i = \sum_{i=1}^{t} h''_i g_i$$

for appropriately defined h''_i. At last, we have arrived at the property $\text{multideg}(h''_i g_i) < \delta$, which allows us to substitute the above equality into the above equation in which we split up f, which yields an expression of f as a linear combination of G in which all terms have multidegree strictly less than δ, which contradicts the minimality of δ. □

• The idea that the proof captures is that if G is a basis, then any $f \in I$ can be written as a linear combination of polynomials in G, by definition. If the multidegree of f, which is the degree of $\text{LT}(f)$, matches the degree of one of the terms in the linear combination, then that term divides $\text{LT}(f)$ which is hence in $\langle \text{LT}(I)\rangle$. However, if the multidegree of f doesn't match the degree of any of the terms in the linear combination, then the multidegree of f must be smaller than some of the multidegrees of the terms of the linear combination (since linear combinations of polynomials never yield increasing multidegrees - only products of polynomials can do that), which mean some cancellation must occur, which means S-polynomials are involved.

7 Buchberger's Algorithm

Earlier, we showed that every polynomial ideal is guaranteed to have a Groebner basis; in this section we give an algorithm for finding them. Given a basis $G = \{g_1, \cdots, g_s\}$ for polynomial ideal I, if G is not a Groebner basis then it's because, by Buchberger's criterion, there's some S-polynomial of elements of G which is not divisible by G, i.e. has non-zero remainder. Something we could try to "force" G to become a Groebner basis is a greedy approach in which at every iteration we use Buchberger's criterion to test if G is a Groebner basis, and if it isn't, then there's some non-zero remainder of the division of some S-polynomial by G which we can add to G, satisfying the constraint we just failed, and proceed until we satisfy all the constraints (which are, namely, that all the S-polynomials are divisible by G) and hence will have a Groebner basis.
Although adding terms to G, which is already a basis, creates a redundant basis, in the sense that not all elements are necessary to have a basis, G will become a Groebner basis, which in computational settings is useful enough to more than compensate for the redundancy. The following algorithm formalizes the above greedy approach.

(Theorem) Buchberger's algorithm: *Let $I = \langle f_1, \cdots, f_s\rangle$ by a polynomial ideal. We can construct a Groebner basis for I with the following algorithm.*

```
procedure GroebnerBasis(f_1, ..., f_s)
    G ← {f_1, ..., f_s}
    G' = {}
    while G ≠ G' do
        G' ← G
        for f ≠ g ∈ G' do
            r ← remainder of PolynomialDivision(S(f, g), G')
            if r ≠ 0 then
                G ← G ∪ {r}
            end if
        end for
    end while
    return G
end procedure
```

• *Proof*: First note that at every iteration of the algorithm, if G starts as a basis for I then it will still be a basis by the end of the iteration, since no elements are removed and hence it still contains the original basis that was given as an argument, and since no element not in I is ever added to G ($G \subset I \rightarrow f, g \in I \rightarrow S(f,g) \in I \rightarrow r \in I$). At the start of the algorithm G is simply the given basis, so it follows inductively that G is always a basis. Moreover, when the algorithm terminates, we must have $r = 0$ for all combinations of $f \neq g \in G$, which means, by Buchberger's criterion, G is a Groebner basis.

To prove that the algorithm always halts, recall the ascending chain condition proven earlier, which states that any ascending chain of ideals in $F[x_1, \cdots, x_n]$ eventually stabilizes. Notice that after every iteration of the loop, $G' \subset G$. Moreover, $G = G' \bigcup_i r_i$ where the r_i's are the remainders of the division by the S-polynomials by G'. Since r_i is such a remainder, by the division algorithm $\text{LT}(r_i)$ cannot be divisible by any leading term of an element of G', which means

$$\text{LT}(r_i) \notin \langle \text{LT}(g'), g' \in G'\rangle \text{ but } \text{LT}(r_i) \in \langle \text{LT}(g), g \in G\rangle$$

Hence, $G' \subset G \rightarrow \langle \text{LT}(g'), g' \in G'\rangle \subset \langle \text{LT}(g), g \in G\rangle$, which means at every iteration we have an ascending chain of ideals, $\langle \text{LT}(g), g \in G\rangle$, which must eventually stabilize, meaning $G' = G$. Thus, the algorithm terminates. □

• Note that the above algorithm is not optimal, computationally. One optimization that may be made is that there is no need to re-check the remainders of all the S-polynomials against G' - once the remainder is zero, it will always be zero, no matter how many new elements are added to G'. There are many other optimizations that can be made, but for the sake of clarity we exclude them.

As touched on above, Buchberger's algorithm begins with a basis and enlarges it until it's a Groebner basis. Because of this, there's a lot of redundancy in the resulting Groebner basis, which will usually be larger than it needs to be. Here's a method we can use to eliminate some of the extraneous generators in the Groebner basis.

(Theorem) Extraneous generators of Groebner bases: *Let G be a Groebner basis for polynomial ideal I. Then any $g \in G$ such that $LT(g) \in \langle LT(f), f \in G - \{g\}\rangle$ is extraneous. That is, $G - \{g\}$ is also a Groebner basis for I.*

• *Proof*: This proposition is intuitive and easy to see, since if we can generate $\mathrm{LT}(g)$ using elements from G other than g, then any element of I whose expression as a linear combination of elements of G depends on g can be replaced by a linear combination depending only on elements of G that aren't g. Formally, if $\mathrm{LT}(g) \in \langle \mathrm{LT}(f), f \in G - \{g\}$ then $\exists f_i \in I$ such that

$$\mathrm{LT}(g) = \sum_i f_i g_i, g_i \neq g \in G$$

It follows that for any $f \in I$,

$$f = \sum_{g_i \in G} h_i g_i = \sum_{g_i \neq g \in G} h_i g_i + hg = \sum_{g_i \neq g \in G} h_i g' + h \sum_{g_i \neq g \in G} f_i g_i$$

Thus, $G - \{g\}$ is also a Groebner basis for I. □

• We define a **minimal Groebner basis** to be one for which none of the above eliminations may me made; it's as small as it can be while remaining a Groebner basis. We can construct minimal Groebner bases by applying Buchberger's algorithm and then using the above theorem to remove extraneous generators.

A polynomial ideal may have more than one minimal Groebner bases, so we single one out as a canonical minimal Groebner basis, filtering so that the canonical form is guaranteed to have nice properties we can work with.

(Definition) Reduced Groebner basis: *A **reduced Groebner basis** G for polynomial ideal I is a Groebner basis for which*

1. $\forall g \in G : \mathrm{LC}(g) = 1$
2. $\forall g \in G$: no monomial term of g is in $\langle \mathrm{LT}(f), f \in G - \{g\}$

• *Existence and uniqueness*: All polynomial ideals have a unique reduced Groebner basis.

• One last point - Buchberger's algorithm also provides a computational way to solve the ideal equality problem (checking if two ideals are the same) - given $\langle f_1, \cdots, f_s\rangle$ and $\langle g_1, \cdots, g_t\rangle$, simply compute the reduced Groebner bases and check if they're equal. This works since reduced Groebner bases are unique and guaranteed to exist.

• The first condition is useful for uniqueness, since many minimal Groebner bases are only unique up to a constant, and the second condition enforces some sense of additional restriction or minimality on G, by forcing every generator in G to be absolutely necessary in the sense that its removal causes the removal of all the terms of that generator.

8 Applications of Groebner Bases

In the beginning of this chapter we posed four central problems in computer algebra and elementary algebraic geometry: ideal description, ideal membership, solving polynomial equations, and the implicitization problem. The Hilbert basis theorem solved the ideal description problem. Now we investigate the application of Groebner bases to the remaining three problems.

8.1 Ideal Membership Problem

When studying properties of Groebner bases, we showed that one way in which Groebner bases are well behaved is that dividing by them can be done uniquely - specifically, division yields a unique remainder. Thus, a polynomial is in an ideal if and only if its remainder when divided by a Groebner basis for that ideal is zero. Therefore, we can combine Buchberger's algorithm with the division algorithm to solve the ideal membership problem.
First, use Buchberger's algorithm to compute a Groebner basis. Then use the division algorithm to check if the remainder is zero. If it is, then the polynomial in question is in the ideal, and otherwise it isn't.

8.2 Polynomial Equations

Any system of polynomial equations

$$f_1(x_1, \cdots, x_n) = \cdots = f_s(x_1, \cdots, x_n) = 0$$

can be viewed as the zero set of a set of polynomials, and considering the ideal generated by those polynomials is a good way to cast the problem in a way amicable to the theory of Groebner bases. Recall that in our study of the Hilbert basis theorem and Groebner bases we found that the affine variety $\mathbf{V}(I)$ of a polynomial ideal I follows

$$I = \langle g_1, \cdots, g_t \rangle \to \mathbf{V}(I) = \mathbf{V}(g_1, \cdots, g_t)$$

It follows that when considering $I := \langle f_1, \cdots, f_s \rangle$ it doesn't matter what basis we use; the zero-set will not change. Thus we can transform the problem into the zero-set of the reduced Groebner basis. We will study this idea, which is the foundation of a field of study known as elimination theory, extensively in the future. From a high level, recasting the problem in terms of Groebner bases will force the equations to successively "eliminate" variables, so that the last equation is in a single variable, the second to last in two variables, and so on. This will allow us to reduce the problem of solving a system of multivariate polynomial equations to solving a single polynomial equation in one variable, since once we can do this we can iteratively back-substitute to obtain a full solution set.

8.3 Implicitization

Finally, consider the last of the four problems: given a set of parametric equations

$$\begin{aligned} x_1 &= f_1(t_1, \cdots, t_m), \\ &\vdots \\ x_n &= f_n(t_1, \cdots, t_m) \end{aligned}$$

which define some subset of an affine variety V in F^n. We wish to reverse engineer the implicit description of V, i.e. to find polynomial equations in $x_1, \cdots, x_n$ which define V. We will, in the next chapter, solve this problem using Groebner bases. For simplicity, suppose that the f_i are polynomials, and consider the affine variety in F^{n+m} given by $\mathbf{V}(x_i - f_i(t_1, \cdots, t_m), 1 \leq i \leq n)$. We will try to eliminate $t_1, \cdots, t_m$ from the equations

$$\begin{aligned} x_1 - f_1(t_1, \cdots, t_m) &= 0 \\ &\vdots \\ x_n - f_n(t_1, \cdots, t_m) &= 0 \end{aligned}$$

to find the equations for V. We can use Groebner bases with respect to the lexicographic ordering $t_1 > \cdots > t_m > x_1 > \cdots > x_n$. If we had a Groeber basis for the ideal $I := \langle x_1 - f_1, \cdots, x_n - f_n \rangle$ then hopefully the Groebner basis should eliminate the first m variables in the lexicographic order, leaving a basis containing polynomials in $x_1, \cdots, x_n$.