MATH536A Paper: Gröbner Bases

Martin Leslie

December 15, 2008

Abstract

An introduction to Gröbner bases and some of their uses in affine algebraic geometry.

Contents

1 Introduction

In his 1965 thesis [Buc65], Bruno Buchberger developed the theory of Gröbner bases which allow computations in multivariate polynomial rings analogous to those we are used to in single variable polynomial rings. This theory can also be seen as a generalization of Gaussian elimination or of integer programming. We follow [CLO06], with minor variations, in our development of the basic theory.

We also give some examples, that show how these techniques can solve some problems from this text and also our class text [Sha94].

We make some notational conventions: For $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ a multi-index, we set $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Throughout, k is a field and ideals and polynomials are assumed to belong to $k[x_1, \ldots, x_n]$ if not otherwise specified. Finally, in pseudocode, '=' is used for right to left assignment and '==' is used for comparison.

2 Trying to extend the division algorithm to multivariate polynomials

To use polynomial long division or Gaussian elimination we need an ordering on our monomials (we usually use $x^{n+1} > x^n$ and $x_1 > x_2 > \cdots > x_n$ respectively). Thus before we try to extend the algorithms we need to come up with an ordering of monomials in $k[x_1, \ldots, x_n]$ or equivalently of elements of $\mathbb{Z}^n_{\geq 0}$.

Before defining exactly what orderings we are interested in we do some work (also crucial for our later results) that allows us to give a nicer definition.

2.1 Monomial ideals and Dickson's lemma

Definition 2.1. An ideal $I \subset k[x_1, \ldots, x_n]$ is a *monomial ideal* if $I = \langle x^\alpha \colon \alpha \in A \rangle$ for some $A \subseteq \mathbb{Z}^n_{\geq 0}$.

Lemma 2.2. *Let $I = \langle x^\alpha \colon \alpha \in A \rangle$ be a monomial ideal. Then a monomial $x^\beta \in I$ if and only if x^α divides x^β for some $\alpha \in A$.*

Proof. Firstly, if x^β is a multiple of x^α for some $\alpha \in A$ then $x^\beta \in I$ because I is an ideal. Conversely, if $x^\beta \in I$ then we can write it as a linear combination of x^{α_i} with polynomial coefficients. Then expanding each polynomial as a sum of monomials we have x^β as a sum of monomials each divisible by some x^α. But this is a polynomial identity so in fact x^β must be exactly one of these monomials and thus has the same property. □

Lemma 2.3. *Let I be a monomial ideal and $f \in k[x_1, \ldots, x_n]$. Then $f \in I$ if and only if f is a k–linear combination of monomials in I. Thus two monomial ideals are equal if and only if they contain the same monomials.*

Proof. Clearly, if f is a k–linear combination of monomials in I then $f \in I$. For the other direction, if $f \in I$ then f is a $k[x_1, \ldots, x_n]$–linear combination of monomials of I. So expanding this out we see that f is a k–linear combination of monomials which are in I by Lemma 2.2. □

The next result shows that monomial ideals are finitely generated.

Theorem 2.4 (Dickson's Lemma)**.** *Let $I = \langle x^\alpha \colon \alpha \in A \rangle \subset k[x_1, \ldots, x_n]$ be a monomial ideal. Then $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$ for some $\alpha_1, \ldots, \alpha_s \in A$.*

Proof. (By induction on n). For the $n = 1$ case we have $I = \langle x_1^\alpha : \alpha \in A \rangle$ for some $A \subset \mathbb{Z}_{\geq 0}$. Take $\beta = \min A$ and then $x_1^\beta \mid x_1^\alpha$ for all $\alpha \in A$ so then $I = \langle x_1^\beta \rangle$ as desired.

So now we assume the theorem is true for $n-1$ and then prove it for n. We write our variables as $x_1, \ldots, x_{n-1}, y$ so a monomial in $k[x_1, \ldots, x_{n-1}, y]$ is of the form $x^\alpha y^m$ where $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$ and $m \in \mathbb{Z}_{\geq 0}$. Take I our monomial ideal and let J be the ideal of $k[x_1, \ldots, x_{n-1}]$ generated by monomials x^α where $x^\alpha y^m \in I$ for some $m \geq 0$. Then our inductive hypothesis implies that $J = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$ for some s.

Also take $m = \max\{m_i\}$ and for each $k < m$ let $J_k = \langle x^\beta : x^\beta y^k \in I \rangle \subset k[x_1, \ldots, x_{n-1}]$. Then again by our inductive hypothesis we have $J_k = \langle x^{\alpha_{k,1}}, \ldots, x^{\alpha_{k,s_k}} \rangle$ for some s_k.

Now if we take a monomial $x^\alpha y^p \in I$ there are two cases: If $p \geq m$ then $x^\alpha \in J$ so there is some x^{α_i} which divides x^α so we have $x^{\alpha_i} y^m \mid x^\alpha y^p$. Otherwise, if $p \leq m-1$ then $x^\alpha \in J_p$ so there exists $\alpha_{p,j}$ such that $x^{\alpha_{p,j}} y^p \mid x^\alpha y^p$. So we see that every monomial in I is divisible by an element of $\{x^{\alpha_i} y^m : 1 \leq i \leq m\} \cup \{x^{\alpha_{k,j}} y^k : 0 \leq k < m, 1 \leq j \leq s_k\}$.

By Lemmas 2.2 and 2.3 this shows that I is generated by the elements of the above set and thus is finitely generated. Switching back to x_n instead of y, we have $I = \langle x^{\beta_1}, \ldots, x^{\beta_s} \rangle$ for some $x^{\beta_i} \in I$. So then for each i there exists α_i with $x^{\alpha_i} \mid x^{\beta_i}$ and then $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$ as required. □

2.2 Monomial orderings

Definition 2.5. A *monomial ordering* on $k[x_1, \ldots, x_n]$ is a relation $>$ on $\mathbb{Z}_{\geq 0}^n$ satisfying:

(i) $>$ is a total ordering.

(ii) If $\alpha > \beta$ and $\gamma \in \mathbb{Z}_{\geq 0}^n$ then $\alpha + \gamma > \beta + \gamma$.

(iii) $\alpha \geq 0$ for all $\alpha \in \mathbb{Z}_{\geq 0}^n$.

Proposition 2.6. *In the definition above we could have replaced (iii) with either of*

(iii') $>$ is a well-ordering.

(iii") Every strictly decreasing sequence $\alpha_1 > \alpha_2 > \ldots$ eventually terminates.

Proof. Assuming conditions (i) and (ii):

- (iii $\implies$ iii'). We need to show that any nonempty $A \subseteq \mathbb{Z}_{\geq 0}^n$ has a smallest element. But $I = \langle x^\alpha : a \in A \rangle$ is a monomial ideal so by Dickson's lemma we have $I = \langle x_1^\alpha, \ldots, x^{\alpha_s} \rangle$ and we can arrange the α_i so that $\alpha_1 < \alpha_2 < \ldots < \alpha_s$. Then for any $\alpha \in A$, x^α is divisible by some x_i^α and thus is divisible by x_1^α. From this we see that $\alpha_1 \leq \alpha$ for all $\alpha \in A$ so α is the smallest element of A.
- (iii' $\implies$ iii"). If there was a non-terminating sequence $\alpha_1 > \alpha_2 > \ldots$ then the set $\{\alpha_1, \alpha_2, \ldots\}$ would not be well ordered under $>$.
- (iii" $\implies$ iii). Take $\alpha \in A$. Then if $0 > \alpha$, by property (ii) we have $\alpha > 2\alpha$, then $2\alpha > 3\alpha$ and so on. This gives a non-terminating strictly decreasing sequence which cannot happen, so we must have $\alpha \geq 0$.

□

Definition 2.7. We have a number of important examples of monomial orderings. In what follows $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ and similarly for β. Also $|\alpha| = \sum_{i=1}^n \alpha_i$.

(i) Lexical order or *lex*. Say $\alpha >_{lex} \beta$ if the leftmost non-zero entry of $\alpha - \beta$ is positive.

(ii) Graded lexical order or *grlex*. Say $\alpha >_{grlex} \beta$ if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and $\alpha >_{lex} \beta$.

(iii) Graded reverse lexical order or *grevlex*. Say $\alpha >_{grevlex} \beta$ if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and the rightmost non-zero entry of $\alpha - \beta$ is negative.

It is a straightforward check that all these satisfy the properties required to be a monomial order.

Note that these orderings depend on the ordering of the variables so there are in fact $n!$ lex orderings. We will use the standard ordering with $x_1 > \cdots > x_n$. Also note that grevlex is not just grlex with the variables switched around. Roughly, grlex breaks ties by choosing the term with the highest power of x_1, grevlex chooses the term with the lowest power of x_n.

Now fixing a monomial order we can write a polynomial as $f = \sum_\alpha a_\alpha x^\alpha$ with the terms in decreasing order. Then define the *multidegree* to be the highest α under this order and define the *leading coefficient*, *leading monomial* and *leading term* as for single variable polynomials. We use the notation $\mathrm{LC}(f), \mathrm{LM}(f), \mathrm{LT}(f)$ respectively for these quantities.

2.3 The division algorithm

To 'divide' a polynomial f by polynomials $f_1, \ldots, f_s$ we aim to write

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

for some $a_i, r \in k[x_1, \ldots, x_n]$. Some experimentation should convince you that this is possible but there should be grave doubts over the uniqueness of the a_i and r.

Theorem 2.8 (Division algorithm for multivariable polynomials)**.** *Fix a monomial order $>$ and let $F = (f_1, \ldots, f_n)$. Then every $f \in k[x_1, \ldots, x_n]$ can be written as*

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

where $a_i, r \in k[x_1, \ldots, x_n]$ and either $r = 0$ or r is a k-linear combination of monomials none of which are divisible by the leading terms of any of $f_1, \ldots, f_s$. Furthermore, if $a_i f_i \neq 0$ the multidegree of f is greater than the multidegree of $a_i f_i$.

Proof. We prove the existence of the a_i and r by giving an algorithm to find them and then proving its correctness. We give the algorithm in pseudocode.

Require: $f_1, \ldots, f_s, f$
Ensure: $a_1, \ldots, a_s, r$ with properties as in Theorem

```
a_1 = 0, ..., a_s = 0, r = 0
p = f
while p ≠ 0 do
  i = 1
  divisionoccurred = false
  while i ≤ s and divisionoccurred == false do
    if LT(f_i) divides LT(p) then
```

$a_i = a_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}$
$p = p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i$
divisionoccurred = true
else
$i = i + 1$
end if
end while
if divisionoccurred == false **then**
$r = r + \mathrm{LT}(p)$
$p = p - \mathrm{LT}(p)$
end if
end while

Here p is the intermediate dividend and r is the intermediate remainder at each stage of the division. To show correctness of the algorithm we show that $f = a_1 f_1 + \cdots + a_s f_s + p + r$ is true after each pass through the main loop. Clearly this is true with the initial values of the variables.

If some $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$ then the only effect of the main loop on this equality is to replace $a_i f_i$ with $a_i f_i + f_i \cdot \mathrm{LT}(p)/\mathrm{LT}(f_i)$ and to replace p with $p - f_i \cdot \mathrm{LT}(p)/\mathrm{LT}(f_i)$ which conserves the right hand side and thus the equality. If no $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$ then the main loop replaces r with $r + \mathrm{LT}(p)$ and p with $p - \mathrm{LT}(p)$ which also preserves this equality.

If the algorithm halts then $p = 0$ and we have the desired equality $f = a_1 f_1 + \cdots + a_s f_s + r$. Also each term that was added to r is not divisible by each $\mathrm{LT}(f_i)$.

To see that the algorithm does terminate, note that p only changes by being redefined to be $p' = p - f_i \cdot \mathrm{LT}(p)/\mathrm{LT}(f_i)$. But $\mathrm{LT}(f_i \cdot \mathrm{LT}(p)/\mathrm{LT}(f_i)) = \mathrm{LT}(f_i) \cdot \mathrm{LT}(p)/\mathrm{LT}(f_i) = \mathrm{LT}(p)$ so p' is the difference of two polynomials with the same leading term and thus the multidegree of p' is less than the multidegree of p. Then if the sequence of p's did not eventually reach zero we would have a nonterminating decreasing sequence of multidegrees which is not possible.

For the bound on the multidegree of $a_i f_i$, note that by construction the terms of each a_i are of the form $\mathrm{LT}(p)/\mathrm{LT}(f_i)$ for some p with $\mathrm{LT}(p) < \mathrm{LT}(f)$. So if $a_i f_i \neq 0$ then the multidegree of $a_i f_i$ is less than or equal to the multidegree of $f_i \cdot \mathrm{LT}(p)/\mathrm{LT}(f_i)$ which is equal to the multidegree of $\mathrm{LT}(p)$ which is less than the multidegree of f. □

Next we see an example where dividing by f_1, f_2 and by f_2, f_1 give different remainders. The computations for these will be done on the next page (omitted from digital version) and show how these calculations can be set out in practice.

Example 2.9. In lex order, if we divide $f = x^2y + xy^2 + y^2$ by $(f_1, f_2) = (xy - 1, y^2 - 1)$ we get

$$f = (x + y)f_1 + f_2 + x + y + 1.$$

If we divide f by (f_2, f_1) we get

$$f = (x + 1)f_1 + xf_2 + 2x + 1.$$

3 Fixing what went wrong: Gröbner bases

We would like to use our division algorithm for the question of ideal membership. If dividing f by $f_1, \ldots, f_s$ gives a remainder of zero then we know that $f \in \langle f_1, \ldots, f_s \rangle$. But the converse is not true. Even if f has a nonzero remainder there may be some way to divide in a different order that gives a remainder of zero (we saw in our example in the last section that remainders are not unique).

As we shall see, Gröbner bases are the solution to this problem.

3.1 Existence of Gröbner bases

Write $\mathrm{LT}(I)$ for the set of leading terms of an ideal and $\langle \mathrm{LT}(I) \rangle$ for the ideal generated by this set.

Definition 3.1. A *Gröbner basis* of an ideal $I \subset k[x_1, \ldots, x_n]$ is a finite subset $G = \{g_1, \ldots, g_t\}$ of I such that

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle.$$

Proposition 3.2. *Every nonzero ideal I of $k[x_1, \ldots, x_n]$ has a Gröbner basis.*

Proof. Notice that $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g) : g \in I \setminus \{0\} \rangle = \langle \mathrm{LM}(g) : g \in I \setminus \{0\} \rangle$ is a monomial ideal. So by Dickson's lemma, $\langle \mathrm{LT}(I) = \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_t) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$ for some finite set of $g_i \in I$. □

Proposition 3.3. *A Gröbner basis is a basis.*

Proof. We have $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$ and need to show that $I = \langle g_1, \ldots, g_t \rangle$. Clearly $\langle g_1, \ldots, g_t \rangle \subseteq I$. Conversely, if $f \in I$ we use our division algorithm to divide f by $g_1, \ldots, g_t$ giving an expression of the form

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

where no term of r is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$. Then $r = f - a_1 g_1 - \ldots - a_t g_t \in I$ so $\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1) \ldots \mathrm{LT}(g_t) \rangle$. But no term of r is divisible by any of the $\mathrm{LT}(g_i)$ and so we must have $r = 0$ which implies that $f \in \langle g_1 \ldots, g_t \rangle$. □

Note that using the last two propositions and the fact that $\{0\}$ is finitely generated we have proved the Hilbert basis theorem: every ideal of $k[x_1, \ldots, x_n]$ has a finite generating set.

3.2 Properties of Gröbner bases

We first prove the promised result on uniqueness of remainders when dividing by a Gröbner basis.

Proposition 3.4. *Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis for an ideal I and f be a polynomial. Then there exists a unique polynomial r satisfying*

(i) No term of r is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$, and

(ii) There is $g \in I$ such that $f = g + r$.

Proof. The division algorithm gives the existence of r satisfying (i) and (ii) with $g = a_1 g_1 + \ldots + a_t g_t \in I$. For uniqueness, if there exists r, g and r', g' both satisfying these properties then $f = g + r = g' + r'$ so $r - r' = g' - g \in I$. If $r - r' \neq 0$ then $\mathrm{LT}(r - r') \in \langle \mathrm{LT}(I) \rangle$ which implies that $\mathrm{LT}(g_i)$ divides $\mathrm{LT}(r - r')$ for some i. But this is not possible because no term of r or r' is divisible by any $\mathrm{LT}(g_i)$. Thus we must have $r = r'$ and thus $g = g'$. □

This uniqueness result gives us a way to decide if a polynomial is inside an ideal (provided we know a Gröbner basis for it).

Corollary 3.5. *A polynomial $f \in I$ if and only if the remainder on division of f by a Gröbner basis G is zero.*

Proof. If the remainder is zero then $f \in I$. Conversely, if $f \in I$ then $f = f + 0$ which satisfies the conditions above and thus by uniqueness any remainder r must be zero. □

Now we try to come up with a test for whether a basis is a Gröbner basis. One way that a generating set can fail to be a Gröbner basis is if polynomial combinations of f_i can have leading terms that are not in the ideal generated by leading terms of the f_i. Thus we need to study how such cancellation can happen.

Definition 3.6. If $f, g \in k[x_1, \ldots, x_n]$ are nonzero polynomials we can find the least common multiple of their leading monomials $x^\gamma = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$. Then the *S-polynomial* of f and g is

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

These S–polynomials provide cancellation of leading terms and in fact are the only way that cancellation happens among sums of terms of the same multidegree as is seen more precisely in the following proposition.

Proposition 3.7. *Let f_i be polynomials all of multidegree δ and $c_i \in k$. If the multidegree of $\sum_{i=1}^s c_i f_i$ is less than δ then $\sum_{i=1}^s c_i f_i$ is a k-linear combination of the S-polynomials $S(f_j, f_k)$ with $1 \leq j, k \leq s$ and each $S(f_j, f_k)$ has multidegree less than δ.*

Proof. We can assume that $\mathrm{LC}(f_i) = 1$ for all i by absorbing the leading coefficient into each c_i. Then the assumption that the multidegree of $\sum c_i f_i$ drops means that $\sum_{i=1}^s c_i = 0$.

Now $\mathrm{LCM}(\mathrm{LM}(f_j), \mathrm{LM}(f_k)) = \mathrm{LCM}(x^\delta, x^\delta) = x^\delta$ and the leading term of each f_i is also x^δ so

$$S(f_j, f_k) = \frac{x^\delta}{x^\delta} f_j - \frac{x^\delta}{x^\delta} f_k = f_j - f_k$$

which has multidegree less than δ.

Now to write $\sum c_i f_i$ as a sum of such terms we use a telescoping sum:

$$\begin{aligned} \sum_{i=1}^s c_i f_i &= c_1(f_1 - f_2) + (c_1 + c_2)(f_2 - f_3) + \ldots + (c_1 + \ldots + c_{s-1})(f_{s-1} - f_s) + (c_1 + \ldots + c_s) f_s \\ &= c_1 S(f_1, f_2) + (c_1 + c_2) S(f_2, f_3) + \ldots + (c_1 + \ldots + c_{s-1}) S(f_{s-1}, f_s) \end{aligned}$$

where the multiple of f_s does not appear in the second line because $\sum_{i=1}^s c_i = 0$. The fact that each of the $S(f_j, f_k)$ has multidegree less than δ implies that this linear combination does also. □

Theorem 3.8 (Buchberger's Criterion)**.** *Let I be an ideal. Then a basis G is a Gröbner basis if and only if for all $i \neq j$ the remainder on division of $S(g_i, g_j)$ by G is zero.*

Proof. We give only the briefest sketch of a proof. See pp 85-87 of [CLO06] for the details.

If G is a Gröbner basis then since $S(g_i, g_j) \in I$, by Corollary 3.5 the remainder on division of $S(g_i, g_j)$ by G is zero. Conversely we need to show that if the remainder of each division is zero then G is a Gröbner basis, that is, show that $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. So take $f \in I$ and we need $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$.

Write $f = \sum h_i g_i$ for polynomial h_i and we have multidegree of f less than or equal to maximum of the multidegree of $h_i g_i$. If there is not equality here then there must be some cancellation and our work on S–polynomials and the assumption on their divisibility allows us to show that we can find an expression for $f = \sum h_i g_i$ where there is equality (this step is where the magic happens). Then it follows that $\mathrm{LT}(f)$ is divisible by some $\mathrm{LT}(g_i)$ as desired. □

3.3 Finding Gröbner bases

The following algorithm gives us a way to find Gröbner bases (although there are many possible practical improvements that we have not included). We use the notation $\overline{f}^F$ for the remainder on division of f by the sequence of polynomials $F = (f_1, \ldots, f_n)$. Note that if F is a Gröbner basis then the order of the f_i doesn't matter.

Theorem 3.9 (Buchberger's Algorithm)**.** *Let $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ be an ideal. Then the following algorithm constructs a Gröbner basis G for I.*

Require: *$F = (f_1, \ldots, f_s)$*
Ensure: *$G = (g_1, \ldots, g_t)$ a Gröbner basis for I with $F \subseteq G$*

```
G = F
repeat
  G' = G
  for each pair {p, q}, p ≠ q ∈ G' do
    S = S(p, q)‾^G'
    if S ≠ 0 then
      G = G ∪ {S}
    end if
  end for
until G == G'
```

Proof. First we show that $G \subseteq I$ at all stages. This is true initially since $F \subseteq I$, and whenever G changes, it is modified by adding an element of the form $\overline{S(p,q)}^{G'}$. Here $p, q \in G'$ so $S(p,q) \in G' \subseteq I$. Thus $\overline{S(p,q)}^{G'}$ is the difference of elements in I so is in I also.

The algorithm terminates when G' equals G which happens only if $\overline{S(p,q)}^{G'} = 0$ for all p, q. Hence at this point G is a Gröbner basis by Buchberger's criterion. Since the size of G can only increase we have $F \subseteq G$.

To see that the algorithm does eventually terminate, notice that after each pass through the main loop where the algorithm doesn't terminate there is some remainder r added to G which is not divisible by the leading term of an element of G'. Thus $\mathrm{LT}(r) \notin \langle \mathrm{LT}(G') \rangle$ but $\mathrm{LT}(r) \in \langle \mathrm{LT}(G) \rangle$ so we have a strict containment $\langle \mathrm{LT}(G') \rangle \subset \langle \mathrm{LT}(G) \rangle$. But if the algorithm didn't terminate we would then have an infinite strictly ascending chain of ideals in $k[x_1, \ldots, x_n]$ which is not possible. □

This algorithm can produce superfluous basis elements. The following lemma allows us to recognize these.

Lemma 3.10. *Let G be a Gröbner basis for an ideal I. If $p \in G$ is a polynomial such that $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \setminus \{p\}) \rangle$ then $G \setminus \{p\}$ is also a Gröbner basis for I.*

Proof. That G is a Gröbner basis implies that $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$. Then the assumption implies that $\langle \mathrm{LT}(G \setminus \{p\})\rangle = \langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$ so $G \setminus \{p\}$ is a Gröbner basis for I also. □

So if we divide each polynomial by its leading coefficient and remove any p that satisfy the above condition we can force a particular form on a Gröbner basis:

Definition 3.11. A *minimal Gröbner basis* for an ideal I is a Gröbner basis G for I such that

(i) $\mathrm{LC}(p) = 1$ for all $p \in G$, and

(ii) for all $p \in G$, $\mathrm{LT}(p) \notin \langle \mathrm{LT}(G \setminus \{p\})\rangle$.

If we go even further we can in fact force the existence of a unique Gröbner basis of a certain form.

Definition 3.12. A *reduced Gröbner basis* for an ideal I is a Gröbner basis G for I such that

(i) $\mathrm{LC}(p) = 1$ for all $p \in G$, and

(ii) for all $p \in G$, no monomial of p lies in $\langle \mathrm{LT}(G \setminus \{p\})\rangle$.

Proposition 3.13. *A nonzero polynomial ideal has a unique reduced Gröbner basis.*

Proof. Let our ideal be I and find a minimal Gröbner basis G for it. Then take $g \in G$ noticing that our minimality constraint gives us that $\mathrm{LT}(g) \notin \langle \mathrm{LT}(G \setminus \{g\})\rangle$. Let $g' = \overline{g}^{G\setminus\{g\}}$ and $G' = (G \setminus \{g\}) \cup \{g'\}$ and notice that $\mathrm{LT}(g') = \mathrm{LT}(g)$ because when we divide g by $G \setminus \{g\}$ the leading term of g must go into the remainder. This shows that $\langle \mathrm{LT}(G')\rangle = \langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$ so G' is a Gröbner basis. It is minimal because $\mathrm{LT}(g') = \mathrm{LT}(g) \notin \langle \mathrm{LT}(G \setminus \{g\})\rangle = \langle \mathrm{LT}(G' \setminus \{g'\})\rangle$.

Now, by construction no monomial of g' is in $\langle \mathrm{LT}(G' \setminus \{g'\})\rangle$ and we say that g' is *reduced* for G'. Notice that g' is also reduced for any other minimal Gröbner basis of I that contains g' and has the same set of leading terms. So we can carry out the process in the first paragraph for each $g \in G$ and each element that has already been reduced will stay reduced for each G' as we do this because we don't change the leading terms.

For uniqueness, first note that if $G = (g_1, \ldots, g_t)$ and $\widetilde{G} = (\tilde{g}_1, \ldots, \tilde{g}_s)$ are both reduced Gröbner bases for I then they have the same leading terms. To see this, take $g_1 \in G$ and then $g_1 = \sum a_i \tilde{g}_i$ and thus we have $\mathrm{LT}(\tilde{g}_i)$ dividing $\mathrm{LT}(g_1)$ for some i. But this also works in the other direction so for some j we have $\mathrm{LT}(g_j)$ dividing $\mathrm{LT}(\tilde{g}_i)$. By minimality this is only possible if $j = 1$ so we must have $\mathrm{LT}(g_1) = \mathrm{LT}(\tilde{g}_i)$ for some i. This works for each g_k and is completely symmetrical so $\mathrm{LT}(G) = \mathrm{LT}(\widetilde{G})$.

So if $g \in G$ there exists $\tilde{g} \in \widetilde{G}$ with $\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$. Then $g - \tilde{g} \in I$ and since G is a Gröbner basis we have $\overline{g - \tilde{g}}^{G} = 0$. But also $\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$ so we have cancellation and since G and $\widetilde{G}$ are reduced none of the terms in the difference are divisible by any elements of G so $\overline{g - \tilde{g}}^{G} = g - \tilde{g}$ so $g = \tilde{g}$. But this works for every $g \in G$ and so $G = \widetilde{G}$. □

This result gives us an algorithm for deciding equality of ideals: two ideals are equal if and only if their reduced Gröbner bases are the same. Most computer algebra systems compute reduced Gröbner bases by default.

4 Computing in SAGE

We use the open source computer algebra system SAGE, described in [SJ05], to do some calculations. SAGE has built-in functions, mainly passing the work off to Singular, to do many of the operations discussed above. We can also use some code written by Jim Carlson that implements the naive algorithms in [CLO06] with the same notation as in this paper, available at `http://www.math.utah.edu/~carlson/cimat/buchberger.sage`.

The first few examples are simple exercises from [CLO06].

Example 4.1. We check if $f = xy^3 - z^2 + y^5 - z^3 \in I = \langle -x^3 + y, x^2y - z\rangle$ by computing a Gröbner basis.

```
sage: R.<x,y,z>=PolynomialRing(QQ)
sage: f=x*y^3-z^2+y^5-z^3
sage: G=Ideal(-x^3+y,x^2*y-z).groebner_basis()
sage: G
[y^2 - x*z, x^2*y - z, x^3 - y]
sage: f.reduce(G)
0
```

The fact that f is zero when reduced modulo G means that $f \in I$.

Example 4.2. We calculate the points of intersection of $x^2 + y^2 + z^2 = 1$, $(x-1)^2 + y^2 + z^2 = 1$ and $2x - 3y = z$ in $\mathbb{C}^3$. To do this, we compute in lex order a Gröbner basis for the ideal $I = \langle x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - 3y - z\rangle$.

```
sage: R.<x,y,z> = PolynomialRing(CC,order='lex')
sage: I=Ideal(x^2+y^2+z^2-1,x^2+y^2+z^2-2*x,2*x-3*y-z)
sage: I.groebner_basis()
[z^2 + (-0.2000)*z - 0.5750, y + 0.3333*z - 0.3333, x - 0.5000]
```

This tells us that $I = \langle z^2 - 1/5z - 5/8, y + 1/3z - 1/3, x - 1/2\rangle$. Notice that all variables except the z variable, last in lex order, have been eliminated in the first equation of our basis. Solving this system of equations is a simple 'back substitution' yielding two solutions $(1/2, (18 + \sqrt{254})/60, (2 - \sqrt{254})/20)$ and $(1/2, (18 - \sqrt{254})/60, (2 + \sqrt{254})/20)$.

Example 4.3. We find an implicit description of the surface S in $\mathbb{R}^3$ formed by taking the union of straight lines joining pairs of points on the lines $(x, y, z) = (t, 0, 1)$ and $(x, y, z) = (0, 1, t)$ with the same value of t.

Such a line has the equation $(x, y, z) = u(t, 0, 1) + (1 - u)(0, 1, t) = (ut, 1 - u, u + t - ut)$ so consider the ideal $I = \langle x - ut, y - 1 + u, z - u - t + ut\rangle$.

```
sage: R.<t,u,x,y,z>=PolynomialRing(CC,order='lex')
sage: I=Ideal(x-u*t,y-1+u,z-u-t+u*t)
sage: G=I.groebner_basis()
sage: G
[x*y + y^2 + y*z + (-2.0000)*y - z + 1.0000, u + y - 1.000, t - x - y - z + 1.000]
```

This calculation shows that $S \subseteq V(xy + y^2 + yz - 2y - z + 1)$. To see that this is in fact an equality, given $(x, y, z) \in V(xy + y^2 + yz - 2y - z + 1)$ we can take $u = 1 - y$ and $t = x + y + z - 1$. Then $ut = x + y + z - 1 - yx - y^2 - yz + y = x$, $1 - u = y$ and $u + t - ut = 1 - y + x + y + z - 1 - x = z$ so $(x, y, z) \in S$.

5 Some problems from Shafarevich

We give solutions to some problems from Shafarevich's text. The amount of work that Gröbner basis techniques save us will be seen to be variable but sometimes the change in perspective is just as interesting.

Problem 1. Let $X = V(y^2 - x^3) \subset \mathbb{A}^2$. Show that every element of $k[X]$ can be written uniquely in the form $P(x) + Q(x)y$ with P, Q polynomials.

Solution. We use lex order with $y > x$. Note that $I = (y^2 - x^3) \subset k[x, y]$ is a Gröbner basis because $\mathrm{LT}(I) = (y^2) = (\mathrm{LT}(y^2 - x^3))$. So division by $y^2 - x^3$ gives a well-defined remainder with y^2 not dividing any term of the remainder. So $f \in k[x, y]$ can be written as $f = h(y^2 - x^3) + r$ with $r(x, y) = P(x) + Q(x)y$ uniquely defined. Then in $k[X]$ we have the desired result. $\Diamond$

Problem 2. Decompose into irreducible components the closed set $X = V(y^2 - xz, z^2 - y^3)$. Show each component is birational to $\mathbb{A}^1$.

Solution. We find a Gröbner basis for $I = (y^2 - xz, z^2 - y^3)$ to be $I = (y^2 - xz, xyz - z^2, x^2z^2 - yz^2)$. This suggests looking at the case $z = 0$ which implies that $y = 0$ and x is arbitrary and the case $z \neq 0$ which using back substitution shows that $y = x^2$ and $z = x^3$. Thus the two components are the x-axis and a twisted cubic both of which are birational to $\mathbb{A}^1$. $\Diamond$

References

[Buc65] B. Buchberger. *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal (German).* PhD thesis, University of Insbruck, Austria, 1965.

[CLO06] D.A. Cox, J.B. Little, and D. O'Shea. *Ideals, varieties, and algorithms.* Springer, 2006.

[Sha94] I.R. Shafarevich. *Basic Algebraic Geometry.* Springer-Verlag, 1994.

[SJ05] William Stein and David Joyner. SAGE: System for Algebra and Geometry Experimentation. *Communications in Computer Algebra*, 39(2), 2005.