An Introduction to Gröbner Bases

Anwyn Woodyatt

April 11, 2023

Abstract

The aim of this paper is to provide an undergraduate friendly introduction to the concept of Gröbner bases. After motivating the subject, we build a solid foundation before formally defining, proving the existence of, and providing the original Buchberger's algorithm to compute, said Gröbner basis. We conclude by briefly summarizing a few applications.

1 Prerequisites

It is expected that the reader has completed an undergraduate course in ring theory and/or is familiar with multi-variable polynomial ring concepts and results. We highlight a few of these which are used directly in definitions and proofs.

Definition 1. Let K be a field (in more generality, K can be any commutative ring). A *monomial* in the polynomial ring $K[x_1, ..., x_n]$ is represented by cx^α where c is an element of K, $x = (x_1, ..., x_n)$ and $\alpha = (a_1, ..., a_n)$ in $\mathbb{Z}^n_{\geq 0}$. For example, x^2y^3.

Lemma 1. ([1]) Let $I = \langle x^\alpha \mid \alpha \in S \subseteq \mathbb{Z}^n_{\geq 0} \rangle$ be a monomial ideal (ideal generated by monomials) in $K[x_1, ..., x_n]$. Then, a monomial x^β is an element of I if and only if x^α divides x^β for some α in S.

Definition 2. A commutative ring with unity K is called *Noetherian* if and only if for every increasing chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$ of K, there exists N in $\mathbb{Z}_{\geq 0}$ such that $I_n = I_N$ for all $n \geq N$.

We have an equivalent definition of Noetherian:

Definition 2. A commutative ring with unity K is called *Noetherian* if and only if every ideal of K is finitely generated.

Theorem 1 (Hilbert Basis Theorem). ([2]) If K is a Noetherian ring then $K[x]$ is a Noetherian ring. Inductively, $K[x_1, ..., x_n]$ is a Noetherian ring.

Proposition 1. ([2]) Every field is Noetherian.

2 Introduction

In his 1965 Ph.D. thesis, Bruno Buchberger introduced the new concept of a *Gröbner basis*, named after his advisor Wolfgang Gröbner. He provided the *Buchberger Algorithm* to compute them (the one we will state and prove in this paper) at the same time ([3]).

We acknowledge that many years earlier in 1913, Nikolai Günther of Russia made a similar discovery; his work was published in Russian journals but ignored internationally until it was recognized in the 1980s ([3]).

The Buchberger algorithm is motivated by what is known as the *Ideal Membership Problem* (6) which asks: given a field K and an ideal I of $K[x_1, ...x_n]$, how can we determine if f in $K[x_1, ..., x_n]$ is an element of I? We know that for a commutative ring, we can write an element of I as a linear combination of the generators. Thus, as one would do in the single variable case, it would be intuitive to divide our polynomial by the generators of I simultaneously using the division algorithm for multi-variable polynomial rings (3), and if the algorithm terminates with zero remainder, we have an element of I. Alas, we will show in the following section that we run into several issues using this method. Namely, unlike the division algorithm in one variable, the multi-variable division algorithm does not output a unique remainder unless the order of divisors is fixed. Consequently, an element of I can have a non-zero remainder. This dilemma says that zero remainder is *sufficient* for ideal membership but not *necessary*. We are left to wonder: can we find a basis such that the unique remainder is independent of divisor order, thus providing a sufficient *and* necessary way to determine elements of I? Indeed! The Gröbner basis of I!

This relatively modern idea has led to many fascinating applications and discoveries in mathematics and science.

3 Ordering and Division Algorithm in $K[x_1, ..., x_n]$

In one variable, we are familiar with the terms *degree* of a *monomial*, and *degree* of a *polynomial*. For example, $4x^2$ is a degree 2 monomial and $4x^2+x+1$ is a degree 2 polynomial in $\mathbb{Q}[x]$. How do these definitions change for multi-variable polynomials?

Let us consider the two variable case: $\mathbf{x} = (x, y)$. Suppose you have the monomials x^2y and xy^2. Both have the same *total degree* $(1 + 2 = 2 + 1 = 3)$. Which one would you define as greater than the other? In fact, it depends on the definition of *monomial ordering* you choose. We provide a few common examples of monomial orderings before outlining the formal criteria.

Definition 3. (Lexicographic Order) Let $\alpha = (a_1, ..., a_n)$, $\beta = (b_1, ..., b_n) \in \mathbb{Z}^n_{\geq 0}$. If $\alpha - \beta$ has a positive leftmost non-zero entry, then we say the degree α is greater than the degree β with respect to lexicographic ordering, abbreviated as $\alpha >_{lex} \beta$. We can equivalently say that x^α is greater than x^β as monomials.

Example. $x > y > z$ since $x = x^1y^0z^0$, $y = x^0y^1z^0$, $z = x^0y^0z^1$ and
$(1, 0, 0) - (0, 1, 0) = (1, -1, 0)$, $(0, 1, 0) - (0, 0, 1) = (0, 1, -1)$, i.e. we have alphabetical

ordering.

Definition 4. (Graded Lex Order) Let α, β as above. If

$$|\alpha| = \sum_{i=1}^{n} a_i > |\beta| = \sum_{i=1}^{n} b_i$$

or

$$|\alpha| = |\beta| \; and \; \alpha >_{lex} \beta,$$

then we say $\alpha >_{grlex} \beta$.
$|\alpha|$ is denoted the *total degree*.

Example. We first notice that again we have alphabetical ordering of the variables.
Another example is $x^4y^7z >_{grlex} x^4y^2z^3$ since $|(4,7,1)| = 12 > 9 = |(4,2,3)|$.

Definition 5. (Graded Reverse Lex Order) Let α, β as above. If

$$|\alpha| = \sum_{i=1}^{n} a_i > |\beta| = \sum_{i=1}^{n} b_i$$

or

$$|\alpha| = |\beta| \; and \; the \; rightmost \; nonzero \; entry \; of \; \alpha - \beta \; is \; negative,$$

then we say $\alpha >_{grevlex} \beta$.

Example. We have the same example as above: $x^4y^7z >_{grevlex} x^4y^2z^3$ because *grevlex* and *grlex* both order by total degree first, but break ties in different ways.
Another example is $(2,3,2) >_{grevlex} (0,0,7)$ since $(2,3,2) - (0,0,7) = (2,3,-5)$.

Definition 6. We call $>$ a *monomial ordering* on the set of monomials $\{x^\alpha \mid x = (x_1, ..., x_n),\ \alpha \in \mathbb{Z}^n_{\geq 0}\}$ in $K[x_1, ..., x_n]$ if it is a relation satisfying the following conditions:
(i) $>$ is a *total* (linear) ordering, i.e. exactly one of

$$x^\alpha > x^\beta,\ x^\alpha = x^\beta,\ x^\beta > x^\alpha$$

is true and the ordering in *transitive*.
(ii) If $x^\alpha > x^\beta, \gamma \in \mathbb{Z}^n_{\geq 0}$, then $x^{\alpha+\gamma} > x^{\beta+\gamma}$
(iii) $>$ is a *well-ordering*, i.e. there exists a (not necessarily unique) minimal monomial.

From now on, $>$ represents an arbitrary fixed monomial ordering. You may be wondering... Do we *have* to impose an ordering? If we do not, then we also run into uniqueness of remainder problems as mentioned in the introduction.

We need just a few more pieces of terminology before we have the foundation to discuss Gröbner bases.

Definition 7. Let $f = \sum_{i=1}^{n} c_i x^{\alpha_i}$ in $K[x_1, ..., x_n]$ (without loss of generality, none of the α_i are equal, otherwise combine them). The *leading term* of f, $LT(f) = c_k x^{\alpha_k}$, is such that $\alpha_k > \alpha_i$ for all i. c_k is denoted the *leading coefficient*.

Definition 8. As above, let $f = \sum_{i=1}^{n} c_i x^{\alpha_i}$ be a polynomial in $K[x_1, ..., x_n]$. The *leading monomial* of f is $LM(f) = x^{\alpha_k}$ such that $\alpha_k > \alpha_i$ for all i.

Remark Note that we distinguish the leading monomial as the leading term without its coefficient. This is different than the general definition of a monomial.

For the definition and proof of the *division algorithm* in $K[x_1, ..., x_n]$, we reference [1] (chapter 2.3). The computation is easy to grasp by examples, which follow. Like normal division, we have a divisor, dividend, quotient and remainder; what's different is that we can have multiple divisors and quotients. Take a peak at the example below to familiarize yourself with the setup.

Essentially, we start by fixing a monomial ordering. This determines leading terms. Then, we apply the division algorithm as we normally would in one variable to the top most divisor (which we will call f_1) and the dividend. That is, we ask, what can we multiply the leading term of f_1 by to get the leading term of the dividend? For example, xy can be multiplied by x to get x^2y below.

Dividing by f_1 builds quotient one. If in any particular step we cannot divide by divisor one (for example, xy cannot be multiplied by anything to get y^2 below), we leave quotient one empty, move to f_2 and build quotient two, and so on. At each step we return to f_1 and work down the list.

If at any step we cannot divide the leading term by *any* of the divisors, that leading term becomes the remainder of that step (bold below) and we continue the division by carrying down the rest of the terms. At the end, we add the remainders of each step for a total remainder.

As we will see in the coming examples, the choice of ordering can simplify or complicate polynomial division in $K[x_1, ..., x_n]$ (sometimes greatly). We also see that, unless order of divisors is fixed, the remainder is not unique — even with a fixed ordering.

The following problems and the worked example in 4 are taken from [1], where additional examples and exercises can be found, but worked out independently.

Example. Order of divisors matters. We use *lex* ordering in the following two divisions and work in $\mathbb{Q}[x, y]$.

To begin, the polynomials are ordered (greatest monomial to the left). Step one is multiplying $xy-1$ by x to get the leading term of the dividend. We write the product below the dividend and subtract, and add x to quotient one.

$$\begin{array}{r} {\scriptstyle q_1=x} \\ {\scriptstyle q_2=} \\ \hline {\scriptstyle f_1=xy-1} \\ {\scriptstyle f_2=y^2-1} \end{array} \overline{\big) \; x^2y + xy^2 + y^2} \\ \underline{-\quad (x^2y - x)} \\ xy^2 + x + y^2$$

Step two is multiplying $xy - 1$ by y to get the leading term of the difference. We write the

new product below the first difference and subtract, and add y to quotient one. We encourage the reader to follow through the remaining steps.

$$
\begin{array}{r}
\overset{q_1=x+y}{\overset{q_2=1}{}} \\
\hline
f_1=xy-1,\ f_2=y^2-1 \big) \; x^2y + xy^2 + y^2 \\
\underline{-\quad (x^2y - x)\qquad\quad} \\
xy^2 + x + y^2 \\
\underline{-\quad (xy^2 - y)\quad} \\
\mathbf{x} + y^2 + y \\
\underline{\qquad\quad (y^2 - 1)} \\
\mathbf{y} + 1 \\
\underline{\qquad\quad\ \ 1}
\end{array}
$$

We finish with remainder $\mathbf{x}+\mathbf{y}+\mathbf{1}$.
We conclude that $x^2y + xy^2 + y^2 = (x + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + x + y + 1$.

On the other hand, switching the order of divisors gives

$$
\begin{array}{r}
\overset{q_1=x+1}{\overset{q_2=x}{}} \\
\hline
f_1=y^2-1,\ f_2=xy-1 \big) \; x^2y + xy^2 + y^2 \\
\underline{-\quad (x^2y - x)\qquad\quad} \\
xy^2 + x + y^2 \\
\underline{-\quad (xy^2 - x)\quad} \\
\mathbf{2x} + y^2 \\
\underline{\qquad\quad\ \ y^2} \\
\underline{-\quad (y^2 - 1)} \\
\mathbf{1}
\end{array}
$$

with remainder $\mathbf{2x}+\mathbf{1}$ — a different remainder!
We conclude that $x^2y + xy^2 + y^2$ can also be written as $(x + 1) \cdot (y^2 - 1) + x \cdot (xy - 1) + 2x + 1$.

We now compute the second division again, this time using *grlex* ordering:

$$
\begin{array}{r}
\overset{q_1=x+1}{\overset{q_2=x}{}} \\
\hline
f_1=y^2-1,\ f_2=xy-1 \big) \; x^2y + xy^2 + y^2 \\
\underline{-\quad (x^2y - x)\qquad\quad} \\
xy^2 + y^2 + x \\
\underline{-\quad (xy^2 - x)\quad} \\
y^2 + 2x \\
\underline{\qquad\quad (y^2 - 1)} \\
\mathbf{2x}+\mathbf{1}
\end{array}
$$

We highlight that we were able to continue dividing by d_1 at row 5, unlike before, because $y^2 >_{grlex} 2x$ whereas $2x >_{lex} y^2$.

4 Algorithm to Construct Gröbner Bases and Proof of Existence

The preceding section brings to light the obstacle that the Ideal Membership Problem faces. With a fixed ordering, we now construct a new basis from our original basis of I such that division in any order of this new basis results in a unique remainder.

Definition 9. Let K be a field. Let I be an ideal of $K[x_1, ..., x_n]$. We say the subset $G = \{g_1, ..., g_d\}$ of I is a *Gröbner basis* (with respect to fixed ordering) for I if $\langle LT(g_1), ..., LT(g_d)\rangle = \langle LT(I)\rangle$, where $\langle LT(I)\rangle$ is the ideal generated by the set of leading terms of elements of I.

Remark 1. G generates I; that is, $\langle g_1, ..., g_d\rangle = I$.

Proof. $\langle g_1, ..., g_d\rangle$ is contained in I since G is contained in I, by the properties of ideals. Conversely, let f be an element of I. We can write $f = p_1g_1 + ... + p_dg_d + r$ for some remainder r using the division algorithm. Since f is in I, $r = f - p_1g_1 + ... + p_dg_d$ is an element of I. Assume r is non-zero. By the definition of Gröbner basis then, $LT(r)$ is in $\langle LT(g_1), ..., LT(g_d)\rangle$, and by Lemma 1 some $LT(g_i)$ divides $LT(r)$. But this contradicts that r is the smallest remainder, thus r must be zero, and f is in $\langle g_1, ..., g_d\rangle$.

□

Remark 2. Note that by 1, since K is a field, K is Noetherian, and thus $K[x_1, ..., x_n]$ is Noetherian. Hence, every ideal in $K[x_1, ..., x_n]$ is finitely generated. The existence of this generating set is what we will eventually build a Gröbner basis from. A Gröbner basis is a specific kind of basis, and in fact is more of a spanning set unless minimal, and non-unique unless reduced 5.

Definition 10. Let x^α, x^β be monomials. Let $\text{lcm}\,(x^\alpha, x^\beta) = x^\gamma$, $\gamma = (c_1, ...c_n)$ and $c_i = max\{a_i,\ b_i\}$. We define the $S - polynomial$: $S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g$ where $x^\gamma = \text{lcm}\,(LM(f), LM(g))$.

Theorem 2 (Buchberger's Criterion). Let I be an ideal of $K[x_1, ..., x_n]$ such that $I = \langle g_1, ...g_d\rangle$. Then $G = \{g_1, ..., g_d\}$ is a Gröbner basis if and only if $\overline{S(g_i, g_j)}^G = 0$ for all i, j in $\{1, ..., d\}$, where $\overline{S(g_i, g_j)}^G$ denotes the remainder of $S(g_i, g_j)$ divided by G.

Proof. ($\Leftarrow$:) We need to show that $\langle LT(g_1), ...LT(g_d)\rangle = \langle LT(I)\rangle$.

$\langle LT(g_1), ...LT(g_d)\rangle \subseteq \langle LT(I)\rangle$ is clear since g_i in I implies $LT(g_i)$ is in $\langle LT(I)\rangle$ for all i in $\{1, ..., d\}$. Thus $\langle LT(g_1), ...LT(g_d)\rangle \subseteq \langle LT(I)\rangle$ since $\langle LT(I)\rangle$ is closed under finite linear combinations and an arbitrary element of $\langle LT(g_1), ...LT(g_d)\rangle$ is written $f_1LT(g_1) + ... + f_dLT(g_d)$ for f_i in $K[x_1, ..., x_n]$.

It remains to show that $\langle LT(I)\rangle \subseteq \langle LT(g_1), ...LT(g_d)\rangle$, and by the same reasoning as above, it is sufficient to show that $LT(I) \subseteq \langle LT(g_1), ...LT(g_d)\rangle$. Let f be arbitrary in I and $LT(f) = a_n x^{\alpha_n}$ in $LT(I)$. Write:

$$f = a_n x^{\alpha_n} + a_{n-1}x^{\alpha_{n-1}} + ... + a_0 = \sum_{i=1}^{d} h_i g_i, h_i \in K[x_1, ..., x_n]$$

We can write f this way since $I = \langle g_1, ..., g_d\rangle$.
By Lemma 1, we need to show that $a_n x^{\alpha_n}$ is divisible by one of $LT(g_i), ..., LT(g_d)$.
Let $\delta = max(deg(h_i g_i))$. There are two cases:

1. $\delta = deg(f) = \alpha_n$, the case with no cancellation in the sum of f.

2. $\delta > deg(f)$, the case with cancellation in the sum of f.

Let's deal with case 1 first, then we will produce $f = \sum_{i=1}^{d} h_i' g_i$ such that $max(deg(h_i' g_i)) = \delta'$ is strictly less than δ, so we can inductively reduce to case 1.

Suppose $f = h_1 g_1 + ... + h_d g_d$ with $deg(f) = \delta$ and $deg(h_i g_i) \leq \delta$ (at least one equality). Then for some i in $\{1, ..., d\}, LM(f) = LM(h_i g_i) = LM(g_i)LM(h_i)$. So in this case, $LM(g_i)$ divides $LM(f)$. This gives that $LT(g_i)$ divides $LT(f)$ since $LM(f) = x^\delta = LM(h_i)LM(g_i)$ implies

$$\begin{aligned} a_n x^\delta &= a_n LM(h_i)LM(g_i) \\ &= \frac{a_n}{b_i} LM(h_i) \cdot b_i LM(g_i) \\ &:= \frac{a_n}{b_i} LM(h_i)LT(g_i) \end{aligned}$$

where $b_i \neq 0$ since $LT(g_i) \neq 0$. This gives case 1.

We now look at **case 2**. We will need a lemma which we state and prove now.

Lemma 2. If $deg(p_i) = \delta$ for all i and $deg(\sum_{i=1}^{n} p_i) < \delta$, then there exists a_{ij} in K such that $\sum_{i=1}^{n} p_i = \sum_{i,j}^{n} a_{ij} S(p_i, p_j)$.

Proof. Write $S(p_i, p_j) = \frac{x^\delta}{LT(p_i)} \cdot p_i - \frac{x^\delta}{LT(p_j)} \cdot p_j$ where $LT(p_i) = b_i x^\delta$ and $LT(p_j) = b_j x^\delta$.

Fix j. Then,

$$\begin{aligned} \sum_{\substack{i=1 \\ i\neq j}}^{n} b_i(\frac{p_i}{b_i} - \frac{p_j}{b_j}) &= \sum_{\substack{i=1 \\ i\neq j}}^{n} (p_i - \frac{b_i}{b_j} p_j) \\ &= \sum_{\substack{i=1 \\ i\neq j}}^{n} p_i - \frac{p_j}{b_j} \sum_{\substack{i=1 \\ i\neq j}}^{n} b_i \\ &= \sum_{i=1}^{n} p_i \end{aligned}$$

where $(\frac{p_i}{b_i} - \frac{p_j}{b_j}) = S(p_i, p_j)$ and $\sum_{\substack{i=1 \\ i \neq j}}^{n} b_i = 0$ since the sum has degree less than δ.

□

Continuing, we now write

$$f = \sum_{deg(h_i g_i) > deg(f)} h_i g_i + \sum_{deg(h_i g_i) \leq deg(f)} h_i g_i$$

and since $deg(h_i g_i) = \delta$ implies $deg(LT(h_i)g_i) = \delta$ by well-ordering, we have

$$\begin{aligned} &= \sum_{deg(h_i g_i) = \delta} LT(h_i)g_i + \sum_{deg(h_i g_i) = \delta} (h_i - LT(h_i))g_i \\ &+ \sum_{deg(f) < deg(h_i g_i) < \delta} h_i g_i + \sum_{deg(h_i g_i) \leq deg(f)} h_i g_i \end{aligned}$$

where the first sum must have degree less than δ and the second sum subtracts $LT(h_i)$, thus has degree less than δ.

Using Lemma 2 above, there exists a_{ij} such that

$$\begin{aligned} \sum_{deg(h_i g_i) = \delta} LT(h_i)g_i &= \sum_{i,j}^{d} a_{ij}\, S(LT(h_i)g_i, LT(h_j)g_j) \\ &= \sum_{i,j}^{d} a_{ij}\, (\frac{x^\delta}{LT(h_i g_i)} LT(h_i)g_i - \frac{x^\delta}{LT(h_j g_j)} LT(h_j)g_j\ ) \\ &= \sum_{i,j}^{d} a_{ij}\, (\frac{x^\delta}{LT(h_i)LT(g_i)} LT(h_i)g_i - \frac{x^\delta}{LT(h_j)LT(g_j)} LT(h_j)g_j\ ) \\ &= \sum_{i,j}^{d} a_{ij}\, (\frac{x^\delta}{x^{\alpha_{ij}}} \frac{x^{\alpha_{ij}} g_i}{LT(g_i)} - \frac{x^\delta}{\alpha_{ij}} \frac{x^{\alpha_{ij}} g_j}{LT(g_j)}\ ) \\ &= \sum_{i,j}^{d} \frac{x^\delta}{x^{\alpha_{ij}}}\, a_{ij}\, S(g_i, g_j) \end{aligned}$$

where we use that $LT(LT(h_k g_k)) = LT(h_k g_k)$ and $LT(h_k g_k) = LT(h_k)LT(g_k)$ by well-ordering, and $x^{\alpha_{ij}} = \text{lcm}(LM(g_i)LM(g_j))$.

Now by assumption, $\overline{S(g_i, g_j)}^{G} = 0$, so $S(g_i, g_j) = \sum_{k=1}^{d} p_k g_k$ with $deg(p_k g_k)$ less than or equal to $deg(S(g_i, g_j))$, which is strictly less than α_{ij}, where the first inequality follows from the division algorithm and the second since $S(g_i, g_j)$ cancels the leading term.

Consequently we have

$$\sum_{deg(h_i g_i)=\delta} LT(h_i)g_i = \sum_{i,j}^{d} \frac{x^\delta}{x^{\alpha_{ij}}}\, a_{ij} \sum_{k=1}^{d} p_k g_k$$
$$= \sum_{i,j}^{d} \sum_{k=1}^{d} \frac{x^\delta}{x^{\alpha_{ij}}} p_k g_k$$

with degree strictly less than δ.

This concludes case 2 and the reverse direction.

($\Rightarrow$:) We need to show that $\overline{S(g_i, g_j)}^G = 0$ for all (g_i, g_j) in G under the assumption that $G = \{g_1, ..., g_d\}$ is Gröbner.

$S(g_i, g_j) = \frac{x^\gamma}{LT(g_i)} \cdot g_i - \frac{x^\gamma}{LT(g_j)} \cdot g_j$ in I implies $LT(S(g_i, g_j))$ in $\langle LT(I)\rangle = \langle LT(g_i), ..., LT(g_d)\rangle$,

so we can move to the next step of the division algorithm without remainder by dividing by some $LT(g_k)$ by Lemma 1.

The next step is dividing $S(g_i, g_j) - (\frac{LT(S(g_i,g_j))}{LT(g_k)} \cdot g_k)$ (in I) by G. By same reasoning as above, we can move to the next step.

The division algorithm terminates by well-ordering, thus we conclude that

$$\overline{S(g_i, g_j)}^G = 0.$$

This concludes the proof.

□

This constructs an algorithm (**Buchberger's Algorithm**) to construct a Gröbner basis from an original generating set G, by adding $\overline{S(g_i, g_j)}^G \neq 0$ to G, and repeating the process with this newly defined G until $\overline{S(g_i, g_j)}^G = 0$ for all $i, j \in \{1, ..., n\}$.

Proposition 2. The Buchberger Algorithm terminates.

Proof. Let $G = \{g_1, ...g_d\}$ be a potential Gröbner basis. If $\overline{S(g_i, g_j)}^G \neq 0$, let $G' = G \cup \{\overline{S(g_i, g_j)}^G\}$. We note that

$$S(g_i, g_j) = \sum_{i=1}^{d} p_i g_i + \overline{S(g_i, g_j)}^G$$

implies $\overline{S(g_i, g_j)}^G$ is in I. So $G \subsetneq G'$. We also have that $\langle LT(G)\rangle \subsetneq \langle LT(G')\rangle$, otherwise $\overline{S(g_i, g_j)}^G$ would not be the remainder. Suppose that the algorithm never terminates. This would imply that

$$\langle LT(G)\rangle \subsetneq \langle LT(G')\rangle \subsetneq \langle LT(G'')\rangle \subsetneq ...$$

which contradicts that $K[x_1, ..., x_n]$ is Noetherian.

Thus, the Buchberger Algorithm terminates.

□

Corollary 1. A Gröbner basis always exists.

Proof. Directly follows from the Buchburger Algorithm and Proposition 2.

□

We provide a working example of the construction of a Gröbner basis using *grlex* ordering.

Example. Let $G_1 = \{x^3 - 2xy, x^2y - 2y^2 + x\}$, $f_1 := x^3 - 2xy$, $f_2 := x^2y - 2y^2 + x$, our potential Gröbner basis. We test this hypothesis in $grlex$:

$S(f_1, f_2) = y \cdot (x^3 - 2xy) - x \cdot (x^2y - 2y^2 + x) = -x^2 := f_3$
$\overline{S(f_1, f_2)}^{G_1} = f_3 \neq 0$ (we omit this division calculation since the remainder occurs immediately)
Since $\overline{S(f_i, f_j)}^{G_1}$ is non-zero for some i, j, G_1 is not a Gröbner basis.

Now let $G_2 = \{f_1, f_2, f_3\}$.
$\overline{S(f_1, f_2)}^{G_2} = 0$ (due to above)
$S(f_1, f_3) = (x^3 - 2xy) - (-x) \cdot (-x^2) = -2xy := f_4$
$\overline{S(f_1, f_3)}^{G_2} = f_4 \neq 0$ (we omit this division calculation since the remainder occurs immediately)
Similarly, since $\overline{S(f_i, f_j)}^{G_2}$ is non-zero for some i, j, G_2 is not a Gröbner basis.

Continuing, let $G_3 = \{f_1, f_2, f_3, f_4\}$
$\overline{S(f_1, f_2)}^{G_3} = 0$ (as before)
$\overline{S(f_1, f_3)}^{G_3} = 0$ (due to above)
$S(f_1, f_4) = y \cdot (x^3 - 2xy) - (-\frac{1}{2}x^2) \cdot (-2xy) = -2xy^2$
$\overline{S(f_1, f_4)}^{G_3} = 0$ (we omit this division calculation since it is only one step)
$S(f_2, f_3) = (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x := f_5$
$\overline{S(f_2, f_3)}^{G_3} = f_5 \neq 0$ (we omit this division calculation since the remainder occurs immediately)

Let $G_4 = \{f_1, f_2, f_3, f_4, f_5\}$
$\overline{S(f_1, f_2)}^{G_4} = \overline{S(f_1, f_3)}^{G_4} = \overline{S(f_1, f_4)}^{G_4} = 0$, as before.
By adding f_5 we have $\overline{S(f_2, f_3)}^{G_4} = 0$.

It remains to check that
$\overline{S(f_1,f_5)}^{G_4}$, $\overline{S(f_2,f_4)}^{G_4}$, $\overline{S(f_2,f_5)}^{G_4}$, $\overline{S(f_3,f_4)}^{G_4}$, $\overline{S(f_3,f_5)}^{G_4}$, $\overline{S(f_4,f_5)}^{G_4} = 0$.

Note that we do not need to check $S(f_2,f_1)$ etc. since $S(f_i,f_j) = -S(f_j,f_i)$, $1 \le i < j \le 5$, and -1 clearly does not affect divisibility as a unit.

$S(f_1,f_5) = y^2 \cdot (x^3 - 2xy) - (-\frac{1}{2}x^3) \cdot (-2y^2 + x) = -2xy + \frac{1}{2}x^4$
We now compute $\overline{S(f_1,f_5)}^{G_4}$:

$$
\begin{array}{r|l}
 & \begin{array}{l} q_1{=}\frac{1}{2}x \\ q_2{=}{-}1 \\ q_3{=}0 \\ q_4{=}1 \\ q_5{=}1 \end{array} \\
\begin{array}{l} f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \end{array} & -2xy + \frac{1}{2}x^4 \\
\hline
 & \underline{-\ (-2xy)} \\
 & \frac{1}{2}x^4 \\
 & \underline{-\ (\frac{1}{2}x^4 - x^2y)} \\
 & -x^2y \\
 & \underline{-\ (-x^2y + 2y^2 - x)} \\
 & -2y^2 + x \\
 & \underline{-\ (-2y^2 + x)} \\
 & 0
\end{array}
$$

Note that this is not the only way to solve $\overline{S(f_1,f_5)}^{G_4}$. Since we are free to choose the order of divisors to compute the remainder, we see that we also get 0 remainder for

$$
\begin{array}{r|l}
 & \begin{array}{l} q_4{=}1 \\ q_3{=}{-}\frac{1}{2}x^2 \\ \cdots \end{array} \\
\begin{array}{l} f_4 \\ f_3 \\ \cdots \end{array} & -2xy + \frac{1}{2}x^4 \\
\hline
 & \underline{-\ (-2xy)} \\
 & \frac{1}{2}x^4 \\
 & \underline{-\ (\frac{1}{2}x^4)} \\
 & 0
\end{array}
$$

Similarly, one can show the remaining $\overline{S(f_i,f_j)}^{G_4} = 0$, so we conclude that G_4 is a Gröbner basis for $\langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$ with respect to *grlex*.

5 Minimal and Reduced Gröbner Basis

We briefly state and discuss the concept of a minimal and reduced Gröbner basis.

Definition 11. Let $G = \{g_i, ..., g_n\}$ be a Gröbner basis. A *minimal Gröbner basis* is one such that all leading coefficients equal 1 and is free of any g_i such that $LT(g_i)$ is in $\langle LT(G\backslash\{g_i\})\rangle$.

Remark 3. $G\backslash\{g_i\}$ is still a Gröbner basis since $\langle LT(G)\rangle = \langle LT(G\backslash\{g_i\})\rangle$.

An ideal I does not have a unique minimal Gröbner basis, although given a minimal Gröbner basis G, $\langle LT(G)\rangle$ forms the unique minimal basis of $\langle LT(I)\rangle$ ([1]).

However, for $I \neq \{0\}$, I does have a unique *reduced* Gröbner basis for a given monomial ordering ([1]):

Definition 12. A *reduced Gröbner basis* G is one such that all leading coefficients equal 1, and for any g_i in G, no monomial of g_i is an element of $\langle LT(G\backslash\{g_i\})\rangle$.

6 The Ideal Membership Problem

How does the existence of a Gröbner basis solve the classical Ideal Membership problem introduced in 2?

Theorem 3. Let $G = \{g_1, ..., g_d\}$ be a Gröbner basis for an ideal I of $K[x_1, ..., x_n]$. Then the remainder when dividing an element f of $K[x_1, ..., x_n]$ by G is independent of the ordering of g_i.

Proof. The division algorithm gives existence of such a remainder. To show uniqueness, let $f = p_1g_1 + ... + p_dg_d + r_1 = q_1g_1 + ... + q_dg_d + r_2$ in $K[x_1, ..., x_n]$ have two distinct remainders. This gives that $0 = p_1g_1 + ... + p_dg_d - q_1g_1 - ... - q_dg_d = r_1 - r_2$ is in I. Thus, $LT(r_1 - r_2)$ is in $\langle LT(g_1), ..., LT(g_d)\rangle$ by the definition of Gröbner basis, and by Lemma 1 some $LT(g_i)$ divides $LT(r_1 - r_2)$. This is a contradiction since no terms of r_1 nor r_2 are divisible by any $LT(g_i)$. We conclude that $r_1 - r_2$ must be zero.

□

Corollary 2. The remainder of f after dividing by Gröbner basis of I yields 0 if and only if f is in I itself.

Proof. This is a direct result from Theorem 3, but we write a full proof.

($\Rightarrow$:) Remainder 0 gives $f = p_1g_1 + ... + p_dg_d$ for p_i in $K[x_1, ..., x_n]$ and g_i in G, so f is an element of I as written as a linear combination of elements of G.

($\Leftarrow$:) (This is identical to Remark 1) We can write $f = p_1g_1 + ... + p_dg_d + r$ for some remainder r using the division algorithm. Since f is in I, $r = f - p_1g_1 + ... + p_dg_d$ is an element of I. Assume r is non-zero. By the definition of Gröbner basis then, $LT(r)$ is in $\langle LT(g_1), ..., LT(g_d)\rangle$, and by Lemma 1 some $LT(g_i)$ divides $LT(r)$. But this contradicts that r is the smallest remainder, thus r must be zero.

□

7 Some Applications in Number Theory

Theoretically, a Gröbner basis exists for any ideal in a polynomial ring over any field K. In particular, this is true for algebraic number fields $\mathbb{Q}(\alpha)$, for algebraic number α. The study of algebraic number fields (finite extensions of the field $\mathbb{Q}$) is central to algebraic number theory, and is introduced in an undergraduate course in number theory. As we have seen, Gröbner bases allow us to study ideals in polynomial rings over such fields.

Another classical application of Gröbner bases is in finding solutions to systems of polynomial equations. For a system of polynomial equations, we can translate this system into an equivalent system equating to zero. We can then study the ideal generated by polynomials and the *affine variety* $\mathbf{V}(I)$:

Definition 13. For an ideal I of $K[x_1, ..., x_n]$, we define

$$\mathbf{V}(I) = \{(a_1, ..., a_n) \in K^n \mid f(a_1, ..., a_n) = 0 \, \forall \, f \in I\}$$

Proposition 3. ([1]) If $I = \langle f_1, ...f_m \rangle \lhd K[x_1, ..., x_n]$, then $\mathbf{V}(I) = \mathbf{V}(f_1, ..., f_m)$.

By Proposition 3, solutions are independent of generating basis, so we can equivalently study the Gröbner system of equations. Interestingly, Gröbner bases in *lex* ordering triangulate (eliminate variables) such systems and can simplify calculations greatly (cf. [1]).

In a 2015 paper ([4]) on the very topic of Gröbner bases over algebraic number fields, a more time efficient algorithm to compute Gröbner bases is proposed. It is well observed that the efficiency of computing Gröbner bases via the Buchberger algorithm is highly dependent on the field arithmetic, where algebraic number fields are relatively difficult.

In another paper ([5]) (2007), Gröbner bases are used to automate a variety of classic proofs of number theoretic nature involving divisibility, congruence, and the notion of coprime, by reduction to our original ideal membership problem.

A final example demonstrates the power of Gröbner bases by reducing computational time.

Definition 14. A *Diophantine equation* is a polynomial equation in two or more variables with integer coefficients, where integer solutions are of interest.

Definition 15. *Pell's equation* is a Diophantine equation of the form $x^2 - Ay^2 = 1$ where A is a positive non-square integer. Again, integer solutions are of interest. This equation can be generalized to $x^2 - Ay^2 = N$ where N is a nonzero integer.

Theorem 2. ([6]) For any integers $a > 1$ and $b > 1$ such that $a \neq b$, the system

$$ax^2 - cz^2 = 1$$
$$by^2 - dz^2 = 1$$

of generalized Pell's equations has at most two integer solutions with x, y, $z > 0$.

When showing a restriction on the set of solutions to a system of generalized Pell's equations, the 2008 paper ([6]) proposes a Gröbner basis method which requires half the classical method time.

References

[1] Cox, David, Little, John, and O'Shea, Donal. *Ideals, Varieties, and Algorithms an Introduction to Algebraic Geometry and Commutative Algebra*. Fourth edition, Berlin, Heidelberg, Springer, 1998.

[2] Dummit, David, and Foote, Richard. *Abstract Algebra*. Third edition, John Wiley and Sons, Inc, 2004.

[3] "Gröbner basis". Wikipedia, The Free Encyclopedia, Wikimedia Foundation, 29 January 2023, `https://en.wikipedia.org/wiki/Gröbner_basis`.

[4] Boku, Dereje Kifle, Decker, Wolfram, Fieker, Claus, and Steenpass, Andreas (2015). "Gröbner Bases Over Algebraic Number Fields." `https://arxiv.org/pdf/1504.04564.pdf`.

[5] Harrison, John (2007). "Automating Elementary Number-Theoretic Proofs Using Gröbner Bases". In: Pfenning, F. (eds) Automated Deduction – CADE-21. CADE 2007. Lecture Notes in Computer Science(), vol 4603. Springer, Berlin, Heidelberg. `https://doi.org/10.1007/978-3-540-73595-3_5`.

[6] Cipu, Mihai. "Gröbner Bases and Diophantine Analysis". *Journal of Symbolic Computation*, vol. 43, no. 10, October 2008, pp. 681-687. **URL**.