

# *The theory of Gröbner bases and applications*

by

*Andrew Barnard Davies*

Submitted in fulfilment of the requirements for the degree

*Magister Scientiae*

in the Department of Mathematics and Applied Mathematics  
in the Faculty of Natural and Agricultural Sciences

University of Pretoria

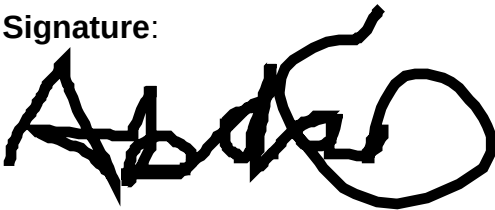
Pretoria

*July 2023*

## DECLARATION

I, the undersigned, declare that the *dissertation*, which I hereby submit for the degree *Magister Scientiae* at the University of Pretoria, is my own independent work and has not previously been submitted by me for a degree at this or any other tertiary institution.

**Signature:**



**Name:**

Andrew Barnard Davies

**Date:**

04-07-2023

ABSTRACT. In this dissertation we study Gröbner bases. Gröbner bases simultaneously generalise Gauss elimination and univariate polynomial long division but for multivariate polynomials. Their use is in solving systems of polynomial equations. We present some practical examples of their use in graph colouring and circle packing problems. We then study, in detail, the underlying theory and algorithms used in the computation of Gröbner bases.

## Contents

Chapter 1. Introduction	3
1.1. Background	3
1.2. Simpler Cases	4
1.3. Applications	6
Chapter 2. Basics and the Hilbert Basis Theorem	12
2.1. Term Orders	12
2.2. The Hilbert Basis Theorem	14
Chapter 3. Polynomial Arithmetic	18
3.1. Division Algorithms	18
Chapter 4. Gröbner bases	23
4.1. Preliminaries	23
4.2. Buchberger's Theorem and Buchberger's Algorithm	26
4.3. Minimal and Reduced Gröbner bases	32
Chapter 5. Improvements to Buchberger's Algorithm	35
5.1. The first new criterion	35
5.2. Modules and Syzygies	38
5.3. The second new criterion	44
5.4. Improving Buchberger's Algorithm	45
Bibliography	48

## CHAPTER 1

## Introduction

### 1.1. Background

Gröbner bases were formalised in 1965 in Buchberger's PhD thesis [2], named for his supervisor Wolfgang Gröbner. An important contribution of Buchberger, however, was his algorithm to compute Gröbner bases, rather than the bases themselves. The idea represented in a Gröbner basis existed prior to being described by its inventor, Bruno Buchberger. Hironaka [5] and Macaulay [6] had done work in related topics and, in fact, Gunther [4] had even published a similar idea several decades earlier, but it was largely overlooked by the mathematical community until its rediscovery several decades later [8]. We first present a more superficial explanation of Gröbner bases for illustrative purposes.

Consider the problem of finding a generating set for a polynomial ideal. In a single variable polynomial ring (which we shall take to be over a field) an ideal  $I$  can be generated by a single polynomial, the greatest common divisor of the elements of  $I$ . In multivariate polynomials, the concept of a greatest common divisor has to be adjusted slightly. A Gröbner basis can be thought of as an analogy for the greatest common divisor of univariate polynomials in the multivariate case. We will develop the concept of dividing multivariate polynomials by other polynomials shortly, but for now we interpret it as something of the form: A polynomial  $f$  divided by some polynomials  $\{g_1, \dots, g_s\}$  equals  $h_1g_1 + \dots + h_sg_s + r$  for some polynomials  $h_1, \dots, h_s$  and a remainder  $r$ .

Gröbner bases are used because systems of polynomial equations can be difficult to solve and having a Gröbner basis for the ideal generated by the polynomials allows for easier solving of the system. This is because in the case of a polynomial system, the ideal generated by the polynomials in the system, and any generating set for this ideal all have the same solution set, also referred to as a variety. For instance, the variety of  $x^2 + y^2 - 1$  is the circle in the  $xy$ -plane with center  $(0, 0)$  and radius 1. When more polynomials are involved, the geometric representation of a their variety becomes the intersection of each of their varieties. So while the original system may be difficult to solve, a Gröbner basis is a different set of polynomials with the same variety, but containing easier to solve polynomials, and simpler geometric representations. What is meant by an easier to solve polynomial is that it contains fewer indeterminates, with the easiest to solve being a polynomial in one indeterminate only.

We will expand on how we can find these easier to solve polynomials. We look at simpler, familiar cases first and develop an analogy for these in the more complicated case. Namely, linear systems and univariate polynomials.

## 1.2. Simpler Cases

**1.2.1. The linear case.** The well-established and familiar procedure of the Gauss-Jordan method is used to solve linear systems. Consider, for example, the system of linear equations:

$$\begin{aligned} 2x + y + 3z &= 1 \\ 6x + 5y + 7z &= 2 \\ 4x + 3y + z &= 3 \end{aligned}$$

We first represent this as an augmented matrix:

$$\left[ \begin{array}{ccc|c} 2 & 1 & 3 & 1 \\ 6 & 5 & 7 & 2 \\ 4 & 3 & 1 & 3 \end{array} \right]$$

To reduce this system to row-echelon form we would perform the following sequence of elementary row operations:

$$\begin{aligned} R_2 &\leftarrow R_2 - 3R_1 \\ R_3 &\leftarrow R_3 - 2R_1 \\ R_3 &\leftarrow R_3 - \frac{1}{2}R_2 \end{aligned}$$

and obtain the new, equivalent system:

$$\left[ \begin{array}{ccc|c} 2 & 1 & 3 & 1 \\ 0 & 2 & -2 & -1 \\ 0 & 0 & -4 & \frac{3}{2} \end{array} \right]$$

which then has solutions  $(x, y, z) = (\frac{3}{2}, \frac{-7}{8}, \frac{-3}{8})$ . Let us now think about this system in a different way. Firstly, let  $\mathbb{R}[x, y, z]$  be the polynomial ring in the indeterminates  $x, y, z$  with real coefficients. Consider the polynomials

$$\begin{aligned} f_1 &= 2x + y + 3z - 1 \\ f_2 &= 6x + 5y + 7z - 2 \\ f_3 &= 4x + 3y + z - 3 \end{aligned}$$

and let  $I$  be the ideal of  $\mathbb{R}[x, y, z]$  generated by  $f_1, f_2, f_3$ , that is

$$I := \{ff_1 + gf_2 + hf_3 \mid f, g, h \in \mathbb{R}[x, y, z]\}.$$

The solution sets  $A := \{(x, y, z) \in \mathbb{R}^3 \mid \text{for all } f \in \{f_1, f_2, f_3\}, f(x, y, z) = 0\}$  and  $B := \{(x, y, z) \in \mathbb{R}^3 \mid \text{for all } f \in I, f(x, y, z) = 0\}$  are equal: For  $(\frac{3}{2}, \frac{-7}{8}, \frac{-3}{8}) \in \mathbb{R}^3$ , we have  $f_1(\frac{3}{2}, \frac{-7}{8}, \frac{-3}{8}) = 0$ ,  $f_2(\frac{3}{2}, \frac{-7}{8}, \frac{-3}{8}) = 0$  and  $f_3(\frac{3}{2}, \frac{-7}{8}, \frac{-3}{8}) = 0$  and clearly for any  $f, g, h \in \mathbb{R}[x, y, z]$ , we also have  $(ff_1 + gf_2 + hf_3)(\frac{3}{2}, \frac{-7}{8}, \frac{-3}{8}) = 0$ . This is the only member of  $A$  and so  $A \subseteq B$ . We cannot have  $A \subsetneq B$ : If, say,  $(a, b, c) \in B$  and  $(a, b, c) \notin A$  then we would have, for some  $i \in \{1, 2, 3\}$ ,  $f_i(a, b, c) \neq 0$ . But  $f_i \in I$  and so  $f_i(a, b, c) = 0$ , and thus both solution sets are equal.

We can view the row operations performed in the Gauss-Jordan procedure in a different way, namely as a form of polynomial division. The first row operation performed gave us the new equation  $2y - 2z = -1$  which we can also view as the polynomial  $f'_2 := 2y - 2z + 1$ . We could then write  $f'_2 = f_2 - 3f_1$ , which is clearly in  $I$ . Similarly, the next two row operations gave us the equation  $-4z = \frac{3}{2}$ . We can write  $f'_3 := f_3 - 2f_1$  and  $f''_3 := f'_3 - \frac{1}{2}f'_2 = -4z - \frac{3}{2}$ . We represent this in terms of  $f_1$  and  $f_2$ : By substitution,  $f''_3 = f_3 - 2f_1 - \frac{1}{2}(f_2 - 3f_1) = f_3 - \frac{1}{2}f_1 - \frac{1}{2}f_2$ . This is the

linear version of the polynomial division concept we are developing. We will develop this concept further with multivariate polynomial systems, which are the main problems of concern for us. The Gauss-Jordan process is in fact a special case of the process we are developing.

**1.2.2. The univariate case.** In the linear case, we reframed the concept of row reduction as a form of polynomial division. We now look at how this procedure behaves in the case of a non-linear, univariate polynomial. Let  $f_1 = 2x^3 + 3x^2 - x + 1 \in R[x]$  and  $f_2 = 2x^2 + x \in R[x]$ . Perform long division:

$$\begin{array}{r|rrrrrr}
 & & x & & +1 & & \\
 2x^2 & +x & & & & & \\
 - & & 2x^3 & +3x^2 & -x & +1 & \\
 \hline
 & & & & 2x^2 & -x & +1 \\
 - & & & & 2x^2 & +x & \\
 \hline
 & & & & & -2x & +1
 \end{array}$$

We then have that  $2x^3 + 3x^2 - x + 1 = (2x^2 + x)(x + 1) + (-2x + 1)$ . Conventionally, the term  $-2x + 1$  is called the remainder,  $r$ . Another way of expressing this, that is similar to Section 1.2.1, is to write  $r = f_1 - x f_2 - f_2$ . Writing  $r$  like this suggests a method: Note that  $x = \frac{2x^3}{2x^2}$  is the ratio of the two largest (with respect to degree) terms in  $f_1$  and  $f_2$  respectively. Then, letting  $r_1 = 2x^2 - x + 1$ , an intermediate remainder, we could write  $r_1 = f_1 - \frac{2x^3}{2x^2} f_2$ . Similarly,  $1 = \frac{2x^2}{2x^2}$  is the ratio of the largest (with respect to degree) terms in  $r_1$  and  $f_2$  respectively. Then  $r = r_1 - 1 \cdot f_2$ . We can see the similarity to the Gauss-Jordan method here. We subtract a multiple of one polynomial from another, where the multiple is in fact the ratio of the largest terms in each polynomial. In Gauss-Jordan these are simply the coefficients of the current variable being eliminated. Here, it is the largest products, what we will call *lead products* (see Definition 2.1.5), of the intermediate remainder and divisor of the current stage of division. This is then the method:  $r_1 = f_1 - \frac{\text{lead product } f_1}{\text{lead product } f_2} \cdot f_2$  and  $r = r_1 - \frac{\text{lead product } r_1}{\text{lead product } f_2} \cdot f_2$ . This is what motivates the definitions in Definition 3.1.2 and Definition 3.1.3, and we would write  $f_1 \xrightarrow{f_2} r_1 \xrightarrow{f_2} r$  or, more compactly,  $f_1 \xrightarrow{f_2}_+ r$ , and we say that  $f_1$  reduces to  $r$  modulo  $f_2$ . This will be the main procedure involved in computing Gröbner bases. With a univariate polynomial the lead product is simply the term with the largest exponent, but we will have to adjust this definition for the multivariate case (see Section 2.1).

**1.2.3. A first look at Gröbner bases and Buchberger's Algorithm.** Let us return to the linear system in Section 1.2.1. We note that in solving the system in the linear case, when we chose to eliminate the indeterminates in a particular order we implicitly selected an order of preference for the indeterminates. We first eliminated  $x$  from the polynomials, and then  $y$ . We were left with one polynomial in terms of only  $z$ , one in terms of only  $y$  and  $z$ , and one in terms of all three indeterminates. Note that we could have swapped the columns around and solved the resulting system and we would obtain the same solution. This is the equivalent of choosing a different order of preference for our indeterminates. We will solve the same system again, this time using Buchberger's Algorithm (Algorithm 4.2.7). The two central ideas that are used in the algorithm are the reduction definition in Definition 3.1.3 and something Buchberger called an " $S$ -polynomial" (see Definition 2.1). The  $S$ -polynomial is a function that takes two polynomials and returns a polynomial, but the specifics are not important for the illustration here.

If we run Buchberger's Algorithm (Algorithm 4.2.7) on the polynomials

$$\begin{aligned} f_1 &= 2x + y + 3z - 1 \\ f_2 &= 6x + 5y + 7z - 2 \\ f_3 &= 4x + 3y + z - 3 \end{aligned}$$

with the order of importance  $x \succ y \succ z$  placed on the indeterminates we find that exactly the same polynomials  $f_2'$  and  $f_3''$  from Section 1.2.1 are generated. If we swapped columns around in the Gauss-Jordan process this would be the same as choosing a different order on our variables in the Gröbner basis calculation. How the algorithm works, in simple terms, is this:

We maintain two lists: A list of polynomials  $G$ , initialised as  $G := \{f_1, f_2, f_3\}$ , and a list of pairs of polynomials, initialised as  $\mathcal{G} := \{(f_1, f_2), (f_1, f_3), (f_2, f_3)\}$ . We then pick and remove a pair from  $\mathcal{G}$  (the algorithm doesn't stipulate how it should be chosen so it is a random choice), say  $(f_1, f_2)$  and find the result of reducing the  $S$ -polynomial of the pair modulo the polynomials in our system. So, in our notation (Definition 3.1.3, Definition 4.2.1), this would look as follows:

$$S(f_1, f_2) \xrightarrow{\{f_1, f_2, f_3\}} + f_4.$$

In this example, the remainder  $f_4 = 2y - 2z + 1$  (which is identical to  $f_2'$  in Section 1.2.1) is not 0 and so we add  $f_4$  to  $G$ . Now  $G = \{f_1, f_2, f_3, f_4\}$ . We also generate all possible new pairs, namely:

$$(f_1, f_4), (f_2, f_4), (f_3, f_4)$$

and add these to  $\mathcal{G}$ . We repeat the process with a new pair, say  $(f_1, f_3)$ , and end up with  $f_5 = -4z - \frac{3}{2}$  (which is identical to  $f_3''$  from Section 1.2.1) The new pairs

$$(f_1, f_5), (f_2, f_5), (f_3, f_5), (f_4, f_5)$$

are added to  $\mathcal{G}$ .

The algorithm continues in this fashion until there are no more pairs left in  $\mathcal{G}$  to operate on. New polynomials are added to  $G$  when the remainder of division of the  $S$ -polynomial of one of the pairs is not 0, and new pairs are generated and added to  $\mathcal{G}$ .

There is a substantial inefficiency in the algorithm that is illustrated in the current example. Two pairs have been divided and two new polynomials added. This is in fact already a Gröbner basis, and all remaining pairs will have remainder 0 after division. However, there are still 8 more pairs to check and the algorithm will continue performing calculations on these pairs without stopping to check whether a Gröbner basis has already been found. These are memory intensive calculations and slow things down considerably. This is why Buchberger also created an improved version of his algorithm, which we look at in Chapter 5. The improvement is that the algorithm can throw away some of the pairs because we already know their division will have remainder 0 without having to calculate it.

In this example, the choice was in fact not random but deliberate so as to mimic exactly what the Gauss-Jordan process did. Allowing things to proceed truly randomly would be analogous to swapping rows around in the Gauss-Jordan process. Different polynomials or rows might be produced but they result in an equivalent system.

### 1.3. Applications

Now that we have a cursory understanding of what Gröbner bases attempt to achieve, we look at a few examples. The purpose is to illustrate the variety of situations in which polynomial systems

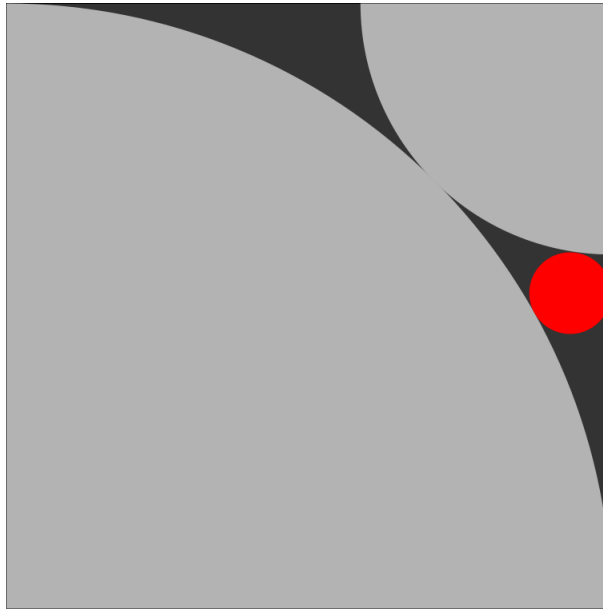


FIGURE 1.3.1.  
 Find the radius of the red circle in the unit square.

occur and how it is often the case that solving them naively is, at the very least, an inconvenient undertaking.

**1.3.1. A “simple” geometry problem.** This is an easily stated problem taken from a YouTube video [7]. Consider Figure 1.3.1. The problem is to calculate the radius of the red circle. We have two quarter circles inscribed in a unit square at opposite corners and we are given that the red circle is tangent to both circles as well as the square. It is easy enough to create a system of equations for this problem: Using a Cartesian co-ordinate system, let the bottom left corner of the square be the origin, let the radius of the red circle be  $r$ , and let the co-ordinates of the center of the red circle be  $(h, k) \in [0, 1] \times [0, 1]$ . It is an easy exercise to see that  $h, k$  and  $r$  satisfy the following equations:

$$\begin{aligned}
 h^2 + k^2 &= (1 + r)^2 \\
 (h - 1)^2 + (k - 1)^2 &= (r + \sqrt{2} - 1)^2 \\
 h + r &= 1.
 \end{aligned}$$

The first two equations are obtained from calculating the distance from  $(h, k)$  to  $(0, 0)$  and  $(1, 1)$  respectively, and the third is trivial. Now we invite the reader to attempt to solve these equations. It is doable, using a few algebraic tricks, but even just these three relatively simple polynomial equations are painful to solve by hand.

If we instead compute the Gröbner basis for the system using a computer and Buchberger’s Algorithm we will have a new system of polynomial equations. Running the basic Buchberger



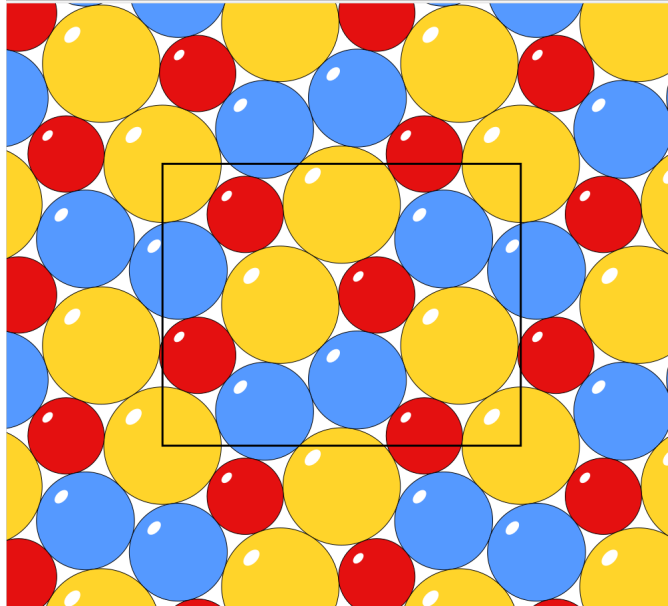


FIGURE 1.3.2.  
A tessellation of the plane with 3 different circles [3].

algorithm (Algorithm 4.2.7) yields the following system of equations

$$\begin{aligned} h + r - 1 &= 0 \\ \frac{49}{8}r^4 - \frac{29}{2}r^3 + \frac{43}{4}r^2 - \frac{5}{2}r + \frac{1}{8} &= 0 \\ -\frac{2401}{32}r^6 + \frac{12593}{96}r^5 - \frac{3815}{144}r^4 - \frac{17801}{432}r^3 + \frac{31871}{2592}r^2 - \frac{1589}{2592}r - \frac{7}{81}k + \frac{7}{162} &= 0. \end{aligned}$$

While these may appear to be worse at first glance this is only due to the size of the coefficients. In actual fact we have obtained an equation in only one variable,  $r$ , the one for which we were trying to solve. This was done by choosing  $r$  as the most important variable, similar to the right-most column of a linear Gauss-Jordan procedure. It should be evident that deriving equations like these by hand is not feasible.

**1.3.2. Circle packing.** Another field of Mathematics that is suitable for an application of a Gröbner basis is tessellating the plane with circles. Consider Figure 1.3.2, taken from [3].

We ask the question: What are the exact<sup>1</sup> radii of the circles in the figure, if the largest circles have radius 1. Letting the radius of the largest circle be 1, we then have two variables: The radii of the smaller circles,  $r_1$  and  $r_2$ , with  $0 < r_1 < r_2 < 1$ . It can be shown that  $r_1$  and  $r_2$  are simultaneous

<sup>1</sup>Here, by exact, we mean as a root of a single variable polynomial.

roots of the following two polynomials in  $r_1$  and  $r_2$ :

$$\begin{aligned} f_1 &= 16r_1^6r_2 - r_1^6 + 48r_1^5r_2^2 + 44r_1^5r_2 - 2r_1^5 + 48r_1^4r_2^3 + 58r_1^4r_2^2 + 40r_1^4r_2 - r_1^4 + 16r_1^3r_2^4 - 20r_1^3r_2^3 \\ &\quad - 28r_1^3r_2^2 + 12r_1^3r_2 - 33r_1^2r_2^4 - 56r_1^2r_2^3 - 38r_1^2r_2^2 + 14r_1r_2^4 + 12r_1r_2^3 - r_2^4 \\ f_2 &= 2r_1^2r_2^2 - 5r_1^2r_2 + r_1^2 + 4r_1r_2^3 - 2r_1r_2^2 - 6r_1r_2 + 2r_2^4 + 3r_2^3 + r_2^2. \end{aligned}$$

There is no clear way to approach finding the roots of the polynomials  $f_1$  and  $f_2$  by hand. We compute a Gröbner basis for the ideal generated by  $f_1$  and  $f_2$ : Just as in Gauss-Jordan elimination, where one can rearrange the columns of the associated matrix and solve for a different variable first, we can pick which of  $r_1$  and  $r_2$  should be solved for first, by applying a term order,  $\succ$ , to the polynomial ring  $\mathbb{R}[r_1, r_2]$ . Upon computing a Gröbner basis for  $\{f_1, f_2\}$  with  $r_1 \succ r_2$ , we obtain the following polynomial in the Gröbner basis

$$89r_1^{14} + 1344r_1^{13} + 4008r_1^{12} - 464r_1^{11} - 2410r_1^{10} + 176r_1^9 + 296r_1^8 - 96r_1^7 + r_1^6$$

as the polynomial in  $r_1$  only. We can compute the Gröbner basis again, this time with  $r_2 \succ r_1$ , and obtain

$$4r_2^{14} - 36r_2^{13} - 27r_2^{12} + 162r_2^{11} + 135r_2^{10} - 88r_2^9 - 73r_2^9 - 14r_2^7 + r_2^6$$

as another polynomial in a different Gröbner basis, this time in terms of  $r_2$  only. Both polynomials give an exact solution, in the sense that  $r_1$  and  $r_2$  are roots of the respective polynomials. Numerical approximations of  $r_1$  and  $r_2$  are

$$\begin{aligned} r_1 &\approx 0.65105018588260919953270 \\ r_2 &\approx 0.83430604285301743967753 \end{aligned}$$

with, as described before, a third radius  $r_3 = 1$ .

**1.3.3. Graph Colouring.** A classic problem to which we can also apply Gröbner bases is that of graph colouring. Consider, for instance, the graph with 8 vertices in Figure 1.3.3 [1, Problem 2.7].

We wish to colour this graph with 3 colours such that no two adjacent vertices have the same colour. We can represent the 3 colours with the 3 cube roots of unity by letting  $\xi = e^{\frac{2\pi i}{3}}$ . Then the 3 colours are  $1, \xi, \xi^2$ . We treat the vertices  $x_1, \dots, x_8$  labelled in the graph as indeterminates, the values of which will correspond to a colour. Then we can create equations using the fact that each variable must be a cube root of unity:

$$x_i^3 - 1 = 0, \quad 1 \leq i \leq 8.$$

Another property to use is that if two distinct vertices  $x_i$  and  $x_j$  are connected by an edge they need to have a different color. We know that  $x_i^3 = x_j^3$  and so

$$(x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0.$$

Since we want  $x_i$  and  $x_j$  to have different colors we must have

$$x_i^2 + x_i x_j + x_j^2 = 0 \quad (i, j) \in \{(i, j) \mid x_i \text{ and } x_j \text{ connected by an edge}\}.$$

The set of pairs of vertices connected by an edge in Figure 1.3.3 is

$$\{(1, 2), (1, 5), (1, 6), (2, 3), (2, 4), (2, 8), (3, 4), (3, 8), (4, 5), (4, 7), (5, 6), (5, 7), (6, 7), (7, 8)\}.$$

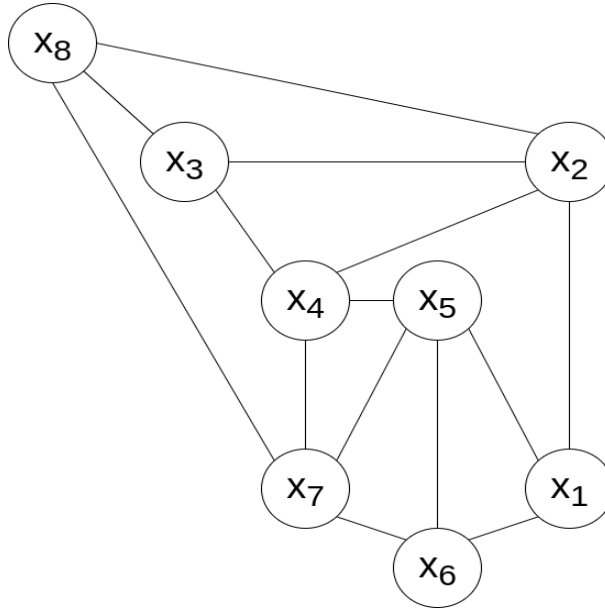


FIGURE 1.3.3.  
A simple graph with 8 vertices.

This brings us to a total of 22 equations for 8 variables. We choose to order the variables (for no particular reason other than there must be an order) as  $x_1 \succ x_2 \succ \dots \succ x_8$ . Computing the Gröbner basis gives us the set

$$G = \left\{ \begin{array}{l} x_1 - x_7, \\ x_2 + x_7 + x_8, \\ x_3 - x_7, \\ x_4 - x_8, \\ x_5 + x_7 + x_8, \\ x_6 - x_8, \\ x_7^2 + x_7x_8 + x_8^2, \\ x_8^3 - 1 \end{array} \right\}.$$

We can now give a colouring for the graph: We can choose any colour for  $x_8$ , since  $x_8^3 - 1$  is the only polynomial in one variable. Let us say that  $x_8$  is red. From the polynomial  $x_7^2 + x_7x_8 + x_8^2$  we know that  $x_7$  must be a different colour from  $x_8$ . This is because if they were the same colour, whether  $x_8 = 1$ ,  $x_8 = \xi$  or  $x_8 = \xi^2$ , we would have  $x_7^2 + x_7x_8 + x_8^2 \neq 0$ . So we say that  $x_7$  is blue, for instance. Now from  $x_1 - x_7 = 0$  and  $x_3 - x_7 = 0$  we know  $x_1$  and  $x_3$  must also be blue. Similarly we must have that  $x_4$  and  $x_6$  are red. Lastly, because  $1 + \xi + \xi^2 = 0$ , the two equations  $x_2 + x_7 + x_8 = 0$  and  $x_5 + x_7 + x_8 = 0$  indicate that  $x_2$  and  $x_5$  have the same colour, and that colour is different from  $x_7$  and  $x_8$ . So we can say that  $x_2$  and  $x_5$  are green. We see that the graph has now been coloured (Figure 1.3.4). This is in fact the only possible colouring of the graph, up to permuting the colours. Some other graphs may have multiple possible colourings and this is reflected in the

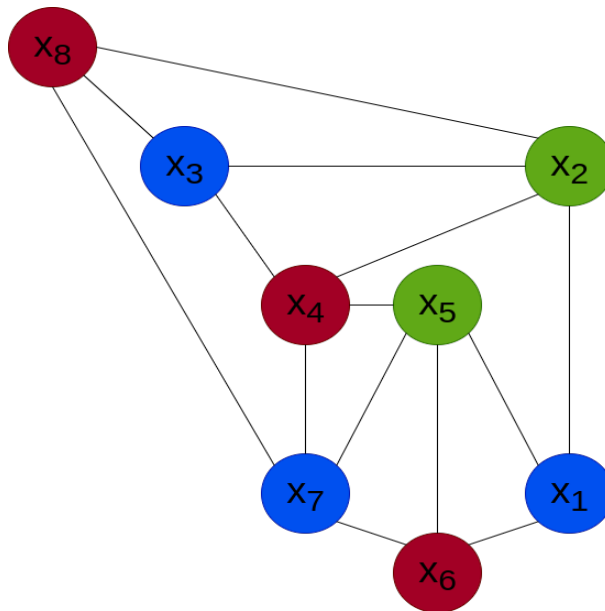


FIGURE 1.3.4.  
A 3 colouring of the graph.

corresponding Gröbner basis: There may be polynomials with multiple solutions for instance, and in general the Gröbner basis will look more complicated.

These three examples should give some sense of the variety of problems in which a Gröbner basis can be used.

Having introduced the general notion of Gröbner bases and some of their applications, we can now delve into the technical aspects. In Chapter 2 we define term orders, develop some theory relating to Noetherian rings, and prove the Hilbert Basis Theorem, a crucial result necessary to prove the correctness of the algorithms used to compute Gröbner bases (Algorithm 4.2.7 and Algorithm 5.4.3).

Chapter 3 is a short chapter on developing the polynomial arithmetic necessary for all the computations performed by the algorithms.

In Chapter 4 we come to the main results of this dissertation. We develop the theory of Gröbner bases and present Buchberger's Theorem (Theorem 4.2.6), Buchberger's Algorithm (Algorithm 4.2.7) and prove the algorithm's correctness.

Lastly, in Chapter 5 we further develop the theory of Gröbner bases in the context of modules, and we present the improved version of Buchberger's Algorithm (Algorithm 5.4.3) and prove its correctness.

## CHAPTER 2

## Basics and the Hilbert Basis Theorem

We will be working almost exclusively with commutative rings of polynomials in  $n$  variables over a field. The examples from Chapter 1 were for polynomials over the real numbers, but in fact the field may be arbitrary and we denote this with  $k$ . We now define some basic notation that will be used extensively:

- We denote  $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ .
- For an  $n \in \mathbb{N}$ , if  $x_1, \dots, x_n$  are indeterminates then we denote the set of all polynomials in these indeterminates, with coefficients in  $k$ , by  $k[x_1, \dots, x_n]$ . This set together with the usual operations of addition and multiplication of polynomials is then a commutative ring.
- For constants  $a \in k$  and  $\beta_1, \dots, \beta_n \in \mathbb{N}_0$ , we consider a polynomial to be a finite sum of terms of the form  $ax_1^{\beta_1} \dots x_n^{\beta_n}$ . We call  $x_1^{\beta_1} \dots x_n^{\beta_n}$  a *power product*.
- We denote with  $P_n$  the set of all power products in  $n$  variables,  $x_1, \dots, x_n$ . Thus  $P_n := \{x_1^{\beta_1} \dots x_n^{\beta_n} \mid (\beta_1, \dots, \beta_n) \in \mathbb{N}_0^n\}$ . When the exponents are arbitrary we will simply refer to the power product by a single capital letter, for compactness, i.e.  $X \in P_n$ . The set  $P_n$  is a basis for the set  $k[x_1, \dots, x_n]$ , interpreted as a vector space over  $k$ .
- If  $R$  is a commutative ring,  $s \in \mathbb{N}$  and  $f_1, \dots, f_s \in R$ , then the ideal generated by these elements is denoted  $\langle f_1, \dots, f_s \rangle := \{u_1 f_1 + \dots + u_s f_s \mid u_1, \dots, u_s \in R\}$ .
- While it is conventional to for  $a|b$  to mean  $a$  divides  $b$ , in this paper we mean the opposite, that  $b$  divides  $a$ .

### 2.1. Term Orders

As mentioned in Chapter 1, we require a method to order the terms in our polynomials. In univariate polynomials the concept of degree is important. One term in a polynomial is always divisible by another term of lower degree. When dividing we proceed from the larger powers to the smaller ones. When dealing with multivariate polynomials, however, this order becomes ambiguous. Consider the polynomial  $x^2 + y^2 + xy$ . All three terms have the same degree so which one is largest? We need to be able to decide on an order so that division can proceed unambiguously. Just as in Gauss-Jordan elimination, where indeterminates are implicitly given some order of preference, we do the same, for instance  $z \succ y \succ x$ . However we need an additional property to be able to decide which of the terms  $x^2, y^2$  and  $xy$  is largest, which we will refer to as a term order. Different term orders will in fact give rise to different Gröbner bases, but for the purposes of a Gröbner basis' existence, and the associated solutions, the choice of term order is not relevant. As a side note, the choice of term order matters under some circumstances when considering the efficiency of calculations [1, Example 2.3.3].

We begin with the usual definition of degree:

DEFINITION 2.1.1. Let  $n \in \mathbb{N}$ ,  $(\beta_1, \dots, \beta_n) \in \mathbb{N}_0^n$  and let  $x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n} = X \in P_n$  be a power product. We define the *degree* of  $X$  to be  $\deg(X) := \sum_{i=1}^n \beta_i$ .

We now define term orders. It should be noted that the definition is rather broad, allowing for many different possible term orderings.

DEFINITION 2.1.2. [1, Definition 1.4.1]. Let  $n \in \mathbb{N}$ . A *term order* on  $P_n$  is a total order  $\prec$  satisfying the following conditions:

- (1) For all  $X \in P_n$  and  $X \neq 1$ :  $1 \prec X$ .
- (2) For all  $Y \in P_n$ :  $X \prec Z \implies XY \prec ZY$ .

We naturally extend the notation in Definition 2.1.2 by defining:  $X \preceq Y \iff X \prec Y$  or  $X = Y$ .

DEFINITION 2.1.3. Let  $n \in \mathbb{N}$  and let  $X, Y \in P_n$ . We say that  $Y$  is *divisible by*  $X$ , written  $Y|X$  if there exists a  $Z \in P_n$  such that  $XZ = Y$ .

And now a simple condition for ordering terms.

PROPOSITION 2.1.4. [1, Proposition 1.4.5]. Let  $n \in \mathbb{N}$ , let  $X \neq Y \in P_n$  such that  $Y|X$  and let  $\prec$  be a term order on  $k[x_1, \dots, x_n]$ . Then  $X \prec Y$ .

PROOF. Since  $Y|X$  there exists a  $Z \in P_n$  such that  $Y = XZ$  and  $Z \neq 1$ . We also have  $1 \prec Z$  from Definition 2.1.2(1). Then from Definition 2.1.2(2) we have  $X \prec XZ = Y$ .  $\square$

We can now provide some more notation based on term orders that will be used extensively.

DEFINITION 2.1.5. Let  $\prec$  be any term order on  $P_n$ . For polynomials

$$f, g, f_1, \dots, f_s \in k[x_1, \dots, x_n]$$

and a finite set  $F := \{f_1, \dots, f_s\}$  we define the following:

- (1) The term with the largest power product in  $f$  with respect to the term order is called the *lead term* of  $f$  and will be denoted by  $\text{lt}(f)$ .
- (2) The power product of the lead term of  $f$  is called the *lead product* and will be denoted by  $\text{lp}(f)$ .
- (3) The coefficient of the lead term of  $f$  is called the *lead coefficient* and will be denoted by  $\text{lc}(f)$ .
- (4) We denote with  $\text{Lt}(F)$  the ideal generated by all lead terms of the polynomials in the set  $F$ , i.e.  $\text{Lt}(F) := \langle \text{lt}(f_1), \dots, \text{lt}(f_s) \rangle$ .
- (5) We define the expression (*lower terms of*  $f$ ) to mean  $f - \text{lt}(f)$ .
- (6) The *least common multiple* of  $f$  and  $g$ , denoted  $\text{lcm}(f, g)$  is a polynomial  $l \in k[x_1, \dots, x_n]$  such that:
  - (a) There exist  $f', g' \in k[x_1, \dots, x_n]$  such that  $ff' = gg' = l$ .
  - (b) If there exists an  $h \in k[x_1, \dots, x_n]$  and  $f'', g'' \in k[x_1, \dots, x_n]$  such that  $ff'' = gg'' = h$  then there exists  $l' \in k[x_1, \dots, x_n]$  such that  $ll' = h$ .
  - (c)  $\text{lc}(l) = 1$ .
- (7) The *greatest common divisor* of  $f$  and  $g$ , denoted  $\text{gcd}(f, g)$ , is a polynomial  $d \in k[x_1, \dots, x_n]$  such that:
  - (a) There exist  $f', g' \in k[x_1, \dots, x_n]$  such that  $df' = f$  and  $dg' = g$ .
  - (b) If there exists an  $h \in k[x_1, \dots, x_n]$  and  $f'', g'' \in k[x_1, \dots, x_n]$  such that  $hf'' = f$  and  $hg'' = g$  then there exists  $d' \in k[x_1, \dots, x_n]$  such that  $hd' = d$ .
  - (c)  $\text{lc}(d) = 1$ .

We now give a few examples of term orders that are used in practice.

EXAMPLE 2.1.6. Let  $n \in \mathbb{N}$ . For  $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \mathbb{N}_0$  we define the *lexicographical order*,  $\prec_{lex}$ , on  $P$  as follows:

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \prec_{lex} x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n} \text{ if for the least } i \text{ such that } \alpha_i \neq \beta_i \text{ we have } \alpha_i < \beta_i.$$

EXAMPLE 2.1.7. Let  $n \in \mathbb{N}$ . For  $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \mathbb{N}_0$  we define the *degree lexicographical order*,  $\prec_{deglex}$ , on  $P$  as follows:

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \prec_{deglex} x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n} \text{ if } \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i & \text{or} \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i & \text{and} \\ x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \prec_{lex} x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n} \end{cases}$$

EXAMPLE 2.1.8. For  $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \mathbb{N}_0$  we define the *degree reverse lexicographical order*,  $\prec_{degrevlex}$ , on  $P$  as follows:

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \prec_{degrevlex} x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n} \text{ if } \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i & \text{or} \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i & \text{and for the greatest } i \text{ such that} \\ & \alpha_i \neq \beta_i \text{ we have } \alpha_i < \beta_i \end{cases}$$

## 2.2. The Hilbert Basis Theorem

Several results in the coming chapters rely on the fact that the term orders defined in the previous section are, in fact, well-orderings. To prove this fact we require some theory on Noetherian rings and the Hilbert Basis Theorem (Theorem 2.2.5).

DEFINITION 2.2.1. A commutative ring  $R$  is *Noetherian* if for any sequence of ideals  $\{I_i\}_{i \in \mathbb{N}}$  in  $R$  such that

$$I_1 \subseteq I_2 \subseteq \cdots$$

there exists an  $N \in \mathbb{N}$  such that  $I_i = I_N$  for all  $i \geq N$ .

The following result provides us with a different but equivalent condition for a ring to be Noetherian, namely that every ideal in the ring is *finitely generated*. This simply means that any ideal has a finite generating set.

THEOREM 2.2.2. [1, Theorem 1.1.2]. *Let  $R$  be a commutative ring. The following conditions are equivalent for  $R$ :*

- (i) *For any ideal  $I \subseteq R$  there exists an  $s \in \mathbb{N}$  and  $f_1, \dots, f_s \in R$  such that  $I = \langle f_1, \dots, f_s \rangle$ .*
- (ii) *The ring  $R$  is Noetherian.*

PROOF. Assume that (i) holds and let  $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$  be an ascending chain of ideals. Let  $I := \bigcup_{i=1}^{\infty} I_i$ , which is then an ideal of  $R$ . By assumption there exists an  $s \in \mathbb{N}$  and  $f_1, \dots, f_s \in R$  such that  $I = \langle f_1, \dots, f_s \rangle$ . For each  $i \in \{1, \dots, s\}$ , we have  $f_i \in I$  which implies that there exists an  $N_i \in \mathbb{N}$  such that  $f_i \in I_{N_i}$ . Letting  $N := \max_{1 \leq i \leq s} (N_i)$  we then have that, for each  $i \in \{1, \dots, s\}$ ,  $f_i \in I_N$ . This means  $I \subseteq I_N$  and so  $I = I_N$  and since  $I = \bigcup_{i=1}^{\infty} I_i$  we have  $I_N = I_{N+1} = I_{N+2} = \cdots$ .

Now assume that the ring  $R$  is Noetherian and suppose that there is an ideal  $I \subseteq R$  that is not finitely generated. Let  $g_1 \in I$  be arbitrary. Since  $g_1$  cannot generate  $I$  there exists  $g_2 \in I$  such that  $g_2 \notin \langle g_1 \rangle$  which implies that  $\langle g_1 \rangle \subsetneq \langle g_1, g_2 \rangle$ . We repeat this process and obtain  $g_3 \in I$  such that  $\langle g_1 \rangle \subsetneq \langle g_1, g_2 \rangle \subsetneq \langle g_1, g_2, g_3 \rangle$ . We can continue this process indefinitely and obtain a strictly

increasing chain of ideals of  $R$ , which violates the assumption that the ring is Noetherian. Thus we must have that there exists some  $s \in \mathbb{N}$  and some  $f_1, \dots, f_s \in R$  such that  $I = \langle f_1, \dots, f_s \rangle$ .  $\square$

The next two results will allow us to show that polynomial rings are Noetherian. The fact that polynomial rings are Noetherian, or equivalently, that all their ideals are finitely generated, is *The Hilbert Basis Theorem* (Theorem 2.2.5).

LEMMA 2.2.3. [1, Theorem 1.1.3]. *Let  $R$  be a commutative Noetherian ring. The polynomial ring  $R[x]$  is Noetherian.*

PROOF. Let  $I \subset R[x]$  be an ideal. We show that  $I$  is finitely generated which, by Theorem 2.2.2, is a sufficient condition for a ring to be Noetherian. We define, for each  $n \in \mathbb{N}_0$ ,

$$I_n := \{r \in R \mid r \text{ is the leading coefficient of a polynomial in } I \text{ of degree } n\} \cup \{0\}.$$

Fix any  $n \in \mathbb{N}_0$ . We claim that  $I_n$  is an ideal of  $R$ . Let  $r \in R$ ,  $r_1 \in I_n$  and let  $f_1 \in I$  be a polynomial corresponding to  $r_1$ . Then the polynomial  $rf_1 \in I$ , has leading coefficient  $rr_1$  and has degree  $n$ , so  $rr_1 \in I_n$ . We also have, for  $r_1, r_2 \in I_n$ , that either  $r_1 + r_2 = 0 \in I_n$  or  $r_1 + r_2 \in I_n$  by taking the sum of corresponding polynomials,  $f_1 + f_2$ , which has the same degree as  $f_1$  and  $f_2$ , and leading coefficient  $r_1 + r_2$ .

We now claim that  $I_n \subseteq I_{n+1}$ : If  $r \in I_n$  then for a corresponding polynomial  $f \in I$  and  $x \in R[x]$ ,  $fx$  is in  $I$ , has degree  $n + 1$  and leading coefficient  $r$ , so  $r \in I_{n+1}$ . These  $\{I_n\}_{n \in \mathbb{N}_0}$  then define an ascending chain of ideals of  $R$ . Since  $R$  is Noetherian there exists an  $N \in \mathbb{N}_0$  such that for all  $n \geq N$ ,  $I_n = I_N$ .

By Theorem 2.2.2, for each  $i \in \mathbb{N}_0$  there exist  $r_{i1}, \dots, r_{it_i} \in R$  that generate  $I_i$ , since  $R$  is Noetherian. Now for each  $i \in \{0, \dots, N\}$  and  $j \in \{1, \dots, t_i\}$ , let  $f_{ij}$  be a polynomial in  $I$  of degree  $i$  with leading coefficient  $r_{ij}$ . Consider the finitely generated ideal  $I' := \langle f_{ij} \mid 0 \leq i \leq N, 1 \leq j \leq t_i \rangle$ . We claim that  $I' = I$ .

Proof of claim: Since each  $f_{ij} \in I$ , we have  $I' \subseteq I$ . For the reverse inclusion, let  $f \in I$  be a polynomial of degree  $m \in \mathbb{N}_0$ . We argue by induction on  $m$  that  $f \in I'$ . If  $f = 0$  or  $m = 0$  then  $f = r$  for some  $r \in R$  and hence  $f \in I_0$ . Then  $f \in I'$ .

Now let  $m > 0$  and assume that all the members of  $I$  of degree less than  $m$  are in  $I'$ . Let  $r$  be the leading coefficient of  $f$ .

If  $m \leq N$  we have  $r \in I_m$  and so there exist  $s_1, \dots, s_{t_m} \in R$  such that  $r = \sum_{j=1}^{t_m} s_j r_{mj}$ . For each  $j \in \{1, \dots, t_m\}$  the polynomial  $f_{mj}$  has degree  $m$  and leading coefficient  $r_{mj}$ . Thus the polynomial  $g := \sum_{j=1}^{t_m} s_j f_{mj}$  is in  $I'$ , has degree  $m$  and has leading coefficient  $r$ . This means the polynomials  $f$  and  $g$  have the same leading coefficient, and so  $f - g$  has degree less than  $m$  and so  $f - g \in I'$  by assumption and thus  $f = (f - g) + g \in I'$ .

On the other hand, if  $m > N$  we have  $r \in I_m = I_N$  and so there exist  $s_1, \dots, s_{t_N} \in R$  such that  $r = \sum_{j=1}^{t_N} s_j r_{Nj}$ . For each  $j \in \{1, \dots, t_N\}$ , the polynomial  $f_{Nj}$  has degree  $N$ , and leading coefficient  $r_{Nj}$ . Thus the polynomial  $g := \sum_{j=1}^{t_N} s_j x^{m-N} f_{Nj}$  is in  $I'$ , has degree  $m$  and has leading coefficient  $r$ . Thus, since  $f$  and  $g$  have the same leading coefficient,  $f - g$  has degree less than  $m$  and so  $f - g \in I'$  by assumption. Then  $f = (f - g) + g \in I'$ .

Hence, by induction on  $m$ , all polynomials in  $I$  are also in  $I'$ . Thus  $I \subseteq I'$  whence  $I = I'$ .  $\square$

We need one more result before we can prove the Hilbert Basis Theorem.

LEMMA 2.2.4. *Let  $2 \leq n \in \mathbb{N}$  and let  $k$  be a field. Let  $k[x_1, \dots, x_{n-1}][x_n]$  denote the polynomial ring in  $x_n$  with coefficients in  $k[x_1, \dots, x_{n-1}]$ . Then  $k[x_1, \dots, x_{n-1}][x_n]$  and  $k[x_1, \dots, x_n]$  are ring-isomorphic.*



PROOF. For any  $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}_0^n$ , define  $\bar{\beta} := (\beta_1, \dots, \beta_{n-1}) \in \mathbb{N}_0^{n-1}$ . In addition, for  $\beta \in \mathbb{N}_0^n$ , define  $x^\beta := x_1^{\beta_1} \cdots x_n^{\beta_n}$  and  $\bar{x}^{\bar{\beta}} := x_1^{\beta_1} \cdots x_{n-1}^{\beta_{n-1}}$ .

Define, for  $r \in k$  and  $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}_0^n$ , the map  $\rho : k[x_1, \dots, x_n] \rightarrow k[x_1, \dots, x_{n-1}][x_n]$  as follows:

$$\rho(rx^\beta) := r\bar{x}^{\bar{\beta}}x_n^{\beta_n}.$$

The map  $\rho$  extends uniquely to a ring homomorphism on the whole of  $k[x_1, \dots, x_n]$ . For a fixed  $N$ ,  $i \in \{1, \dots, N\}$ , and  $\beta_i = (\beta_{i1}, \dots, \beta_{in}) \in \mathbb{N}_0^n$ , we have  $\sum_{i=1}^N r_i x^{\beta_i} \in k[x_1, \dots, x_n]$ , and all polynomials in  $k[x_1, \dots, x_n]$  can be expressed in this manner. Now define:

$$\begin{aligned} \rho\left(\sum_{i=1}^N r_i x^{\beta_i}\right) &= \sum_{i=1}^N \rho(r_i x^{\beta_i}) \\ &= \sum_{i=1}^N r_i \bar{x}^{\bar{\beta}_i} x_n^{\beta_{in}}. \end{aligned}$$

Define, for  $p \in k[x_1, \dots, x_{n-1}]$  and  $d \in \mathbb{N}_0$ , the map  $\sigma : k[x_1, \dots, x_{n-1}][x_n] \rightarrow k[x_1, \dots, x_n]$  as

$$\sigma(px_n^d) := px_n^d.$$

The map  $\sigma$  extends uniquely to a ring homomorphism on the whole of  $k[x_1, \dots, x_n][x_{n-1}]$ . For a fixed  $N$ ,  $p_1, \dots, p_N \in k[x_1, \dots, x_{n-1}]$  and  $d_1, \dots, d_N \in \mathbb{N}_0$  we have  $\sum_{i=1}^N p_i x_n^{d_i} \in k[x_1, \dots, x_{n-1}][x_n]$  and any polynomial in  $k[x_1, \dots, x_{n-1}][x_n]$  can be expressed in this manner. Now define:

$$\sigma\left(\sum_{i=1}^N p_i x_n^{d_i}\right) = \sum_{i=1}^N (p_i x_n^{d_i}).$$

The maps  $\rho$  and  $\sigma$  are inverses. So we have that  $k[x_1, \dots, x_n]$  and  $k[x_1, \dots, x_{n-1}][x_n]$  are ring-isomorphic.  $\square$

Now we have all the pieces needed to prove the Hilbert Basis Theorem, an important result. It is used in the proofs of Theorem 4.2.9 and Theorem 5.4.4, which, respectively, establish the correctness of Algorithm 4.2.7 and Algorithm 5.4.3.

**THEOREM 2.2.5.** (Hilbert Basis Theorem) [1, Theorem 1.1.1]. *Let  $n \in \mathbb{N}$  and let  $k$  be a field. The polynomial ring  $k[x_1, \dots, x_n]$  in  $n$  indeterminates is Noetherian.*

PROOF. We proceed by induction on the number of indeterminates. With one indeterminate we are in the situation in Lemma 2.2.3, and so we have that  $k[x_1]$  is a Noetherian ring, since the field  $k$  is Noetherian.<sup>1</sup>

Now fix a natural number  $i$  and assume that  $k[x_1, \dots, x_i]$  is a Noetherian ring. Consider

$$k[x_1, \dots, x_i][x_{i+1}]$$

the polynomial ring over  $x_{i+1}$  with coefficients in  $k[x_1, \dots, x_i]$ . By Lemma 2.2.4 this ring is ring-isomorphic to  $k[x_1, \dots, x_{i+1}]$ , under an isomorphism  $I$ .

Now, since  $k[x_1, \dots, x_i]$  is Noetherian by the induction hypothesis, we can say that

$$k[x_1, \dots, x_i][x_{i+1}]$$

<sup>1</sup>This is trivial:  $k$  and  $\{0\}$  are the only ideals of  $k$ .

is also Noetherian, using Lemma 2.2.3. Thus we have that  $k[x_1, \dots, x_{i+1}]$  is Noetherian, since  $k[x_1, \dots, x_i][x_{i+1}] \cong k[x_1, \dots, x_{i+1}]$ . This completes the induction and so we have that for any  $n \in \mathbb{N}$ ,  $k[x_1, \dots, x_n]$  is Noetherian.  $\square$

Finally we come to the crucial result that term orders are well-orderings. As previously mentioned, this is needed to prove that the underlying algorithms for computing Gröbner bases terminate.

PROPOSITION 2.2.6. [1, Theorem 1.4.6]. *Let  $n \in \mathbb{N}$ . Any term order  $\prec$  on  $P_n$  is a well-ordering.*

PROOF. Suppose for a contradiction that there exists a sequence  $(X_i) \in P_n$  such that  $X_1 \succ X_2 \succ \dots$ . We claim that we have a chain of ideals in  $k[x_1, \dots, x_n]$ :

$$\langle X_1 \rangle \subsetneq \langle X_1, X_2 \rangle \subsetneq \dots$$

For every  $i \in \mathbb{N}$  we prove the claim that  $\langle X_1, \dots, X_i \rangle \neq \langle X_1, \dots, X_{i+1} \rangle$ . Fix an  $i \in \mathbb{N}$  and suppose that  $\langle X_1, \dots, X_i \rangle = \langle X_1, \dots, X_{i+1} \rangle$ . Then there exist polynomials  $u_1, \dots, u_i \in k[x_1, \dots, x_n]$  such that  $X_{i+1} = \sum_{k=1}^i u_k X_k$ . For any  $j \in \{1, \dots, i\}$ ,  $u_j$  can be written as a linear combination of power products and we have that every term of the polynomial  $u_j X_j$  is a term multiplied by  $X_j$ , meaning each term of  $u_j X_j$  is divisible by  $X_j$ . Thus for each term of  $\sum_{k=1}^i u_k X_k$  there exists some  $X_j \in \{X_1, \dots, X_i\}$  that divides that term. However, we must have a term in  $\sum_{j=1}^i u_j X_j$  whose power product is  $X_{i+1}$ . Thus  $X_{i+1}$  is divisible by some  $X_j \in \{X_1, \dots, X_i\}$  which, from Proposition 2.1.4, implies that  $X_j \prec X_{i+1}$ . However from the assumption that  $X_1 \succ X_2 \succ \dots$  and the fact that  $j < i + 1$ , we must have  $X_{i+1} \succ X_j$ , a contradiction. So we have proved the claim and thus have an infinite, increasing chain of ideals in  $k[x_1, \dots, x_n]$ , violating the Hilbert Basis Theorem. This proves that  $\prec$  is a well-ordering.  $\square$

## CHAPTER 3

## Polynomial Arithmetic

Much of our computing power will be dedicated to polynomial arithmetic. Throughout the various methods for computing Gröbner bases we make heavy use of some simple arithmetic algorithms.

### 3.1. Division Algorithms

The multivariate division algorithm (Algorithm 3.1.5), if applied to a linear polynomial, is in fact identical to the row operations performed in Gauss elimination, as illustrated in the linear case in Section 1.2.1. We give the univariate polynomial division algorithm for the reader to compare, but do not prove its correctness.

ALGORITHM 3.1.1. *The division algorithm (univariate).*

**Input:** Two polynomials  $f, g \in k[x_1]$ ,  $g \neq 0$

**Output:** A quotient and remainder,  $q, r$ , such that  $f = gq + r$   
and  $r = 0$  or  $\deg(r) < \deg(g)$

**Implementation:**

**Initialisation:**  $q := 0$ ,  $r := f$

**While**  $r \neq 0$  and  $\deg(g) \leq \deg(r)$ :

$$q := q + \frac{\text{lt}(r)}{\text{lt}(g)}$$

$$r := r - \frac{\text{lt}(r)}{\text{lt}(g)}g$$

The following definition is the multivariate analog to polynomial long division, hereafter referred to as polynomial reduction. This idea was mentioned previously, in Chapter 1, and we formalise it here.

DEFINITION 3.1.2. [1, Definition 1.5.1]. Let  $n \in \mathbb{N}$  and let  $f, g, h \in k[x_1, \dots, x_n]$ , with  $g \neq 0$ . We say that  $f$  *reduced to  $h$  modulo  $g$*  in one step, written  $f \xrightarrow{g} h$ , if  $\text{lp}(g)$  divides a non-zero term  $cX$ ,  $c \in k$  and  $X \in P_n$ , that appears in  $f$  and  $h = f - \frac{cX}{\text{lt}(g)}g$ .

Next, we extend this idea to allow us to reduce a polynomial by several polynomials.

DEFINITION 3.1.3. [1, Definition 1.5.3]. Let  $s, n \in \mathbb{N}$ , let  $f, h \in k[x_1, \dots, x_n]$  be polynomials and let  $F = \{f_1, \dots, f_s\} \subseteq k[x_1, \dots, x_n]$  be a set of non-zero polynomials. We say that  $f$  *reduces to  $h$  modulo  $F$* , denoted  $f \xrightarrow{F}_+ h$ , if there exists a sequence of indices  $i_1, \dots, i_t \in \{1, \dots, s\}$  and a sequence of polynomials  $h_1, \dots, h_{t-1} \in k[x_1, \dots, x_n]$  such that

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \dots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h.$$

One can see the analogy between the univariate and multivariate division. Both are expressing a polynomial as a combination of other polynomials. This is by design, since expressing a polynomial this way is exactly what it means for that polynomial to be in the ideal generated by the polynomials used in the reduction.

DEFINITION 3.1.4. [1, Definition 1.5.5]. Let  $s, n \in \mathbb{N}$ , let  $f \in k[x_1, \dots, x_n]$  and let  $F = \{f_1, \dots, f_s\} \subseteq k[x_1, \dots, x_n]$  be a set of polynomials. Let  $f \xrightarrow{F}_+ r$  for some  $r \in k[x_1, \dots, x_n]$ . If  $r = 0$  or not one of the power products in  $r$  is divisible by any of the leading power products of polynomial in  $F$  we call  $r$  a *remainder* and say that  $r$  is *reduced with respect to  $F$* . If not one of the power products in  $f$  is divisible by any of the leading power products of polynomials in  $F$  then we say  $f$  is *irreducible modulo  $F$* .

We now present the division algorithm for multivariate polynomials. It is an extremely important algorithm, as it is used in virtually every step of the computation of a Gröbner basis and is responsible for most of the computing power used.

ALGORITHM 3.1.5. [1, Algorithm 1.5.1]. *The Division Algorithm (multivariate).*

Input:  $f, f_1, \dots, f_s \in k[x_1, \dots, x_n]$  with  $f_1, \dots, f_s$  all non-zero.

Output:  $r$ , the remainder when  $f$  is reduced modulo  $f_1, \dots, f_s$

Implementation:

Initialisation:  $u_1, \dots, u_s := 0$ ,  $r := 0$ ,  $h := f$ .

While  $h \neq 0$ :

If there exists an  $i \in \{1, \dots, s\}$  such that  $\text{lp}(h) | \text{lp}(f_i)$  then:

Choose the least such  $i$

$$u_i := u_i + \frac{\text{lt}(h)}{\text{lt}(f_i)}$$

$$h := h - \frac{\text{lt}(h)}{\text{lt}(f_i)} f_i$$

Else:

$$r := r + \text{lt}(h)$$

$$h := h - \text{lt}(h)$$

Return  $r$

We provide a simple example illustrating Algorithm 3.1.5.

EXAMPLE 3.1.6. The Division Algorithm

Let  $f_1 = xy - y$ ,  $f_2 = y^2 - x$ , and  $f = xy^2$  and reduce  $f$  modulo  $\{f_1, f_2\}$  as in Algorithm 3.1.5, using the term order  $\prec_{\text{deglex}}$ , (Example 2.1.7), with  $y \succ x$ . Initialising the working variables, we have  $h = f$  and  $r = u_1 = u_2 = 0$ .

On the first pass through the while loop, we have that  $xy = \text{lp}(f_1)$  divides  $\text{lp}(h) = xy^2$ . Then

$$u_1 := u_1 + \frac{\text{lt}(h)}{\text{lt}(f_1)} = 0 + \frac{xy^2}{xy} = y$$

$$h := h - \frac{\text{lt}(h)}{\text{lt}(f_1)} f_1 = xy^2 - y(xy - y) = y^2$$

On the second pass through the while loop, we have that  $\text{lp}(f_1) = xy$  does not divide  $\text{lp}(h) = y^2$ , but  $\text{lp}(f_2) = y^2$  does. Then

$$u_2 := u_2 + \frac{\text{lt}(h)}{\text{lt}(f_2)} = 0 + \frac{y^2}{y^2} = 1$$

$$h := h - \frac{\text{lt}(h)}{\text{lt}(f_2)} f_2 = y^2 - 1 \cdot (y^2 - x) = x$$

On the third pass through the while loop, we have that neither  $\text{lp}(f_1) = xy$  divides  $\text{lp}(h) = x$  nor  $\text{lp}(f_2) = y^2$  divides  $\text{lp}(h)$ . Then

$$r := r + \text{lt}(h) = x$$

$$h := h - \text{lt}(h) = 0$$

The while loop then stops, since  $h = 0$ , and we have that

$$f \longrightarrow_{+}^{\{f_1, f_2\}} x$$

with  $f = yf_1 + f_2 + x$ .

Importantly, the lead product of the polynomial being reduced is either cancelled and written as a product of the lead products of the reducers or it is the lead product of the remainder. This fact is encapsulated in the proof of correctness for the algorithm below.

**THEOREM 3.1.7.** [1, Theorem 1.5.9]. *Let  $\prec$  be a term order. For  $s, n \in \mathbb{N}$ , given a set of non-zero polynomials  $F := \{f_1, \dots, f_s\}$  and  $f \in k[x_1, \dots, x_n]$ , Algorithm 3.1.5 produces polynomials  $u_1, \dots, u_s, r \in k[x_1, \dots, x_n]$  such that  $f = u_1 f_1 + \dots + u_s f_s + r$ . The remainder  $r$  is reduced with respect to  $F$  and  $\text{lp}(f) = \max(\max_{1 \leq i \leq s} (\text{lp}(u_i) \text{lp}(f_i)), \text{lp}(r))$ .*

**PROOF.** We first show that the algorithm terminates. For each  $i = 1, \dots, s$ , let  $h_j, u_{ij}, r_j$  be the values of  $h$ ,  $u_i$  and  $r$  respectively after the  $j$ -th iteration of the while loop in Algorithm 3.1.5. We claim that  $\{\text{lp}(h_j)\}_{j \in \mathbb{N}_0}$  is a strictly decreasing sequence with respect to  $\prec$ . At the  $j$ -th iteration, there are two cases for the computation of  $h_{j+1}$ . The first is that  $\text{lp}(h_j) \mid \text{lp}(f_i)$  for some  $i \in \{1, \dots, s\}$ , and so  $h_{j+1} = h_j - \frac{\text{lt}(h_j)}{\text{lt}(f_i)} f_i$ . We can then write  $h_j - \frac{\text{lt}(h_j)}{\text{lt}(f_i)} f_i = h_j - \frac{\text{lt}(h_j)}{\text{lt}(f_i)} (\text{lt}(f_i) + \text{lower terms of } f_i)$  to see that the leading term of  $h_j$  is cancelled and only smaller terms are added to  $h_j$ . The second case is that  $\text{lp}(h_j) \nmid \text{lp}(f_i)$  for all  $i \in \{1, \dots, s\}$ , and so  $h_{j+1} = h_j - \text{lt}(h_j)$ . In this case the leading term of  $h_j$  is removed. In both cases we have  $\text{lp}(h_{j+1}) \prec \text{lp}(h_j)$ . Thus  $\{\text{lp}(h_j)\}_{j \in \mathbb{N}_0}$  is a strictly decreasing sequence of power products and since our term order is a well-ordering the sequence must have a least element, specifically  $h_l = 0$  for some  $l \in \mathbb{N}$ . Hence the algorithm terminates.

To show that  $r$  cannot be reduced modulo  $F$ , we note that  $r_0 = 0$ . At every stage of iteration  $j \geq 1$ , if an alteration is made to  $r_j$ , it is the adding of the term  $\text{lt}(h_j)$ . For this to happen we must have had that  $\text{lp}(h_j) \nmid \text{lp}(f_i)$  for all  $i \in \{1, \dots, s\}$ . Thus no term of  $r_j$  is divisible by any  $\text{lp}(f_i)$  at any stage of iteration  $j$ . Thus when the algorithm terminates we have that  $r$  will also have no terms that are divisible by any  $\text{lp}(f_i)$ . Thus  $r$  cannot be reduced modulo  $F$ .

It remains to prove  $\text{lp}(f) = \max(\max_{1 \leq i \leq s}(\text{lp}(u_i)\text{lp}(f_i)), \text{lp}(r))$ . We do this by showing that  $\text{lp}(f) = \max(\max_{1 \leq i \leq s}(\text{lp}(u_i)\text{lp}(f_i)), \text{lp}(r), \text{lp}(h_j))$  is a loop invariant<sup>1</sup>. The loop invariant  $\text{lp}(f)$  has the correct value upon initialization: We have (for  $j = 0$ )  $u_{i0} = 0$  for each  $i \in \{1, \dots, s\}$ ,  $r_0 = 0$  and  $h_0 = f$  so  $\text{lp}(f) = \text{lp}(h_0)$  and thus  $\text{lp}(f) = \max(\max_{1 \leq i \leq s}(\text{lp}(u_{i0})\text{lp}(f_i)), \text{lp}(r_0), \text{lp}(h_0))$  is true.

Now assume the loop has iterated  $j \geq 1$  times and that for the values of  $u_{1j}, \dots, u_{sj}, r_j, h_j$  we have  $\text{lp}(f) = \max(\max_{1 \leq i \leq s}(\text{lp}(u_{ij})\text{lp}(f_i)), \text{lp}(r_j), \text{lp}(h_j))$ . Upon iteration there are two cases: Either  $\text{lp}(h_j) | \text{lp}(f_k)$  for some  $k \in \{1, \dots, s\}$  or  $\text{lp}(h_j) \nmid \text{lp}(f_k)$  for all  $k \in \{1, \dots, s\}$ . Note also that, since  $\{\text{lp}(h_j)\}_{j \in \mathbb{N}_0}$  was shown to be a strictly decreasing sequence, for  $j \geq 1$ , we have  $\text{lp}(h_j) \prec \text{lp}(f)$ .

Case 1: Let  $\text{lp}(h_j) | \text{lp}(f_k)$  for some  $k \in \{1, \dots, s\}$ . Since  $\text{lp}(h_j) \prec \text{lp}(f)$  for  $j \geq 1$ , we must have one of the products in  $\{\text{lp}(u_{ij})\text{lp}(f_i)\}_{i \in \{1, \dots, s\}} \cup \{\text{lp}(r_j)\} \cup \{h_j\}$  equal to  $\text{lp}(f)$ . It may be the case that there is more than one  $k \in \{1, \dots, s\}$  such that  $\text{lp}(h_j) | \text{lp}(f_k)$ . For the least such  $k$  we add the term  $\frac{\text{lt}(h_j)}{\text{lt}(f_k)}$  to  $u_{kj}$  and subtract the polynomial  $\frac{\text{lt}(h_j)}{\text{lt}(f_k)} f_k$  from  $h_j$  to obtain  $u_{k(j+1)}$  and  $h_{j+1}$  respectively. The other values  $\{u_{ij}\}_{i \neq k}$  and  $r_j$  remain unchanged through this iteration. We claim that the updated values  $u_{k(j+1)}$  and  $h_{j+1}$  will preserve the equality  $\text{lp}(f) = \max(\max_{1 \leq i \leq s}(\text{lp}(u_{i(j+1)})\text{lp}(f_i)), \text{lp}(r_{j+1}), \text{lp}(h_{j+1}))$ . We need only consider any new products that appear in  $\{\text{lp}(u_{i(j+1)})\text{lp}(f_i)\}_{i \in \{1, \dots, s\}} \cup \{\text{lp}(r_{j+1})\} \cup \{h_{j+1}\}$  and we show that they are less than  $\text{lp}(f)$  with respect to the term order  $\prec$ . We already know that  $\text{lp}(h_{j+1}) \prec \text{lp}(f)$ . For  $\text{lp}(u_{k(j+1)})\text{lp}(f_k)$ , the only difference between  $u_{k(j+1)}$  and  $u_{kj}$  is the term  $\frac{\text{lt}(h_j)}{\text{lt}(f_k)}$ . For this term consider  $\text{lp}(\frac{\text{lt}(h_j)}{\text{lt}(f_k)} f_k)$ : We have  $\text{lp}(\frac{\text{lt}(h_j)}{\text{lt}(f_k)} f_k) = \text{lp}(\frac{\text{lt}(h_j)}{\text{lt}(f_k)})\text{lp}(f_k) = \text{lp}(h_j) \prec \text{lp}(f)$  and so any new products in  $\frac{\text{lt}(h_j)}{\text{lt}(f_k)} f_k$  are also less than  $\text{lp}(f)$ . Since, for some  $k \in \{1, \dots, s\}$ , we had  $\text{lp}(h_j) | \text{lp}(f_k)$ ,  $r_j$  is unaltered and  $r_j = r_{j+1}$ . Thus the equality  $\text{lp}(f) = \max(\max_{1 \leq i \leq s}(\text{lp}(u_{i(j+1)})\text{lp}(f_i)), \text{lp}(r_{j+1}), \text{lp}(h_{j+1}))$  is preserved.

Case 2: Let  $\text{lp}(h_j) \nmid \text{lp}(f_k)$  for all  $k \in \{1, \dots, s\}$ . In this case  $r_j$  and  $h_j$  are altered by addition and subtraction of  $\text{lt}(h_j)$  respectively and all  $\{u_{ij}\}_i$  are unaltered. Clearly if one of  $\text{lp}(r_j)$  or  $\text{lp}(h_j)$  was equal to  $\text{lp}(f)$  before alteration one of them will be afterwards as well, since the only change is  $\text{lt}(h_j)$  being subtracted from  $h_j$  and added to  $r_j$ . So in this case we also have  $\text{lp}(f) = \max(\max_{1 \leq i \leq s}(\text{lp}(u_{i(j+1)})\text{lp}(f_i)), \text{lp}(r_{j+1}), \text{lp}(h_{j+1}))$

In both cases we have  $\text{lp}(f) = \max(\max_{1 \leq i \leq s}(\text{lp}(u_{i(j+1)})\text{lp}(f_i)), \text{lp}(r_{j+1}), \text{lp}(h_{j+1}))$  and since the algorithm terminates with  $h_l = 0$  we must have  $\text{lp}(f) = \max(\max_{1 \leq i \leq s}(\text{lp}(u_{il})\text{lp}(f_i)), \text{lp}(r_l))$ . Letting  $u_{1l}, \dots, u_{sl}$  and  $r_l$  denote the outputs of the algorithm,  $u_1, \dots, u_s$  and  $r$  respectively, we have the result.  $\square$

It should be noted that the remainder computed by the above algorithm need not be unique. For example, consider  $f = x^2y^2 + x + y$ ,  $f_1 = x^2y + 1$ , and  $f_2 = xy^2 + 1$ . If we use  $\prec_{lex}$ , (Example 2.1.6) with  $x \succ y$  and run Algorithm 3.1.5, we see that  $u_1 = y$ ,  $u_2 = 0$ ,  $r_1 = x$  and  $f = u_1f_1 + u_2f_2 + r_1$ , thus

$$f \longrightarrow_{\{f_1, f_2\}} r_1$$

and  $r_1$  is reduced modulo  $\{f_1, f_2\}$ . Then  $\text{lp}(f) = \max\{\max\{\text{lp}(g_1)\text{lp}(x)\}, \text{lp}(y)\} = x^2y^2$ , as promised by Theorem 3.1.7. Now, we reverse the roles of  $f_1$  and  $f_2$ . We then have  $u_1 = x$ ,  $u_2 = 0$ ,  $r_2 = y$  and  $f = u_1f_1 + u_2f_2 + r_2$ , and thus

$$f \longrightarrow_{\{f_1, f_2\}} r_2$$

<sup>1</sup>A *loop invariant* is a value in the loop of an algorithm that doesn't change from any one iteration of the loop to the next.

and  $r_2$  is reduced modulo  $\{f_1, f_2\}$ . We still have  $\text{lp}(f) = \max\{\max\{\text{lp}(g_1)\text{lp}(y)\}, \text{lp}(x)\} = x^2y^2$ , but  $r_1 \neq r_2$ .

Theorem 4.1.9 will show that a sufficient condition for a set of polynomials to be a Gröbner basis for an ideal is that the remainder upon applying the division algorithm is always unique, for any polynomial.

## CHAPTER 4

## Gröbner bases

We now come to the main results of this dissertation. Here we formally define the Gröbner basis and present an algorithm used in its computation. We prove the correctness of the algorithm as well as several other important results. Corollary 4.1.5 guarantees the existence of a Gröbner basis and Theorem 4.3.7 guarantees we can find a unique Gröbner basis.

### 4.1. Preliminaries

**DEFINITION 4.1.1.** Let  $t, n \in \mathbb{N}$  and let  $G := \{g_1, \dots, g_t\} \subseteq k[x_1, \dots, x_n]$  be a set of non-zero polynomials contained in an ideal  $I$  of  $k[x_1, \dots, x_n]$ . The set  $G$  is called a *Gröbner basis* for  $I$  if, for all non-zero  $f \in I$ , there exists  $i \in \{1, \dots, t\}$  such that  $\text{lp}(g_i)$  divides  $\text{lp}(f)$ .

The following theorem gives some equivalent conditions for when a finite subset of an ideal is a Gröbner basis. These equivalent conditions are very useful in proving some of the other results that follow.

**THEOREM 4.1.2.** [1, Theorem 1.6.2]. *Let  $n, t \in \mathbb{N}$ , let  $I$  be a non-zero ideal of  $k[x_1, \dots, x_n]$  and let  $G = \{g_1, \dots, g_t\} \subseteq I$ . The following statements are equivalent:*

- (i) *The set  $G$  is a Gröbner basis for  $I$ .*
- (ii) *For any  $f \in k[x_1, \dots, x_n]$ ,  $f \in I$  if and only if  $f \rightarrow_+^G 0$ .*
- (iii) *For any  $f \in k[x_1, \dots, x_n]$ ,  $f \in I$  if and only if there exist  $h_1, \dots, h_t \in k[x_1, \dots, x_n]$  such that  $f = \sum_{i=1}^t h_i g_i$  with  $\text{lp}(f) = \max_{1 \leq i \leq t} (\text{lp}(h_i) \text{lp}(g_i))$ .*
- (iv)  *$Lt(G) = Lt(I)$ .*

**PROOF.** (i) $\Rightarrow$ (ii): Let  $G$  be a Gröbner basis for  $I$  and let  $f \in k[x_1, \dots, x_n]$  be arbitrary. Assume  $f \in I$ . By Theorem 3.1.7 there exists  $r \in k[x_1, \dots, x_n]$ , reduced with respect to  $G$ , and  $u_1, \dots, u_t \in k[x_1, \dots, x_n]$  such that  $f = \sum_{i=1}^t g_i u_i + r$ . If  $r = 0$  we have  $f \rightarrow_+^G 0$ . If  $r \neq 0$  then, since we have  $f, g_1 u_1 + \dots + g_t u_t \in I$ , we have  $r = f - (g_1 u_1 + \dots + g_t u_t) \in I$ . By the definition of a Gröbner basis, there exists an  $i \in \{1, \dots, t\}$  such that  $\text{lp}(g_i)$  divides  $\text{lp}(r)$ . This then contradicts the fact that  $r$  is reduced with respect to  $G$  and so we cannot have  $r \neq 0$ . Thus  $r = 0$  and  $f \rightarrow_+^G 0$ .

Conversely, assume that  $f \rightarrow_+^G 0$ . Then by Theorem 3.1.7 there exist  $u_1, \dots, u_t \in k[x_1, \dots, x_n]$  such that  $f = g_1 u_1 + \dots + g_t u_t$  and so  $f \in I$ .

(ii)  $\Rightarrow$  (iii): Let  $f \in k[x_1, \dots, x_n]$  be arbitrary and assume that  $f \in I$  if and only if  $f \rightarrow_+^G 0$ . First assume that  $f \in I$ . Then by assumption we have  $f \rightarrow_+^G 0$ , so by Theorem 3.1.7 there exist  $h_1, \dots, h_t \in k[x_1, \dots, x_n]$  such that  $f = \sum_{i=1}^t h_i g_i$  and  $\text{lp}(f) = \text{lp}(\sum_{i=1}^t h_i g_i) = \max_{1 \leq i \leq t} (\text{lp}(h_i) \text{lp}(g_i))$ .

Conversely, assume that for some  $h_1, \dots, h_t \in k[x_1, \dots, x_n]$  we have  $f = \sum_{i=1}^t h_i g_i$  and  $\text{lp}(f) = \max_{1 \leq i \leq t} (\text{lp}(h_i) \text{lp}(g_i))$ . Clearly we have  $f \in I$ .



(iii)  $\Rightarrow$  (iv): Assume that for an arbitrary  $f \in k[x_1, \dots, x_n]$ ,  $f \in I$  if and only if there exist  $h_1, \dots, h_t \in k[x_1, \dots, x_n]$  such that  $f = \sum_{i=1}^t h_i g_i$  and  $\text{lp}(f) = \max_{1 \leq i \leq t} (\text{lp}(h_i) \text{lp}(g_i))$ . Since  $G \subseteq I$ , we have  $\text{Lt}(G) \subseteq \text{Lt}(I)$ . For the reverse inclusion, let  $f \in I$ . Then there exist  $h_1, \dots, h_t \in k[x_1, \dots, x_n]$  such that  $f = \sum_{i=1}^t h_i g_i$ . Choose an  $i \in \{1, \dots, t\}$  such that  $\text{lp}(f) = \text{lp}(h_i) \text{lp}(g_i)$ . Since  $\text{lp}(g_i) \in \text{Lt}(G)$ , it follows that  $\text{lp}(f) \in \text{Lt}(G)$ . The result follows since for an arbitrary  $f \in I$  we have shown that  $\text{lt}(f) \in \text{Lt}(G)$  and since  $\text{Lt}(I)$  is the ideal generated by all the  $\text{lt}(f)$  we have the desired result.

(iv)  $\Rightarrow$  (i): Let  $f \in I$  be arbitrary. Then  $\text{lt}(f) \in \text{Lt}(I) = \text{Lt}(G)$  and hence there exist  $h_1, \dots, h_t \in k[x_1, \dots, x_n]$  such that  $\text{lt}(f) = \sum_{i=1}^t h_i \text{lt}(g_i)$ . Each term in the right hand side of the previous expression is divisible by some  $\text{lp}(g_i)$ . Thus  $\text{lt}(f)$ , the only term in the left hand side, is also divisible by some  $\text{lp}(g_i)$ , and so  $G$  is a Gröbner basis.  $\square$

As a corollary to the above theorem we see that, as promised in Chapter 1, the Gröbner basis generates the ideal for which it is a basis.

**COROLLARY 4.1.3.** [1, Corollary 1.6.3]. *Let  $n \in \mathbb{N}$  and let  $I$  be an ideal in  $k[x_1, \dots, x_n]$ . If  $G = \{g_1, \dots, g_t\}$  is a Gröbner basis for  $I$ , then  $I = \langle g_1, \dots, g_t \rangle$ .*

**PROOF.** Each  $g_i$  is in  $I$  and so  $\langle g_1, \dots, g_t \rangle \subseteq I$ . For the reverse inclusion, let  $f \in I$ . By Theorem 4.1.2(ii),  $f \xrightarrow{G}_+ 0$  and so there exist  $h_1, \dots, h_t$  such that  $f = \sum_{i=1}^t h_i g_i$  and so  $f \in \langle g_1, \dots, g_t \rangle$ .  $\square$

The next result is crucial in allowing us to show the existence of Gröbner bases, and makes use of the Hilbert Basis Theorem (Theorem 2.2.5).

**LEMMA 4.1.4.** [1, Lemma 1.6.4]. *Let  $n \in \mathbb{N}$ , and let  $S$  be a set of power products. Let  $I$  be the ideal generated by  $S$  and let  $f \in k[x_1, \dots, x_n]$ . Then  $f$  is in  $I$  if and only if for every product  $X$  appearing in  $f$  there exists a  $Y_i \in S$  such that  $Y_i$  divides  $X$ . Moreover, there exists a finite subset  $S_0$  of  $S$  such that  $I = \langle S_0 \rangle$ .*

**PROOF.** Let  $f \in I$  be arbitrary. Then there exists  $t \in \mathbb{N}$ ,  $h_1, \dots, h_t \in k[x_1, \dots, x_n]$  and  $X_1, \dots, X_t \in S$  such that

$$f = \sum_{i=1}^t h_i X_i.$$

Each term on the right hand side of the above equation is divisible by some  $X_i$  in  $S$ , and hence every term of the left hand side must also be divisible by some term  $X_i \in S$ .

For the converse, assume that for every product  $X$  appearing in  $f$  there exists an  $X_i \in S$  such that  $X_i$  divides  $X$ . Each such  $X$  is in  $I = \langle S \rangle$  because  $X = ZX_i$  for some  $Z \in P_n$ . Hence  $f$  is in  $I$ .

For the final statement note that, by the Hilbert Basis Theorem (Theorem 2.2.5),  $I$  has a finite generating set, say  $\{b_1, \dots, b_m\} = B \subseteq I$ . Since  $S$  generates  $I$ , for each  $b_i \in B$  there exist  $t_i \in \mathbb{N}$ ,  $g_1, \dots, g_{t_i} \in k[x_1, \dots, x_n]$  and  $X_{i1}, \dots, X_{it_i} \in S$  such that  $b_i = \sum_{j=1}^{t_i} g_i X_{ij}$ . We claim that the set  $S_0 := \{X_{ij} \mid i \in \{1, \dots, m\}, j \in \{1, \dots, t_i\}\}$  is then the required set, i.e.  $S_0$  generates  $I$ .

To prove this, note that since  $S_0 \subseteq S$  we have  $\langle S_0 \rangle \subseteq \langle S \rangle = I$ . For the reverse inclusion, since  $B$  generates  $I$ , for an arbitrary  $f \in I$  there exist  $g_1, \dots, g_m \in k[x_1, \dots, x_n]$  such that  $f = \sum_{i=1}^m g_i b_i$ . Each of these  $b_i$  can be written as a combination of elements from  $S_0$ , as shown above. Thus  $f \in \langle S_0 \rangle$  and so  $I \subseteq \langle S_0 \rangle$ . The claim is then proved.  $\square$

Lemma 4.1.4 gives rise to the following corollary that tells us that a Gröbner basis always exists for any non-zero ideal of  $k[x_1, \dots, x_n]$ :

**COROLLARY 4.1.5.** [1, Corollary 1.6.5]. *Let  $n \in \mathbb{N}$  and let  $I \subseteq k[x_1, \dots, x_n]$  be a non-zero ideal.  $I$  has a Gröbner basis.*

**PROOF.** By Lemma 4.1.4 the leading term ideal  $\text{Lt}(I)$  has a finite generating set. Without loss of generality we can let  $t \in \mathbb{N}$  and write this set as  $\{\text{lt}(g_1), \dots, \text{lt}(g_t)\}$  with  $g_1, \dots, g_t \in I$ . If we let  $G = \{g_1, \dots, g_t\}$  then we have, by Theorem 4.1.2, that  $\text{Lt}(G) = \text{Lt}(I)$  and hence  $G$  is a Gröbner basis for  $I$ .  $\square$

**DEFINITION 4.1.6.** Let  $t \in \mathbb{N}$  and let  $G := \{g_1, \dots, g_t\} \subseteq k[x_1, \dots, x_n]$ . We say  $G$  is a *Gröbner basis* if it is a Gröbner basis for the ideal  $\langle G \rangle$  that  $G$  generates.

The following small result is necessary to prove one of the more important results later on (Lemma 5.1.4).

**LEMMA 4.1.7.** [1, Exercise 1.6.13]. *Let  $\{g_1, \dots, g_t\} \subseteq k[x_1, \dots, x_n]$  and let  $0 \neq h \in k[x_1, \dots, x_n]$ .  $\{g_1, \dots, g_t\}$  is a Gröbner basis if and only if  $\{hg_1, \dots, hg_t\}$  is a Gröbner basis.*

**PROOF.** Firstly, let  $\{g_1, \dots, g_t\}$  be a Gröbner basis and let  $f \in \langle hg_1, \dots, hg_t \rangle$ . Thus for some  $u_1, \dots, u_t \in k[x_1, \dots, x_n]$  we can write  $f = u_1hg_1 + \dots + u_thg_t$ . If we can find an  $i \in \{1, \dots, t\}$  such that  $\text{lp}(f) | \text{lp}(hg_i)$  then  $\{hg_1, \dots, hg_t\}$  will be a Gröbner basis. Let  $g := u_1g_1 + \dots + u_tg_t$ , then we have  $f = hg$ . Since  $g \in \langle g_1, \dots, g_t \rangle$  and  $\{g_1, \dots, g_t\}$  is a Gröbner basis, by Definition 4.1.1 there exists an  $i' \in \{1, \dots, t\}$  such that  $\text{lp}(g) | \text{lp}(g_{i'})$  and hence  $\text{lp}(f) = \text{lp}(hg) | \text{lp}(hg_{i'})$  so  $\{hg_1, \dots, hg_t\}$  is a Gröbner basis.

Now assume that  $\{hg_1, \dots, hg_t\}$  is a Gröbner basis and let  $f \in \langle g_1, \dots, g_t \rangle$ . Thus for some  $u_1, \dots, u_t \in k[x_1, \dots, x_n]$  we can write  $f = u_1g_1 + \dots + u_tg_t$ . Now we have  $hf \in \langle hg_1, \dots, hg_t \rangle$  and so there exists an  $i \in \{1, \dots, t\}$  such that  $\text{lp}(hf) | \text{lp}(hg_i)$ . Then we immediately have that  $\text{lp}(f) | \text{lp}(g_i)$  and so  $\{g_1, \dots, g_t\}$  is a Gröbner basis.  $\square$

Before we can prove the upcoming crucial Theorem 4.1.9 we need to prove another small result:

**LEMMA 4.1.8.** [1, Theorem 1.6.7]. *Let  $c \in k \setminus \{0\}$ ,  $X \in P_n$ , let  $g \in k[x_1, \dots, x_n]$  and let  $G = \{g_1, \dots, g_t\} \subseteq k[x_1, \dots, x_n]$  such that  $g \rightarrow_+^G r$ . Assume that the remainder of  $g$  reduced modulo  $G$  is unique. Then we have, for each  $i \in \{1, \dots, t\}$ ,  $g - cXg_i \rightarrow_+^G r$ .*

**PROOF.** Fix an arbitrary  $i \in \{1, \dots, t\}$ . We are able to represent  $g$  in the following way: There exists  $m \in \mathbb{N}$ ,  $a, c_1, \dots, c_m \in k$  and  $X_1, \dots, X_m \in P_n$  with  $X_j \neq X \text{lp}(g_i)$  for  $j \in \{1, \dots, m\}$  such that  $g = (\sum_{j=1}^m c_j X_j) + aX \text{lp}(g_i)$ , with  $a$ , the coefficient of  $X \text{lp}(g_i)$ , possibly being zero. We have 3 cases to consider:

Case 1:  $a = 0$ . Then the coefficient of  $X \text{lp}(g_i)$  in  $g - cXg_i$  is  $-c \text{lc}(g_i)$ . This is non-zero and so  $g - cXg_i \rightarrow^{g_i} g \rightarrow_+^G r$ , which is what we require.

Case 2:  $a = \text{clc}(g_i)$ . Let  $g - cXg_i \rightarrow_+^G r_1$ . Now, since  $aX \text{lp}(g_i) = \text{clc}(g_i)X \text{lp}(g_i)$ , we have  $g \rightarrow^{g_i} g - cXg_i \rightarrow_+^G r_1$ . But then we have that  $g \rightarrow_+^G r$  and  $g \rightarrow_+^G r_1$  and, because we have assumed remainders are unique,  $r_1 = r$  and so we have that  $g - cXg_i \rightarrow_+^G r$ .

Case 3:  $a \neq 0$  and  $a \neq \text{clc}(g_i)$ . Let  $h := g - \frac{a}{\text{lc}(g_i)}Xg_i$ . Then the coefficient of  $X \text{lp}(g_i)$  in  $h$  is 0, so we have  $g \rightarrow^{g_i} h$ . Similarly, since  $a \neq \text{clc}(g_i)$ , we have  $g - cXg_i \rightarrow^{g_i} h$ . Letting  $h \rightarrow_+^G r_2$  we have  $g \rightarrow^{g_i} h \rightarrow_+^G r_2$  and again by the uniqueness of remainders we have  $r = r_2$  yielding the final sequence  $g - cXg_i \rightarrow^{g_i} h \rightarrow_+^G r$ .  $\square$

**THEOREM 4.1.9.** [1, Theorem 1.6.7]. *Let  $n, t \in \mathbb{N}$  and let  $G := \{g_1, \dots, g_t\} \subseteq k[x_1, \dots, x_n]$ . Then  $G$  is a Gröbner basis if and only if for all  $f \in k[x_1, \dots, x_n]$ , the remainder of the reduction of  $f$  modulo  $G$  is unique.*

PROOF. Let  $G$  be a Gröbner basis, let  $f \in k[x_1, \dots, x_n]$  and suppose that  $f \xrightarrow{G}_+ r_1$  and  $f \xrightarrow{G}_+ r_2$  with  $r_1, r_2$  reduced with respect to  $G$ . Then there exist  $u_1, \dots, u_t, v_1, \dots, v_t \in k[x_1, \dots, x_n]$  such that  $f - r_1 = \sum_{i=1}^t u_i g_i$  and  $f - r_2 = \sum_{i=1}^t v_i g_i$ . Thus  $f - r_1, f - r_2 \in \langle G \rangle$  and so  $r_1 - r_2 \in \langle G \rangle$ , and  $r_1 - r_2$  is reduced with respect to  $G$ , since each power product in  $r_1 - r_2$  is a power product in  $r_1$  or  $r_2$  or both. Now, Theorem 4.1.2(ii) implies that  $r_1 - r_2 = 0$ , and so we have that the remainder of the reduction of  $f$  modulo  $G$  is unique.

Now, assume that for every polynomial  $f \in k[x_1, \dots, x_n]$  the remainder of the reduction of  $f$  modulo  $G$  is unique. Let  $f \in \langle G \rangle$  and suppose that  $f \xrightarrow{G}_+ r$ . Since  $f \in \langle G \rangle$  there exist  $h_1, \dots, h_t$  such that  $f = \sum_{i=1}^t h_i g_i$ .

First we write each  $h_i$  as a particular sum of terms: Let  $S$  be a finite enumerated list of all the products appearing in  $\{h_i\}_{i \in \{1, \dots, t\}}$ , hence for some  $k \in \mathbb{N}$  we have  $S = \{X_1, \dots, X_k\}$ . For each  $i \in \{1, \dots, t\}$ , there exists a set of coefficients  $C_i = \{c_{i1}, \dots, c_{ik}\}$ , not all 0, such that  $h_i = \sum_{j=1}^k c_{ij} X_j$ . Then we can apply Lemma 4.1.8 to  $f$ , with  $c_{11}, X_1, g_1$  to obtain  $f - c_{11} X_1 g_1 \xrightarrow{G}_+ r$ . Apply the lemma again to  $f - c_{11} X_1 g_1$ , with  $c_{12}, X_2$  and  $g_1$  to obtain  $f - c_{11} X_1 g_1 - c_{12} X_2 g_1 \xrightarrow{G}_+ r$ . Repeating this process through all the terms  $c_{ij} X_j g_i$ , we can exhaust every term that appears in  $f$  and obtain

$$0 \xrightarrow{G}_+ r.$$

Now we can see that we must have  $r = 0$  and so we have, for an arbitrary  $f \in \langle G \rangle$ , that  $f \xrightarrow{G}_+ 0$  which, by Theorem 4.1.2, means that  $G$  is a Gröbner basis.  $\square$

## 4.2. Buchberger's Theorem and Buchberger's Algorithm

In this section we present the algorithm that Buchberger created. We begin this section with a definition that will form the core of any computation of a Gröbner basis, previously mentioned in Chapter 1, the  $S$ -polynomial.

DEFINITION 4.2.1. Let  $n \in \mathbb{N}$ , let  $f, g \in k[x_1, \dots, x_n]$  be non-zero, and let  $\prec$  be a term order. The polynomial

$$S(f, g) = \frac{\text{lcm}(\text{lp}(f), \text{lp}(g))}{\text{lt}(f)} f - \frac{\text{lcm}(\text{lp}(f), \text{lp}(g))}{\text{lt}(g)} g$$

is called the  $S$ -polynomial of  $f$  and  $g$ .

REMARK 4.2.2. By construction the  $S$ -polynomial of two polynomials  $f, g \in k[x_1, \dots, x_n]$  will cancel the leading term of both  $f$  and  $g$ . i.e. neither  $\text{lt}(f)$  nor  $\text{lt}(g)$  appear in  $S(f, g)$ .

PROPOSITION 4.2.3. For two polynomials  $f, g \in k[x_1, \dots, x_n]$  and a product  $X \in P_n$ , if  $\text{lp}(f) = \text{lp}(g) = X$  then  $\text{lp}(S(f, g)) \prec X$ .

PROOF. From Definition 4.2.1 we have  $\text{lcm}(\text{lp}(f), \text{lp}(g)) = X$ . Together with the fact that  $\text{lt}(f) = \text{lc}(f)\text{lp}(f)$  and  $\text{lt}(g) = \text{lc}(g)\text{lp}(g)$  we get

$$S(f, g) = \frac{X}{\text{lc}(f)X} f - \frac{X}{\text{lc}(g)X} g = \frac{1}{\text{lc}(f)} f - \frac{1}{\text{lc}(g)} g.$$

This results in the lead terms of  $f$  and  $g$  being equal, and so they cancel. Since both  $f$  and  $g$  are only multiplied by a constant their other products are unchanged. Since these products were smaller than the leading product to begin with, they remain so. Therefore  $\text{lp}(S(f, g)) \prec \text{lp}(f) = X$ .  $\square$

LEMMA 4.2.4. Let  $t \in \mathbb{N}$ , let  $f, g \in k[x_1, \dots, x_n]$ , let  $F = \{f_1, \dots, f_t\} \subseteq k[x_1, \dots, x_n]$  and let  $X \in P_n$ . We have the following:

- (i) If  $f \xrightarrow{+F} g$  then  $Xf \xrightarrow{+F} Xg$ .  
 (ii) If  $f \in F$  then  $fg \xrightarrow{+F} 0$ .

PROOF. (i) Since  $f \xrightarrow{+F} g$  there exists a sequence of indices  $i_1, \dots, i_s \subseteq \{1, \dots, t\}$  such that  $f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \dots \xrightarrow{f_{i_{s-1}}} h_{s-1} \xrightarrow{f_{i_s}} g$ . From Definition 3.1.2 we see that, for some  $X_1, X_2 \in P_n$ ,  $h_1 = f - X_1 f_{i_1}$  and  $h_2 = h_1 - X_2 f_{i_2}$  meaning  $h_2 = f - X_1 f_{i_1} - X_2 f_{i_2}$ . Continuing in this fashion we see that  $g = f - X_1 f_{i_1} \dots - X_s f_{i_s}$  and if we multiply this equation on both sides by  $X$  we obtain  $Xg = Xf - X X_1 f_{i_1} - \dots - X X_s f_{i_s}$ . By Definition 3.1.3 we immediately have  $Xf \xrightarrow{+F} Xg$  as required.

(ii) If  $f \in F$  then  $fg$  reduces to 0 modulo  $F$  trivially in one step, since for any  $g \in k[x_1, \dots, x_n]$ ,  $fg - fg = 0$  and Definition 3.1.3 gives the result.  $\square$

LEMMA 4.2.5. [1, Lemma 1.7.5]. *Let  $n, s \in \mathbb{N}$ , let  $\prec$  be a term order, and let  $F := \{f_1, \dots, f_s\} \subseteq k[x_1, \dots, x_n]$  be a set of non-zero polynomials such that  $\text{lp}(f_1) = \text{lp}(f_2) = \dots = \text{lp}(f_s) = X$ . Let  $f = \sum_{i=1}^s c_i f_i$  with  $c_i \in k$ ,  $i \in \{1, \dots, s\}$ . If  $\text{lp}(f) \prec X$ , then  $f$  is a linear combination of  $\{S(f_i, f_j)\}_{1 \leq i < j \leq s}$ , with coefficients in  $k$ .*

PROOF. For each  $i \in \{1, \dots, s\}$  we write  $f_i = a_i X + (\text{lower terms of } f_i)$ , with  $a_i \in k/\{0\}$ . By the assumption that  $\text{lp}(f) \prec X$  we must have that the coefficients corresponding to  $X$  in each  $f_i$  cancel each other out, so  $\sum_{i=1}^s c_i a_i = 0$ . For any  $i \neq j$  we have  $S(f_i, f_j) = \frac{1}{a_i} f_i - \frac{1}{a_j} f_j$  due to the assumption of equal leading products and so we can write:

$$\begin{aligned}
 f &= \sum_{i=1}^s c_i f_i \\
 &= \sum_{i=1}^s c_i a_i \left( \frac{1}{a_i} f_i \right) \\
 &= c_1 a_1 \left( \frac{1}{a_1} f_1 - \frac{1}{a_2} f_2 \right) + c_1 a_1 \frac{1}{a_2} f_2 + c_2 a_2 \left( \frac{1}{a_2} f_2 - \frac{1}{a_3} f_3 \right) + \sum_{i=3}^s c_i a_i \left( \frac{1}{a_i} f_i \right) \\
 &\vdots \\
 &= c_1 a_1 \left( \frac{1}{a_1} f_1 - \frac{1}{a_2} f_2 \right) + (c_1 a_1 + c_2 a_2) \left( \frac{1}{a_2} f_2 - \frac{1}{a_3} f_3 \right) + (c_1 a_1 + c_2 a_2 + c_3 a_3) \left( \frac{1}{a_3} f_3 - \frac{1}{a_4} f_4 \right) + \dots \\
 &\quad + (c_1 a_1 + \dots + c_{s-1} a_{s-1}) \left( \frac{1}{a_{s-1}} f_{s-1} - \frac{1}{a_s} f_s \right) + \sum_{i=1}^s c_i a_i \left( \frac{1}{a_s} f_s \right) \\
 &= \left( \sum_{i=1}^{s-1} \left( \sum_{j=1}^i c_j a_j \right) \left( \frac{1}{a_i} f_i - \frac{1}{a_{i+1}} f_{i+1} \right) \right) + \underbrace{\left( \sum_{i=1}^s c_i a_i \right)}_{=0} \frac{1}{a_s} f_s \\
 &= \left( \sum_{i=1}^{s-1} \left( \sum_{j=1}^i c_j a_j \right) S(f_i, f_{i+1}) \right).
 \end{aligned}$$

$\square$

**THEOREM 4.2.6.** (Buchberger's Theorem) [1, Theorem 1.7.4]. *Let  $t, n \in \mathbb{N}$  and let  $G = \{g_1, \dots, g_t\}$  be a set of non-zero polynomials in  $k[x_1, \dots, x_n]$ . Then  $G$  is a Gröbner basis if and only if for all  $i \neq j \in \{1, \dots, t\}$  we have*

$$S(g_i, g_j) \xrightarrow{G}_+ 0.$$

**PROOF.** Let  $G$  be a Gröbner basis for the ideal  $I := \langle G \rangle$ . We have that  $S(g_i, g_j) \in I$  for any  $i \neq j$  and so by Theorem 4.1.2 we have  $S(g_i, g_j) \xrightarrow{G}_+ 0$ .

We now prove the converse. Assume that  $S(g_i, g_j) \xrightarrow{G}_+ 0$  for all  $i \neq j$ . Let  $f \in I$ . Thus there exist  $h_1, \dots, h_t \in k[x_1, \dots, x_n]$  such that  $f = \sum_{i=1}^t h_i g_i$ . We can write  $f$  as such a combination of  $g_i$ 's in a number of ways and since the term order is a well-ordering (Proposition 2.2.6) we can choose a representation where  $X := \max_{1 \leq i \leq t} (\text{lp}(h_i) \text{lp}(g_i))$  is a minimum with respect to the given term order.

We claim that  $X = \text{lp}(f)$ . Firstly, since  $f$  is a sum of polynomials of the form  $h_i g_i$  and for each of these we have  $\text{lp}(h_i g_i) = \text{lp}(h_i) \text{lp}(g_i) \preceq X$ , we must have  $\text{lp}(f) \preceq X$ . Now suppose  $\text{lp}(f) \prec X$ . We will find a different representation of  $f$ , say some  $u_1, \dots, u_t \in k[x_1, \dots, x_n]$  and  $f = \sum_{i=1}^t u_i g_i$ , such that  $\max_{1 \leq i \leq t} (\text{lp}(u_i) \text{lp}(g_i)) \prec X$  for a contradiction. Let  $S = \{i \in \{1, \dots, t\} \mid \text{lp}(h_i) \text{lp}(g_i) = X\}$ . Since  $X$  is the maximum of all the  $\text{lp}(h_i) \text{lp}(g_i)$  there must be at least one element in  $S$ . For each  $i \in S$  there exist an  $X_i \in P_n$  and  $c_i \in k$  such that  $h_i = c_i X_i + (\text{lower terms of } h_i)$ . Now let  $g := \sum_{i \in S} c_i X_i g_i$ . This construction enables us to write

$$\begin{aligned} f &= \sum_{i=1}^t h_i g_i \\ &= \sum_{i \in S} h_i g_i + \sum_{i \notin S} h_i g_i \\ &= \sum_{i \in S} (c_i X_i + (\text{lower terms of } h_i)) g_i + \sum_{i \notin S} h_i g_i \\ &= \sum_{i \in S} c_i X_i g_i + \sum_{i \in S} (\text{lower terms of } h_i) g_i + \sum_{i \notin S} h_i g_i \\ &= g + \sum_{i \in S} (\text{lower terms of } h_i) g_i + \sum_{i \notin S} h_i g_i. \end{aligned}$$

The terms in  $\sum_{i \in S} (\text{lower terms of } h_i) g_i$  are smaller than the terms in  $g$ , with respect to the term order. For each  $i \notin S$  we have  $\text{lp}(h_i) \prec X$ , and so the terms in  $\sum_{i \notin S} h_i g_i$  are also smaller than the terms in  $g$  with respect to the term order. Then we have  $\text{lp}(g) = \text{lp}(f) \prec X$ . Now, by construction,  $g$  meets the criteria of Lemma 4.2.5: We have  $\text{lp}(X_i g_i) = X$  for each  $i \in S$  and  $g = \sum_{i \in S} c_i X_i g_i$  with  $\text{lp}(g) \prec X$ . Thus there exist  $d_{ij} \in k$  such that

$$g = \sum_{i < j \in S} d_{ij} S(X_i g_i, X_j g_j).$$

Recalling that, for each  $k \in S$ ,  $\text{lp}(X_k g_k) = \text{lp}(h_k) \text{lp}(g_k) = X$  we have, for each  $i < j \in S$ , that  $X = \text{lcm}(\text{lp}(X_i g_i), \text{lp}(X_j g_j))$  and so from Definition 4.2.1, letting  $X_{ij} := \text{lcm}(\text{lp}(g_i), \text{lp}(g_j))$  we

obtain, for each  $i < j \in S$

$$\begin{aligned}
 S(X_i g_i, X_j g_j) &= \frac{X}{\text{lt}(X_i g_i)} X_i g_i - \frac{X}{\text{lt}(X_j g_j)} X_j g_j \\
 &= \frac{X}{\text{lt}(g_i)} g_i - \frac{X}{\text{lt}(g_j)} g_j \\
 &= \frac{X}{X_{ij}} \left( \frac{X_{ij}}{\text{lt}(g_i)} g_i - \frac{X_{ij}}{\text{lt}(g_j)} g_j \right) \\
 &= \frac{X}{X_{ij}} S(g_i, g_j).
 \end{aligned}$$

By hypothesis,  $S(g_i, g_j) \xrightarrow{G}_+ 0$  and by Lemma 4.2.4,  $\frac{X}{X_{ij}} S(g_i, g_j) \xrightarrow{G}_+ \frac{X}{X_{ij}} \cdot 0 = 0$ . Therefore, since  $S(X_i g_i, X_j g_j) = \frac{X}{X_{ij}} S(g_i, g_j)$ , we have  $S(X_i g_i, X_j g_j) \xrightarrow{G}_+ 0$ . Thus, by Theorem 3.1.7, for each  $i < j \in S$  there exist  $h_{ij1}, \dots, h_{ijt} \in k[x_1, \dots, x_n]$  such that:

$$S(X_i g_i, X_j g_j) = \sum_{\nu=1}^t h_{ij\nu} g_\nu$$

and  $\max_{1 \leq \nu \leq t} (\text{lp}(h_{ij\nu}) \text{lp}(g_\nu)) = \text{lp}(S(X_i g_i, X_j g_j))$ . Since  $\text{lp}(X_i g_i) = \text{lp}(X_j g_j) = X$  by Proposition 4.2.3, we obtain

$$\max_{1 \leq \nu \leq t} (\text{lp}(h_{ij\nu}) \text{lp}(g_\nu)) = \text{lp}(S(X_i g_i, X_j g_j)) \prec \max_{1 \leq i < j \leq t} (\text{lp}(X_i g_i), \text{lp}(X_j g_j)) = X.$$

Now we write

$$\begin{aligned}
 f &= g + \sum_{i \in S} (\text{lower terms of } h_i) g_i + \sum_{i \notin S} h_i g_i \\
 &= \sum_{i < j \in S} d_{ij} S(X_i g_i, X_j g_j) + \sum_{i \in S} (\text{lower terms of } h_i) g_i + \sum_{i \notin S} h_i g_i \\
 &= \sum_{i < j \in S} \sum_{\nu=1}^t d_{ij} h_{ij\nu} g_\nu + \sum_{i \in S} (\text{lower terms of } h_i) g_i + \sum_{i \notin S} h_i g_i \\
 &= \sum_{\nu=1}^t \left( \sum_{i < j \in S} d_{ij} h_{ij\nu} \right) g_\nu + \sum_{i \in S} (\text{lower terms of } h_i) g_i + \sum_{i \notin S} h_i g_i.
 \end{aligned}$$

Now, for  $1 \leq \nu \leq t$ , set

$$u_\nu := \begin{cases} \sum_{i < j \in S} d_{ij} h_{ij\nu} + (\text{lower terms of } h_\nu) & \text{if } \nu \in S \\ \sum_{i < j \in S} d_{ij} h_{ij\nu} + h_\nu & \text{if } \nu \notin S \end{cases}$$

and obtain  $f = \sum_{\nu=1}^t u_\nu g_\nu$ , a new representation for  $f$ . Now for  $\nu \in S$  we have

$$\text{lp}(u_\nu) \preceq \max(\max_{i < j \in S} (\text{lp}(h_{ij\nu})), \text{lp}(\text{lower terms of } h_\nu)),$$

and for  $\nu \notin S$  we have

$$\text{lp}(u_\nu) \preceq \max(\max_{i < j \in S} (\text{lp}(h_{ij\nu})), \text{lp}(h_\nu)).$$

We have shown above that for each  $i < j \in S$  we have  $\max_{1 \leq \nu \leq t} (\text{lp}(h_{ij\nu}) \text{lp}(g_\nu)) \prec X$ . We also have, for  $\nu \in S$ ,  $\text{lp}(\text{lower terms of } h_\nu) \text{lp}(g_\nu) \prec X$  and, for  $\nu \notin S$ ,  $\text{lp}(h_\nu) \text{lp}(g_\nu) \prec X$ . Thus we

have  $\max_{1 \leq \nu \leq t}(\text{lp}(u_\nu)\text{lp}(g_\nu)) \prec X$ . This contradicts the minimality of  $X$  with respect to  $\prec$  in the representation of  $f$ .

Therefore we have  $\text{lp}(f) = X$ . By Theorem 4.1.2(iii),  $G$  is a Gröbner basis.  $\square$

With this theorem we now have a powerful new condition and are in a position to describe how we might actually compute a Gröbner basis. The strategy is this: We begin with a given list of polynomials,  $F = \{f_1, \dots, f_t\} \in k[x_1, \dots, x_n]$  say, that generate an ideal for which we are to compute a Gröbner basis. We form all possible pairs of polynomials in  $F$  and maintain them in a list,  $\mathcal{G}$ . For each pair  $\{f_i, f_j\} \in \mathcal{G}$  we calculate

$$S(f_i, f_j) \xrightarrow{+}_F h.$$

From Theorem 4.2.6 we know that if  $h \neq 0$  then  $F$  could not have been a Gröbner basis for  $\langle F \rangle$ . We add  $h$  to  $G$  and add all the pairs  $\{f_i, h\}_{i \in \{1, \dots, t\}}$  to  $\mathcal{G}$ . Then reducing all the  $S$ -polynomials of pairs in  $\mathcal{G}$  modulo  $F$  again, we update the lists with any new non-zero remainders that are calculated and repeat. Due to an argument detailed in Theorem 4.2.9, making use of the Hilbert Basis Theorem, we find that eventually this procedure must stop. At that point the requirement of Theorem 4.2.6 is met and we have a Gröbner basis for  $\langle F \rangle$ . We note that there is no indication as to how many additional polynomials will be added to arrive at a Gröbner basis and, indeed, sometimes so many calculations are performed that computer systems can run out of memory. However, given infinite resources, the procedure described above will find a Gröbner basis, and this is Buchberger's Algorithm. The precise description is given below.

ALGORITHM 4.2.7. [1, Algorithm 1.7.1]. (*Buchberger's Algorithm*).

**Input:**  $F = \{f_1, \dots, f_s\}$  a list of non-zero polys in  $k[x_1, \dots, x_n]$

**Output:**  $G$ , a Gröbner basis for  $\langle F \rangle$

**Initialization:**

$$G := F$$

$$\mathcal{G} := \{(f_i, f_j) \subseteq G \mid 1 \leq i < j \leq s\}$$

**Implementation:**

**While**  $\mathcal{G} \neq \emptyset$ :

**Choose and remove a pair**  $(f, g) \in \mathcal{G}$

**Compute remainder**  $S(f, g) \xrightarrow{+}_G h$

**If**  $h \neq 0$ :

**Add new pairs**

$\{(u, h) \mid \text{for all } u \in G\}$  to  $\mathcal{G}$

**Add**  $h$  to  $G$

**Return**  $G$ .

We provide an example to illustrate the algorithm at work. There are numerous tedious computations, and so we truncate the example.

EXAMPLE 4.2.8. Buchberger's Algorithm

Let  $f_1 = y^2 + xy + x^2$ ,  $f_2 = y + x$  and  $f_3 = y$ . We use Algorithm 4.2.7 to compute a Gröbner basis for  $I = \langle f_1, f_2, f_3 \rangle$ , using  $\prec_{lex}$  (Example 2.1.6) with  $y \succ x$ . We initialise  $G := \{f_1, f_2, f_3\}$  and  $\mathcal{G} := \{\{f_1, f_2\}, \{f_1, f_3\}, \{f_2, f_3\}\}$ .

On the first pass through the while loop, we remove the first pair  $\{f_1, f_2\}$  from  $\mathcal{G}$ . Then

$$\mathcal{G} := \{\{f_1, f_3\}, \{f_2, f_3\}\}$$

and

$$S(f_1, f_2) \longrightarrow_+^G x^2$$

Letting  $f_4 := x^2$ , we have

$$\mathcal{G} := \{\{f_1, f_3\}, \{f_2, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$$

$$G := \{f_1, f_2, f_3, f_4\}$$

On the second pass through the while loop, we remove the pair  $\{f_1, f_3\}$  from  $\mathcal{G}$ . Then

$$\mathcal{G} := \{\{f_2, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$$

and

$$S(f_1, f_3) \longrightarrow_+^G 0$$

Since the S-polynomial reduced to 0 we don't add the result to  $G$ .

On the third pass through the while loop, we remove the pair  $\{f_2, f_3\}$  from  $\mathcal{G}$ . Then

$$\mathcal{G} := \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$$

and

$$S(f_2, f_3) \longrightarrow_+^G x$$

Letting  $f_5 := x$ , we have

$$\mathcal{G} := \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}, \{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$$

$$G := \{f_1, f_2, f_3, f_4, f_5\}$$

On the fourth pass through the while loop, we remove the pair  $\{f_1, f_4\}$  from  $\mathcal{G}$ . Then

$$\mathcal{G} := \{\{f_2, f_4\}, \{f_3, f_4\}, \{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$$

and

$$S(f_1, f_4) \longrightarrow_+^G 0$$

Again, we have a 0 remainder, and so nothing is added to  $G$ .

On the subsequent passes through the while loop, all S-polynomials reduce to 0 and we exhaust the pairs in  $\mathcal{G}$ . The algorithm terminates when  $\mathcal{G}$  is empty, and we have  $G = \{f_1, f_2, f_3, f_4, f_5\}$ , which is then a Gröbner basis for  $\langle f_1, f_2, f_3 \rangle$ .

As usual, we follow up the algorithm with a proof of its correctness.

**THEOREM 4.2.9.** [1, Theorem 1.7.8]. *Algorithm 4.2.7 terminates and produces a Gröbner basis for any given list of polynomials.*

**PROOF.** Let  $F, G$  be as in the algorithm. Suppose with a view to a contradiction that the algorithm does not terminate. Then, as the algorithm iterates, we obtain a strictly increasing infinite sequence: Let  $G_i$  denote the value of  $G$  at the start of the  $i$ -th iteration of the while-loop in Algorithm 4.2.7 that produces a non-zero  $h$ . Then we have the chain:

$$G_1 \subsetneq G_2 \subsetneq \dots$$



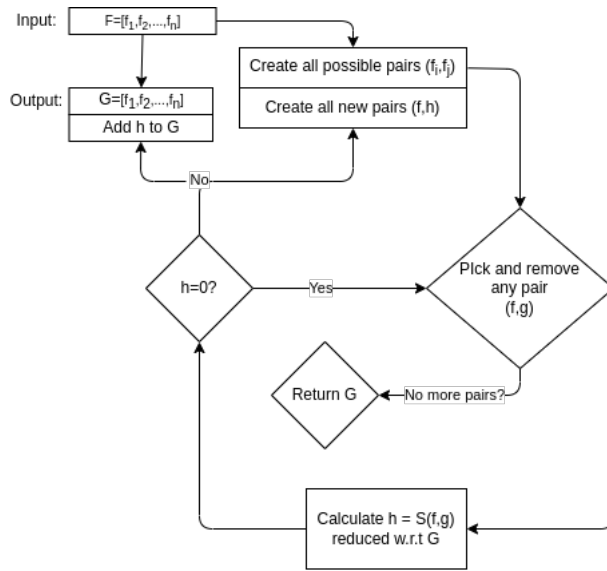


FIGURE 4.2.1. A flow diagram for Algorithm 4.2.7.

At each step, a  $G_i$  is obtained from a  $G_{i-1}$  by adding a non-zero remainder,  $h$ , of the reduction of an  $S$ -polynomial of two elements of  $G_{i-1}$  modulo  $G_{i-1}$ . By Definition 3.1.3,  $h$  is reduced with respect to  $G_{i-1}$  and so  $\text{lt}(h) \notin \text{Lt}(G_{i-1})$  which now gives us

$$\text{Lt}(G_1) \subsetneq \text{Lt}(G_2) \subsetneq \dots$$

Here we see we have obtained a strictly increasing chain of ideals which contradicts the Hilbert Basis Theorem, and so the algorithm must terminate. To see that Algorithm 4.2.7 produces a Gröbner basis, note that the first polynomial,  $h_1$  say, added to  $G$  satisfied, for some  $f_i, f_j \in F$ ,  $S(f_i, f_j) \xrightarrow{F} h_1$  and so we have  $h_1 \in \langle F \rangle$ . Clearly, any subsequent polynomials added will also be in  $\langle F \rangle$  and so we have  $F \subseteq G \subseteq \langle F \rangle$ . Thus  $\langle F \rangle \subseteq \langle G \rangle \subseteq \langle F \rangle$ , which makes  $G$  a generating set for the ideal  $\langle F \rangle$ . Furthermore, for any polynomials  $g_i, g_j \in G$  we have, by virtue of how they are constructed in the algorithm,  $S(g_i, g_j) \xrightarrow{G} 0$  which, by Theorem 4.2.6, makes  $G$  a Gröbner basis for  $\langle F \rangle$ .  $\square$

We also include a flow diagram to help understand the workings of Algorithm 4.2.7, in Figure 4.2.

### 4.3. Minimal and Reduced Gröbner bases

The results from Section 4.1 and Section 4.2 tell us of the existence and computation of a Gröbner basis. However, a Gröbner basis is not necessarily unique and depends on the order in which polynomials are reduced as well as the term order applied. The results in this section show that we can define a stricter condition to impose on a Gröbner basis that actually makes it unique.

**DEFINITION 4.3.1.** Let  $t, n \in \mathbb{N}$ . A Gröbner basis  $G = \{g_1, \dots, g_t\}$  in  $k[x_1, \dots, x_n]$  is called *minimal* if  $\text{lc}(g_i) = 1$  for  $i \in \{1, \dots, t\}$  and  $\text{lp}(g_j) \nmid \text{lp}(g_i)$  for all  $i \neq j$ .

LEMMA 4.3.2. [1, Lemma 1.8.2]. *Let  $t, n \in \mathbb{N}$  and let  $G = \{g_1, \dots, g_t\}$  be a Gröbner basis for an ideal  $I \subseteq k[x_1, \dots, x_n]$ . If  $\text{lp}(g_1) | \text{lp}(g_2)$  then  $\{g_2, \dots, g_t\}$  is also a Gröbner basis for  $I$ .*

PROOF. Firstly, note that if  $\text{lp}(g_1) | \text{lp}(g_2)$  then for any polynomial  $f \in k[x_1, \dots, x_n]$  such that  $\text{lp}(f) | \text{lp}(g_1)$  we have  $\text{lp}(f) | \text{lp}(g_2)$ .

Let  $f \in I$ . By Definition 4.1.1 we have  $\text{lp}(f) | \text{lp}(g_i)$  for some  $i \in \{1, \dots, t\}$ . If  $i \neq 1$  then  $\text{lp}(f) | \text{lp}(g_i)$  for some  $i \in \{2, \dots, t\}$ . If  $i = 1$  then  $\text{lp}(f) | \text{lp}(g_2)$  as noted above. In both cases we have  $\text{lp}(f) | \text{lp}(g_i)$  for some  $i \in \{2, \dots, t\}$  making  $\{g_2, \dots, g_t\}$  a Gröbner basis for  $I$ .  $\square$

COROLLARY 4.3.3. [1, Corollary 1.8.3]. *Let  $t, n \in \mathbb{N}$  and let  $G = \{g_1, \dots, g_t\}$  be a Gröbner basis for an ideal  $I \subseteq k[x_1, \dots, x_n]$ . There exists an  $H \subseteq G$  which is a minimal Gröbner basis for  $I$ .*

PROOF. We can renumber as necessary without loss of generality, and use Lemma 4.3.2 to remove all  $g_i$  if, for  $j \neq i$ , there is a  $g_j$  such that  $\text{lp}(g_i) | \text{lp}(g_j)$  and still have a Gröbner basis. Divide the remaining  $g_i$  by  $\text{lc}(g_i)$  and the basis is then a minimal basis.  $\square$

PROPOSITION 4.3.4. [1, Proposition 1.8.4]. *For  $s, t \in \mathbb{N}$ , if  $G = \{g_1, \dots, g_t\}$ , and  $F = \{f_1, \dots, f_s\}$  are minimal Gröbner bases for an ideal  $I$ , then  $s = t$  and, after renumbering if necessary,  $\text{lt}(f_i) = \text{lt}(g_i)$  for  $i \in \{1, \dots, t\}$ .*

PROOF. Firstly,  $f_1 \in I$  and  $G$  is a Gröbner basis for  $I$  so there exists  $i$  such that  $\text{lp}(f_1) | \text{lp}(g_i)$ . Renumbering if necessary, we can assume  $i = 1$ .  $g_1$  is also in  $I$ , and so symmetrically we can obtain  $j$  such that  $\text{lp}(g_1) | \text{lp}(f_j)$ . Now we have that  $\text{lp}(g_1) | \text{lp}(f_j)$  and  $\text{lp}(f_1) | \text{lp}(g_1)$  and so  $\text{lp}(f_1) | \text{lp}(f_j)$ .  $F$  is minimal so this must mean that  $j = 1$ . Thus we have that  $\text{lp}(f_1) = \text{lp}(g_1)$ .

The argument can be repeated for all the remaining polynomials in  $G$  and  $F$ . In general for a fixed  $i \in \{1, \dots, s\}$ , after having shown that  $\text{lp}(f_1) = \text{lp}(g_1)$ ,  $\text{lp}(f_2) = \text{lp}(g_2)$ ,  $\dots$ ,  $\text{lp}(f_{i-1}) = \text{lp}(g_{i-1})$  we consider  $f_i \in I$ . There exists a  $j \in \{1, \dots, s\}$  such that  $\text{lp}(f_i) | \text{lp}(g_j)$ . We must have  $j \in \{i, \dots, s\}$  because otherwise one of  $\text{lp}(g_1), \dots, \text{lp}(g_{i-1})$  would divide  $\text{lp}(f_i)$  and so one of  $\text{lp}(f_1), \dots, \text{lp}(f_{i-1})$  also divides  $\text{lp}(f_i)$  as they have already been shown to be equal. This contradicts the minimality of  $F$ , and so we can renumber to obtain  $j = i$  and  $\text{lp}(f_i) = \text{lp}(g_i)$ . This process will exhaust both the bases, which then are necessarily the same size, i.e.  $s = t$ .  $\square$

So we see that minimal bases always exist, but there is a stricter condition we can impose.

DEFINITION 4.3.5. Let  $n, t \in \mathbb{N}$ . A Gröbner basis  $G = \{g_1, \dots, g_t\} \subseteq k[x_1, \dots, x_n]$  is called a *reduced Gröbner basis* if, for any  $i \in \{1, \dots, t\}$ ,  $\text{lc}(g_i) = 1$  and for  $j \neq i$  and  $j \in \{1, \dots, t\}$ , no terms in  $g_i$  are divisible by any  $\text{lp}(g_j)$ .

The following result tells us that a reduced Gröbner basis exists for a given minimal basis, and how it can be obtained.

COROLLARY 4.3.6. [1, Corollary 1.8.6]. *Let  $G = \{g_1, \dots, g_t\}$  be a minimal Gröbner basis for the ideal  $I$ . Consider the following series of reductions:*

$$\begin{aligned}
 g_1 &\longrightarrow_+^{H_1} h_1 && \text{with } h_1 \text{ reduced with respect to } H_1 := \{g_2, \dots, g_t\} \\
 g_2 &\longrightarrow_+^{H_2} h_2 && \text{with } h_2 \text{ reduced with respect to } H_2 := \{h_1, g_3, \dots, g_t\} \\
 g_3 &\longrightarrow_+^{H_3} h_3 && \text{with } h_3 \text{ reduced with respect to } H_3 := \{h_1, h_2, g_4, \dots, g_t\} \\
 &\vdots && \\
 g_t &\longrightarrow_+^{H_t} h_t && \text{with } h_t \text{ reduced with respect to } H_t := \{h_1, h_2, \dots, h_{t-1}\}
 \end{aligned}$$

Then  $H := \{h_1, \dots, h_t\}$  is a reduced Gröbner basis for  $I$ .

PROOF. Due to  $G$  being minimal we have that, for each distinct  $i, j \in \{1, \dots, t\}$ ,  $\text{lp}(g_i) \nmid \text{lp}(g_j)$ . Starting with  $i = 1$  and  $j \in \{2, \dots, t\}$ , we have  $\text{lp}(g_1) \nmid \text{lp}(g_j)$  and so when reducing  $g_1$  with respect to  $H_1$  we have  $\text{lt}(h_1) = \text{lt}(g_1)$ , as the leading term of  $g_1$  cannot be cancelled. This implies that  $\text{lp}(g_2) \nmid \text{lp}(h_1)$  and so we can repeat the previous argument with  $g_2$  and  $H_2$ . Then we have  $\text{lt}(h_2) = \text{lt}(g_2)$ . We continue until we have, for each  $i \in \{1, \dots, t\}$ ,  $\text{lt}(h_i) = \text{lt}(g_i)$ . Since  $G$  was minimal we get  $\text{lc}(h_i) = \text{lc}(g_i) = 1$  and so immediately  $H$  is a minimal Gröbner basis for  $I$ . Now, each  $g_i$  is reduced using  $\text{lp}(h_1), \dots, \text{lp}(h_{i-1}), \text{lp}(g_{i+1}), \dots, \text{lp}(g_t)$  and  $\text{lp}(h_j) = \text{lp}(g_j)$  for all  $j \in \{1, \dots, t\}$ . Therefore  $h_i$  is reduced with respect to  $H/\{h_i\}$  for each  $i \in \{1, \dots, t\}$ , which means no terms in  $h_i$  are divisible by any  $\text{lp}(h_j)$  for  $j \in \{1, \dots, t\} \setminus \{i\}$ . Thus  $H$  is a reduced Gröbner basis.  $\square$

THEOREM 4.3.7. [1, Theorem 1.8.7]. *Let  $t, n \in \mathbb{N}$  and let  $\prec$  be a term order. Every non-zero ideal  $I$  contained in  $k[x_1, \dots, x_n]$  has a unique reduced Gröbner basis with respect to  $\prec$ .*

PROOF. Any Gröbner basis has a minimal Gröbner basis, by Corollary 4.3.3, and a reduced Gröbner basis can be obtained from a minimal Gröbner basis by Proposition 4.3.4. Therefore we need only prove uniqueness. Let  $G := \{g_1, \dots, g_t\}$  and  $H := \{h_1, \dots, h_s\}$  be reduced Gröbner bases for  $I$ . Proposition 4.3.4 tells us that  $s = t$  and, for each  $i \in \{1, \dots, t\}$ ,  $\text{lt}(g_i) = \text{lt}(h_i)$ . Fix an  $i \in \{1, \dots, t\}$ . If  $g_i \neq h_i$  then  $g_i - h_i \in I$  and this implies that there exists  $j$  such that  $\text{lp}(g_i - h_i) \mid \text{lp}(h_j)$ . Since  $\text{lt}(g_i) = \text{lt}(h_i)$  we have  $\text{lp}(g_i - h_i) \prec \text{lp}(h_i)$ . Now if  $i = j$  we would have  $\text{lp}(g_i - h_i) \mid \text{lp}(h_i)$  and  $\text{lp}(g_i - h_i) \prec \text{lp}(h_i)$ , a contradiction, so we conclude  $i \neq j$ . However  $\text{lp}(h_j) = \text{lp}(g_j)$ , so we have that a term of  $g_i - h_i$  is divisible by  $\text{lp}(h_j) = \text{lp}(g_j)$  for  $i \neq j$ . Thus a term of  $g_i$  or  $h_i$  is divisible by  $\text{lp}(g_j)$  or  $\text{lp}(h_j)$  for  $i \neq j$ . This contradicts the fact that  $G$  and  $H$  are reduced and so  $g_i = h_i$ .  $\square$

## CHAPTER 5

## Improvements to Buchberger's Algorithm

As discussed previously, the simplicity of Buchberger's Algorithm comes at the cost of possibly having to compute prohibitively large numbers of  $S$ -polynomials and their reductions. It turns out to be the case that many of these computations are unnecessary. This chapter details some results (Lemma 5.1.4 and Corollary 5.3.2) and an algorithm (Algorithm 5.4.3) that allow us to predict at least some of the  $S$ -polynomials that will can be ignored, potentially saving on computation costs. For example, in the linear case in Section 1.2.1, we saw that a Gröbner basis had been found after two calculations, but Buchberger's Algorithm would continue to perform the remaining eight calculations. Algorithm 5.4.3 will be able to recognise which of those eight calculations needn't have been performed.

This chapter introduces two sub-algorithms that will be used to improve Buchberger's Algorithm.

During Buchberger's Algorithm, if we are computing a Gröbner basis for the ideal generated by  $G = \{f_1, \dots, f_i\}$ , before we reduce one of the  $S$ -polynomials, say  $S(f_i, f_j)$ , we can check if Lemma 5.1.4 holds which will then tell us that  $S(f_i, f_j) \rightarrow_+^{\{f_i, f_j\}} 0$ . Clearly then, since  $f_i, f_j \in G$ , we also have  $S(f_i, f_j) \rightarrow_+^G 0$ . Thus we needn't perform this reduction in the first place and the algorithm can continue. This is detailed in a sub-algorithm, Algorithm 5.4.1. The improved algorithm will also check if the conditions of Corollary 5.3.2 hold for 3 distinct pairs, say  $(f_i, f_j), (f_j, f_k)$  and  $(f_i, f_k)$ , and if it does we can safely remove one of the pairs and avoid having to reduce its  $S$ -polynomial. This is explained in detail in Section 5.2.

We begin with some preliminary definitions and results that will form the basis of the first sub-algorithm. Then we develop some new theory involving modules that allows us to create the second sub-algorithm.

### 5.1. The first new criterion

There are three results in this section. The first two are needed to prove the third, and the third result used in the sub-algorithm. They make use of properties of modulo reduction and relative primeness of power products.

The first result tells us we can divide the arguments of an  $S$ -polynomial by a common divisor and have it still reduce to 0.

LEMMA 5.1.1. *Let  $f, g, d \in k[x_1, \dots, x_n]$  and suppose that  $d$  divides both  $f$  and  $g$ . If*

$$S(f, g) \rightarrow_+^{\{f, g\}} 0$$

*then  $S(\frac{f}{d}, \frac{g}{d}) \rightarrow_+^{\{\frac{f}{d}, \frac{g}{d}\}} 0$ .*

PROOF. Firstly we show that  $S(\frac{f}{d}, \frac{g}{d}) = \frac{1}{d}S(f, g)$ . Since  $d$  divides  $f$  and  $g$ , there exist polynomials  $f'$  and  $g'$  such that  $f = df'$  and  $g = dg'$ . If we define  $X := \text{lcm}(\text{lt}(f), \text{lt}(g))$  and

$X' := \text{lcm}(\text{lt}(f'), \text{lt}(g'))$  then we have

$$S\left(\frac{f}{d}, \frac{g}{d}\right) = \frac{X'}{\text{lt}(f')}f' - \frac{X'}{\text{lt}(g')}g'$$

and

$$\frac{1}{d}S(f, g) = \frac{1}{d}\left(\frac{X}{\text{lt}(f)}f - \frac{X}{\text{lt}(g)}g\right) = \frac{X}{\text{lt}(f)}f' - \frac{X}{\text{lt}(g)}g'.$$

It remains to show that  $\frac{X}{\text{lt}(f)} = \frac{X'}{\text{lt}(f')}$  and  $\frac{X}{\text{lt}(g)} = \frac{X'}{\text{lt}(g')}$ . Now, since  $f = df'$  and  $g = dg'$  we have

$$\text{lt}(f) = \text{lt}(df') = \text{lt}(d)\text{lt}(f')$$

and similarly

$$\text{lt}(g) = \text{lt}(d)\text{lt}(g').$$

This implies that

$$X = \text{lcm}(\text{lt}(f), \text{lt}(g)) = \text{lcm}(\text{lt}(d)\text{lt}(f'), \text{lt}(d)\text{lt}(g')) = \text{lt}(d)X'.$$

Now we can write  $\frac{X}{\text{lt}(f)} = \frac{\text{lt}(d)X'}{\text{lt}(d)\text{lt}(f')} = \frac{X'}{\text{lt}(f')}$  and similarly we have  $\frac{X}{\text{lt}(g)} = \frac{X'}{\text{lt}(g')}$ . Thus we have proved that  $\frac{1}{d}S(f, g) = S\left(\frac{f}{d}, \frac{g}{d}\right)$ .

Now, assume that  $S(f, g) \rightarrow_+^{\{f, g\}} 0$ . Thus there exist polynomials  $u, v \in k[x_1, \dots, x_n]$  such that  $S(f, g) = uf + vg$ . Trivially, we then have

$$\frac{1}{d}S(f, g) = \frac{1}{d}(uf + vg) = u\frac{f}{d} + v\frac{g}{d}$$

and, since  $\frac{1}{d}S(f, g) = S\left(\frac{f}{d}, \frac{g}{d}\right)$ , the result is proved.  $\square$

**DEFINITION 5.1.2.** We say that two power products  $X, Y \in P_n$  are *relatively prime* if  $\text{gcd}(X, Y) = 1$  or equivalently that  $\text{lcm}(X, Y) = XY$ .

The next result is a special case of the main result of this section.

**LEMMA 5.1.3.** [1, Lemma 3.3.1]. *Let  $f, g \in k[x_1, \dots, x_n]$  and assume  $\text{gcd}(f, g) = 1$ . Then the following statements are equivalent:*

- (i)  $S(f, g) \rightarrow_+^{\{f, g\}} 0$ .
- (ii)  $\text{lp}(f)$  and  $\text{lp}(g)$  are relatively prime.

**PROOF.** (i)  $\implies$  (ii): Assume that  $S(f, g) \rightarrow_+^{\{f, g\}} 0$ . Let  $D = \text{gcd}(\text{lp}(f), \text{lp}(g))$ . Then there exist  $X, Y \in P_n$  such that  $\text{lp}(f) = DX$  and  $\text{lp}(g) = DY$ . If  $D = 1$  then we have the result. Now assume that  $D \neq 1$ . We have

$$S(f, g) = \frac{Y}{\text{lc}(f)}f - \frac{X}{\text{lc}(g)}g$$

and, by the initial assumption that  $S(f, g) \rightarrow_+^{\{f, g\}} 0$  and Theorem 3.1.7, there exist  $u, v \in k[x_1, \dots, x_n]$  such that  $S(f, g) = uf + vg$  and  $\text{lp}(uf) \preceq \text{lp}(S(f, g))$  and  $\text{lp}(vg) \preceq \text{lp}(S(f, g))$ . Now we have that

$$uf + vg = \frac{Y}{\text{lc}(f)}f - \frac{X}{\text{lc}(g)}g$$

and so

$$\left(\frac{X}{\text{lc}(g)} + v\right)g = \left(\frac{Y}{\text{lc}(f)} - u\right)f.$$

Thus since  $\gcd(f, g) = 1$  we have that  $f$  divides  $\frac{X}{\text{lc}(g)} + v$  and  $g$  divides  $\frac{Y}{\text{lc}(f)} - u$ .

We have  $\text{lp}(uf) \preceq \text{lp}(S(f, g))$ . Thus by Remark 4.2.2 we have  $\text{lp}(u)DX \preceq \text{lp}(S(f, g)) \prec X\text{lp}(g)$ . But  $\text{lp}(S(f, g)) \prec X\text{lp}(g) \prec XDY$ . Thus  $\text{lp}(u) \prec Y$  and hence  $\text{lp}(\frac{Y}{\text{lc}(f)} - u) = Y$ . Thus, since  $g$  divides  $\frac{Y}{\text{lc}(f)} - u$ , we have  $\text{lp}(g)$  divides  $\text{lp}(\frac{Y}{\text{lc}(f)} - u)$  which means that  $DY$  divides  $Y$  so  $D = 1$ . Thus we have proved that  $\text{lp}(f)$  and  $\text{lp}(g)$  are relatively prime.

(ii)  $\implies$  (i) Assume that  $\text{lp}(f)$  and  $\text{lp}(g)$  are relatively prime. For some  $a, b \in k$  and  $X, Y \in P_n$  we can write  $f = aX +$  (lower terms of  $f$ ) and  $g = bY +$  (lower terms of  $g$ ). Letting  $f' = f - aX$  and  $g' = g - bY$  we can write  $X = \frac{1}{a}(f - f')$  and  $Y = \frac{1}{b}(g - g')$ .

Case 1:  $g' = f' = 0$ . Then  $f$  and  $g$  both consist of single terms and  $S(f, g) = 0$  (see Remark 4.2.2).

Case 2:  $f' = 0$  and  $g' \neq 0$ . Since  $\gcd(\text{lp}(f), \text{lp}(g)) = 1$  and  $\text{lcm}(\text{lp}(f), \text{lp}(g)) = XY$  we have

$$\begin{aligned} S(f, g) &= \frac{1}{a}Yf - \frac{1}{b}Xg \\ &= \frac{1}{ab}(g - g')f - \frac{1}{ab}fg \\ &= -\frac{1}{ab}fg'. \end{aligned}$$

Thus by Lemma 4.2.4(ii) we have that  $S(f, g) \xrightarrow{\{f, g\}} 0$ .

Case 3: Symmetrical to Case 2, interchanging  $f$  and  $g$ .

Case 4:  $f' \neq 0$  and  $g' \neq 0$ . Again, since  $\gcd(\text{lp}(f), \text{lp}(g)) = 1$  we have

$$\begin{aligned} S(f, g) &= \frac{1}{a}Yf - \frac{1}{b}Xg \\ &= \frac{1}{ab}(g - g')f - \frac{1}{ab}(f - f')g \\ &= \frac{1}{ab}(f'g - g'f). \end{aligned}$$

We claim that  $\text{lp}(f'g) \neq \text{lp}(g'f)$ . If  $\text{lp}(f'g) = \text{lp}(g'f)$  then  $\text{lp}(f')\text{lp}(g) = \text{lp}(f)\text{lp}(g')$  and since  $\gcd(\text{lp}(f), \text{lp}(g)) = 1$  we have  $\text{lp}(f')|\text{lp}(f)$  and  $\text{lp}(g')|\text{lp}(g)$ . This is a contradiction, as  $\text{lp}(f') \prec \text{lp}(f)$  and  $\text{lp}(g') \prec \text{lp}(g)$  and so  $\text{lp}(f'g) \neq \text{lp}(g'f)$ . Thus, without loss of generality, we assume that  $\text{lp}(f'g) \succ \text{lp}(g'f)$ . This means that  $\text{lt}(f'g - g'f) = \text{lt}(f'g)$  and so  $\text{lp}(f'g - g'f)$  is divisible by  $\text{lp}(g)$ . Since  $\text{lt}(g) = bY$  we have  $\text{lt}(f'g - g'f) = \text{blt}(f')Y$ .

Thus we can write

$$\begin{aligned} f'g - g'f &= f'g - \text{lt}(f')g + \text{lt}(f')g - g'f \\ &= ((f' - \text{lt}(f'))g - g'f) + \text{lt}(f')g \\ &= ((f' - \text{lt}(f'))g - g'f) + \frac{\text{blt}(f')Y}{bY}g \\ &= ((f' - \text{lt}(f'))g - g'f) + \frac{\text{lt}(f'g - g'f)}{\text{lt}(g)}g. \end{aligned}$$

Multiplying both sides by  $\frac{1}{ab}$  and rearranging, we have

$$\frac{1}{ab}(f'g - g'f) - \frac{1}{ab} \frac{\text{lt}(f'g - g'f)}{\text{lt}(g)}g = \frac{1}{ab}((f' - \text{lt}(f'))g - g'f).$$

Using Definition 3.1.2 we then have:

$$S(f, g) = \frac{1}{ab}(f'g - g'f) \xrightarrow{g} \frac{1}{ab}((f' - \text{lt}(f'))g - g'f).$$

The polynomial  $\frac{1}{ab}((f' - \text{lt}(f'))g - g'f)$  can be treated the same way: Using the fact that  $\gcd(\text{lp}(f), \text{lp}(g)) = 1$ , we must have  $\text{lp}((f' - \text{lt}(f'))g) \neq \text{lp}(g'f)$ , and so  $\text{lp}((f' - \text{lt}(f'))g - g'f)$  is divisible by either  $\text{lp}(g)$  or  $\text{lp}(f)$ . Thus  $\frac{1}{ab}((f' - \text{lt}(f'))g - g'f)$  can be reduced modulo  $\{f, g\}$  and another term from either  $(f' - \text{lt}(f'))g$  or  $f'g'$  is cancelled. We can continue in this fashion until all terms have been removed and obtain:

$$S(f, g) \xrightarrow{+\{f, g\}} 0$$

and so by Lemma 4.2.6,  $\{f, g\}$  is a Gröbner basis.  $\square$

Now we come to the main result of the section.

LEMMA 5.1.4. [1, Lemma 3.3.1]. *Let  $f, g \in k[x_1, \dots, x_n]$ , non-zero, and let  $d := \gcd(f, g)$ . The following statements are equivalent:*

- (i)  $S(f, g) \xrightarrow{+\{f, g\}} 0$ .
- (ii)  $\text{lp}(\frac{f}{d})$  and  $\text{lp}(\frac{g}{d})$  are relatively prime.

PROOF. (i) $\implies$ (ii). Assume that  $S(f, g) \xrightarrow{+\{f, g\}} 0$ . By Lemma 5.1.1 we have that  $S(\frac{f}{d}, \frac{g}{d}) \xrightarrow{+\{\frac{f}{d}, \frac{g}{d}\}} 0$ . Since  $\gcd(\frac{f}{d}, \frac{g}{d}) = 1$ , Lemma 5.1.3 immediately gives the result.

(ii) $\implies$ (i). Assume that  $\text{lp}(\frac{f}{d})$  and  $\text{lp}(\frac{g}{d})$  are relatively prime. Thus  $\gcd(\frac{f}{d}, \frac{g}{d}) = 1$  and so we can use Lemma 5.1.3. Thus  $\{\frac{f}{d}, \frac{g}{d}\}$  is a Gröbner basis by Theorem 4.2.6 and by Lemma 4.1.7  $\{f, g\}$  is also a Gröbner basis. Theorem 4.2.6 immediately gives that  $S(f, g) \xrightarrow{+\{f, g\}} 0$ .  $\square$

The above result gives us a relatively easy to check criterion for determining when an  $S$ -polynomial is going to reduce to zero. During Buchberger's Algorithm, if we are computing a Gröbner basis for a set  $G = \{f_1, \dots, f_t\}$ , before we reduce one of the  $S$ -polynomials, say  $S(f_i, f_j)$ , we can check if Lemma 5.1.4 holds which will then tell us that  $S(f_i, f_j) \xrightarrow{+\{f_i, f_j\}} 0$ . Clearly then, since  $f_i, f_j \in G$ , we also have  $S(f_i, f_j) \xrightarrow{+G} 0$ . This is implemented into Algorithm 5.4.3 as a sub-algorithm (Algorithm 5.4.1).

## 5.2. Modules and Syzygies

This section reframes our algebraic definitions in the form of modules, with some results (like Theorem 4.2.6) being proved again in this new form.

DEFINITION 5.2.1. Let  $s \in \mathbb{N}$ . For a commutative ring  $R$  we interpret  $R^s$  as a  $R$ -bimodule.

We also define some new notation that will be used extensively in this section.

DEFINITION 5.2.2. Let  $s \in \mathbb{N}$  and let  $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ . Note that the second and third definitions below depend on the polynomials  $f_1, \dots, f_s$ .

- We denote with  $e_1, \dots, e_s$  the standard basis for the  $k[x_1, \dots, x_n]$ -bimodule  $k[x_1, \dots, x_n]^s$ .
- We define, for distinct  $i, j, k \in \{1, \dots, s\}$ :

$$X(f_i) = \text{lp}(f_i)$$

and

$$X(f_i, f_j) := \text{lcm}(\text{lp}(f_i), \text{lp}(f_j))$$

and

$$X(f_i, f_j, f_k) := \text{lcm}(\text{lp}(f_i), \text{lp}(f_j), \text{lp}(f_k)).$$

When the polynomial arguments are clear from context, we omit them and simply write  $X_i$ ,  $X_{ij}$  and  $X_{ijk}$ .

- We define, for distinct  $i, j \in \{1, \dots, s\}$ ,  $\tau(f_i, f_j) := \frac{X_{ij}}{c_i X_i} e_i - \frac{X_{ij}}{c_j X_j} e_j \in k[x_1, \dots, x_n]^s$ , where  $c_i X_i = \text{lt}(f_i)$  and  $c_j X_j = \text{lt}(f_j)$ . Again, when the context is clear, we omit the polynomial arguments and write  $\tau_{ij}$ .

REMARK 5.2.3. The  $\tau_{ij}$  defined above is the module equivalent of the  $S$ -polynomial from Chapter 4. Indeed, we can see that for  $(f_1, \dots, f_s) \in k[x_1, \dots, x_n]^s$  we have  $\tau_{ij} \cdot (f_1, \dots, f_s) = S(f_i, f_j)$ .

We now define a map, the kernel of which is an essential part of the theory used to develop the second criterion.

DEFINITION 5.2.4. Let  $s \in \mathbb{N}$ ,  $f_1, \dots, f_s \in k[x_1, \dots, x_n]$  and let  $\langle f_1, \dots, f_s \rangle = I \subseteq k[x_1, \dots, x_n]$  be the ideal generated by  $f_1, \dots, f_s$ . Consider the  $k[x_1, \dots, x_n]$ -bimodule homomorphism  $\phi_I : k[x_1, \dots, x_n]^s \rightarrow I$  defined by:

$$(h_1, \dots, h_s) \mapsto \sum_{i=1}^s h_i f_i \quad (h_1, \dots, h_s) \in k[x_1, \dots, x_n]^s.$$

We call  $\ker(\phi_I)$  the *syzygy module* of the  $1 \times s$  matrix  $[f_1 \ \dots \ f_s]$ , denoted  $\text{Syz}(f_1, \dots, f_s)$ . An element  $(h_1, \dots, h_s)$  of  $\text{Syz}(f_1, \dots, f_s)$  is called a *syzygy*.

The following lemma seems arbitrary but is particularly useful in the result that follows. We are working towards being able to express syzygies in terms of the  $\tau_{ij}$  elements defined in Definition 5.2.2.

LEMMA 5.2.5. Let  $n \in \mathbb{N}$ , let  $c_1, \dots, c_s \in k \setminus \{0\}$  and let  $X_1, \dots, X_s \in P_n$  be power products in  $k[x_1, \dots, x_n]$ . Let  $X \in P_n$  be arbitrary. Define  $A_X := \{(d_1 Y_1, \dots, d_s Y_s) \in k[x_1, \dots, x_n]^s \mid (Y_i X_i = X \text{ and } d_i = c_i) \text{ or } d_i = 0 \text{ and } Y_i \in P_n \text{ for each } i \in \{1, \dots, s\}\}$ . Then any element  $(h_1, \dots, h_s) \in k[x_1, \dots, x_n]^s$  can be written as a sum of elements in  $\bigcup_{X \in P_n} A_X$ .

PROOF. Let  $(h_1, \dots, h_s) \in k[x_1, \dots, x_n]^s$ , not all zero, be arbitrary. Consider the polynomials

$$c_1 X_1 h_1, \dots, c_s X_s h_s.$$

Only finitely many unique power products can appear with non-zero coefficients in these polynomials. We denote them as  $Z_1, \dots, Z_t$ . Thus for each  $i \in \{1, \dots, s\}$  and  $j \in \{1, \dots, t\}$  there exist  $a_{ij} \in k$  not all zero such that  $c_i h_i X_i = \sum_{j=1}^t a_{ij} Z_j$ . Define  $S_i := \{j \in \{1, \dots, t\} \mid a_{ij} \neq 0\}$  and define

$$Y_{ij} := \begin{cases} \frac{Z_j}{X_i} & \text{if } j \in S_i \\ 0 & \text{if } j \notin S_i. \end{cases}$$

$Y_{ij}$  is well defined: Since each  $Z_j$  for which  $a_{ij} \neq 0$  is equal to some product from  $h_i$  multiplied by  $X_i$ , we always have  $Z_j \mid X_i$  for  $j \in S_i$ . Thus we can write

$$c_i X_i h_i = \sum_{j \in S_i} a_{ij} Z_j$$

and hence

$$h_i = \sum_{j=1}^t \frac{a_{ij}}{c_i} Y_{ij}$$



and thus

$$(h_1, \dots, h_s) = \left( \sum_{j=1}^t \frac{a_{1j}}{c_1} Y_{1j}, \dots, \sum_{j=1}^t \frac{a_{sj}}{c_s} Y_{sj} \right) = \sum_{j=1}^t \left( \frac{a_{1j}}{c_1} Y_{1j}, \dots, \frac{a_{sj}}{c_s} Y_{sj} \right).$$

We can see that for each  $j \in \{1, \dots, t\}$  we have that  $(\frac{a_{1j}}{c_1} Y_{1j}, \dots, \frac{a_{sj}}{c_s} Y_{sj})$  has the required property: Either  $a_{ij} = 0$  or  $Y_{ij} X_i = Z_j$  for each  $i \in \{1, \dots, s\}$ .  $\square$

DEFINITION 5.2.6. Let  $s, n \in \mathbb{N}$ , let  $X_1, \dots, X_s \in P_n$  and let  $c_1, \dots, c_s \in k \setminus \{0\}$ . Then, for a product  $X \in P_n$  we call a syzygy  $(h_1, \dots, h_s) \in \text{Syz}(c_1 X_1, \dots, c_s X_s)$  *homogeneous of degree  $X$*  if, for each  $i \in \{1, \dots, s\}$  there exist  $a_i \in k$  and  $Y_i \in P_n$  such that  $h_i = a_i Y_i$  and  $X_i Y_i = X$ . If, for a power product  $X \in P_n$ , a syzygy  $(h_1, \dots, h_s) \in \text{Syz}(c_1 X_1, \dots, c_s X_s)$  is homogeneous of degree  $X$  then we say  $(h_1, \dots, h_s)$  is *homogeneous*.

The next result allows us to precisely describe a generating set for a syzygy module of terms.

PROPOSITION 5.2.7. [1, Proposition 3.2.3]. *Let  $n, s \in \mathbb{N}$ , and let  $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ . Then, using the notation of Definition 5.2.2,  $\text{Syz}(\text{lt}(f_1), \dots, \text{lt}(f_s))$  is generated, as a  $k[x_1, \dots, x_n]$ -bimodule, by*

$$\{\tau_{ij} \in k[x_1, \dots, x_n]^s \mid 1 \leq i < j \leq s\}$$

and the syzygies in this set are homogeneous.

PROOF. There exist  $c_1, \dots, c_s \in k \setminus \{0\}$  and  $X_1, \dots, X_s \in P_n$  such that  $\text{lt}(f_i) = c_i X_i$  for each  $i \in \{1, \dots, s\}$ . Then  $\text{Syz}(\text{lt}(f_1), \dots, \text{lt}(f_s)) = \text{Syz}(c_1 X_1, \dots, c_s X_s)$ . Note that for distinct  $i, j \in \{1, \dots, s\}$  we have

$$\begin{aligned} (c_1 X_1, \dots, c_s X_s) \cdot \left( \frac{X_{ij}}{c_i X_i} e_i - \frac{X_{ij}}{c_j X_j} e_j \right) &= (c_1 X_1, \dots, c_s X_s) \cdot \left( 0, \dots, \underset{i^{\text{th co-ord}}}{\frac{X_{ij}}{c_i X_i}}, 0, \dots, 0, -\underset{j^{\text{th co-ord}}}{\frac{X_{ij}}{c_j X_j}}, 0, \dots, 0 \right) \\ &= c_i X_i \left( \frac{X_{ij}}{c_i X_i} \right) - c_j X_j \left( \frac{X_{ij}}{c_j X_j} \right) \\ &= X_{ij} - X_{ij} \\ &= 0 \end{aligned}$$

(this precisely reflects Remark 4.2.2) and so

$$\tau_{ij} \in \text{Syz}(c_1 X_1, \dots, c_s X_s).$$

We denote the submodule of  $\text{Syz}(c_1 X_1, \dots, c_s X_s)$  generated by the set  $\{\tau_{ij} \mid 1 \leq i < j \leq s\}$  as

$$\langle \tau_{ij} \mid 1 \leq i < j \leq s \rangle.$$

We have thus shown that

$$\langle \tau_{ij} \mid 1 \leq i < j \leq s \rangle \subseteq \text{Syz}(c_1 X_1, \dots, c_s X_s).$$

For the reverse inclusion, we let  $(h_1, \dots, h_s) \in \text{Syz}(c_1 X_1, \dots, c_s X_s)$ . From Lemma 5.2.5 we can write  $(h_1, \dots, h_s)$  as a sum of elements of  $\bigcup_{X \in P_n} A_X$ , where  $A_X$  is defined as in Lemma 5.2.5. Hence  $(h_1, \dots, h_s) = \sum_{X \in P_n} (d_1^{(X)} Y_1^{(X)}, \dots, d_s^{(X)} Y_s^{(X)})$ . This sum is well defined, since, as shown in Lemma 5.2.5, the  $d_i^{(X)}$  correspond to one of the finitely many products that appear in  $(X_1 h_1, \dots, X_s h_s)$

and so only finitely many of the  $(d_1^{(X)}, \dots, d_s^{(X)})$  are non-zero. Since  $(h_1, \dots, h_s) \in \text{Syz}(c_1 X_1, \dots, c_s X_s)$  we have

$$\begin{aligned}
 0 &= (h_1, \dots, h_s) \cdot (c_1 X_1, \dots, c_s X_s) \\
 &= \sum_{X \in P_n} (d_1^{(X)} Y_1^{(X)}, \dots, d_s^{(X)} Y_s^{(X)}) \cdot (c_1 X_1, \dots, c_s X_s) \\
 &= \sum_{X \in P_n} \sum_{j=1}^s d_j^{(X)} c_j (Y_j^{(X)} X_j) \\
 &= \sum_{X \in P_n} \left[ \sum_{j=1}^s d_j^{(X)} c_j \right] X \text{ (because } Y_j^{(X)} X_j = X \text{ as per Lemma 5.2.5)}.
 \end{aligned}$$

Thus for every  $X \in P_n$  we have

$$\sum_{j=1}^s d_j^{(X)} c_j = 0$$

and, recalling again that  $Y_i^{(X)} X_i = X$ ,

$$\begin{aligned}
 (d_1^{(X)} Y_1^{(X)}, \dots, d_s^{(X)} Y_s^{(X)}) &= d_1^{(X)} Y_1^{(X)} e_1 + \dots + d_s^{(X)} Y_s^{(X)} e_s \\
 &= d_1^{(X)} c_1 \frac{X}{c_1 X_1} e_1 + \dots + d_s^{(X)} c_s \frac{X}{c_s X_s} e_s \\
 &= d_1^{(X)} c_1 \frac{X}{X_{12}} \left( \frac{X_{12}}{c_1 X_1} e_1 - \frac{X_{12}}{c_2 X_2} e_2 \right) \\
 &\quad + (d_1^{(X)} c_1 + d_2^{(X)} c_2) \frac{X}{X_{23}} \left( \frac{X_{23}}{c_2 X_2} e_2 - \frac{X_{23}}{c_3 X_3} e_3 \right) + \dots \\
 &\quad + (d_1^{(X)} c_1 + \dots + d_{s-1}^{(X)} c_{s-1}) \frac{X}{X_{(s-1)s}} \left( \frac{X_{(s-1)s}}{c_{s-1} X_{s-1}} e_{s-1} - \frac{X_{(s-1)s}}{c_s X_s} e_s \right) \\
 &\quad + \underbrace{(d_1^{(X)} c_1 + \dots + d_s^{(X)} c_s)}_{=0} \frac{X_{(s-1)s}}{c_s X_s} e_s \\
 &= \sum_{j=2}^s \left[ \sum_{i=1}^{j-1} d_i^{(X)} c_i \right] \left[ \frac{X}{X_{(j-1)j}} \right] \tau_{(j-1)j} \\
 &= \sum_{j=2}^s g_j \tau_{(j-1)j} \text{ where } g_j = \sum_{i=1}^{j-1} d_i^{(X)} c_i \left[ \frac{X}{X_{(j-1)j}} \right]
 \end{aligned}$$

Thus for each  $X \in P_n$ , we can write  $(d_1^{(X)} Y_1^{(X)}, \dots, d_s^{(X)} Y_s^{(X)})$  as a linear combination of elements of  $\{\tau_{ij} | 1 \leq i < j \leq s\}$  and hence, as  $(h_1, \dots, h_s) = \sum_{X \in P_n} (d_1^{(X)} Y_1^{(X)}, \dots, d_s^{(X)} Y_s^{(X)})$  we have that  $(h_1, \dots, h_s)$  is also a linear combination of elements of  $\{\tau_{ij} | 1 \leq i < j \leq s\}$ , i.e.  $(h_1, \dots, h_s) \in \langle \tau_{ij} | 1 \leq i < j \leq s \rangle$  and we are done.  $\square$

The following theorem is the most important result of this section. It is effectively the module equivalent of Buchberger's Theorem (Theorem 4.2.6). We know how to find a generating set for a syzygy module of terms and when these terms are the leading terms of a set of polynomials, the theorem below gives us a property that the syzygies in the generating set must have in order for the set of polynomials to be a Gröbner basis.

**THEOREM 5.2.8.** [1, Theorem 3.2.5]. *Let  $s \in \mathbb{N}$  and let  $G = \{g_1, \dots, g_s\}$  be a set of non-zero polynomials in  $k[x_1, \dots, x_n]$ . Let  $\mathcal{B} \subseteq k[x_1, \dots, x_n]^s$  be a finite set of homogeneous syzygies that generate  $\text{Syz}(\text{lt}(g_1), \dots, \text{lt}(g_s))$ . Then  $G$  is a Gröbner basis for the ideal  $\langle g_1, \dots, g_s \rangle$  if and only if for each  $(b_1, \dots, b_s) \in \mathcal{B}$  we have*

$$b_1 g_1 + \dots + b_s g_s \xrightarrow{G} + 0.$$

PROOF. Assume that  $G$  is a Gröbner basis. From Theorem 4.1.2 and the fact that for any  $(b_1, \dots, b_s) \in \mathcal{B}$  we have  $b_1g_1 + \dots + b_sg_s \in \langle g_1, \dots, g_s \rangle$ , we get  $b_1g_1 + \dots + b_sg_s \xrightarrow{G} 0$ .

Conversely, assume that, for each  $(b_1, \dots, b_s) \in \mathcal{B}$ , we have  $b_1g_1 + \dots + b_sg_s \xrightarrow{G} 0$ . Let  $g \in \langle g_1, \dots, g_s \rangle$  be arbitrary. We aim to use Theorem 4.1.2 (iii), and so for some  $u_1, \dots, u_s \in k[x_1, \dots, x_n]$  we let  $g = u_1g_1 + \dots + u_sg_s$  be a representation of  $g$  such that

$$X = \max_{1 \leq i \leq s} (\text{lp}(u_i)\text{lp}(g_i))$$

is a minimum with respect to  $\prec$ . With a view to a contradiction, suppose that  $\text{lp}(g) \prec X$ . Let  $S := \{i \in \{1, \dots, s\} \mid \text{lp}(u_i)\text{lp}(g_i) = X\}$ . Since the leading product of  $g$  is less than  $X$  it must be the case that the coefficient of  $X$  in  $g$  is zero. We thus have:

$$\sum_{i \in S} \text{lt}(u_i)\text{lt}(g_i) = 0.$$

We define  $h_S := \sum_{i \in S} \text{lt}(u_i)e_i$ . We immediately have that  $h_S \in \text{Syz}(\text{lt}(g_1), \dots, \text{lt}(g_s))$  and  $h_S$  is homogeneous of degree  $X$ . We label the elements of  $\mathcal{B}$  as  $\{(b_{11}, \dots, b_{s1}), \dots, (b_{1l}, \dots, b_{sl})\}$ . Since  $\mathcal{B}$  generates  $\text{Syz}(\text{lt}(g_1), \dots, \text{lt}(g_t))$  we have, for some  $a_1, \dots, a_l \in k[x_1, \dots, x_n]$ :

$$h_S = \sum_{i=1}^l a_i(b_{1i}, \dots, b_{si}).$$

Because  $h_S$  is a homogeneous syzygy, we can assume that each  $a_1, \dots, a_l$  is a term such that, for each  $i \in \{1, \dots, l\}$  and each  $j \in \{1, \dots, s\}$ ,  $\text{lp}(a_i)\text{lp}(b_{ji})\text{lp}(g_j) = X$  whenever  $a_ib_{ji} \neq 0$ . Fix an  $i \in \{1, \dots, l\}$ . By assumption we have:

$$\sum_{j=1}^s b_{ji}g_j \xrightarrow{G} 0.$$

Thus by Theorem 3.1.7 there exist  $u_{1i}, \dots, u_{si} \in k[x_1, \dots, x_n]$  such that:

$$\sum_{j=1}^s b_{ji}g_j = \sum_{j=1}^s u_{ji}g_j$$

and  $\text{lp}(\sum_{j=1}^s b_{ji}g_j) = \max_{1 \leq j \leq s} \text{lp}(u_{ji})\text{lp}(g_j)$ . However, since  $(b_{1i}, \dots, b_{si}) \in \text{Syz}(\text{lt}(g_1), \dots, \text{lt}(g_s))$  we have  $\sum_{j=1}^s b_{ji}\text{lt}(g_j) = 0$  so the lead term of  $\sum_{j=1}^s b_{ji}g_j$  is cancelled, thus:

$$\max_{1 \leq j \leq s} \text{lp}(u_{ji})\text{lp}(g_j) = \text{lp}\left(\sum_{j=1}^s b_{ji}g_j\right) \prec \max_{1 \leq j \leq s} (\text{lp}(b_{ji})\text{lp}(g_j)).$$

Thus we write

$$\begin{aligned}
 g &= \sum_{i=1}^s u_i g_i \\
 &= \sum_{i \in S} u_i g_i + \sum_{i \notin S} u_i g_i \\
 &= \sum_{i \in S} \text{lt}(u_i) g_i + \underbrace{\sum_{i \in S} (\text{lower terms of } u_i) g_i + \sum_{i \notin S} u_i g_i}_{\text{products lower than } X} \\
 &= h_S \cdot (g_1, \dots, g_s) + \sum_{i \in S} (\text{lower terms of } u_i) g_i + \sum_{i \notin S} u_i g_i \\
 &= \sum_{i=1}^l \sum_{j=1}^s a_i b_{ji} g_j + \sum_{i \in S} (\text{lower terms of } u_i) g_i + \sum_{i \notin S} u_i g_i \\
 &= \sum_{i=1}^l \sum_{j=1}^s a_i u_{ji} g_j + \sum_{i \in S} (\text{lower terms of } u_i) g_i + \sum_{i \notin S} u_i g_i.
 \end{aligned}$$

We now have that all terms in last line have maximum lead product less than  $X$ , because

$$\max_{i,j} \text{lp}(a_i) \text{lp}(u_{ji}) \text{lp}(g_j) \prec \max_{i,j} \text{lp}(a_i) \text{lp}(b_{ji}) \text{lp}(g_j) = X,$$

and so we have a representation for  $g$  as a linear combination of  $g_1, \dots, g_s$  that contradicts the minimality of  $X$ . Therefore the assumption that  $\text{lp}(g) \prec X$  was false and so  $\text{lp}(g) = X$ . Since  $g$  was chosen arbitrarily we have, by Theorem 4.1.2(iii), that  $\{g_1, \dots, g_s\}$  is a Gröbner basis.  $\square$

To sum up, this result tells us that a set  $G := \{g_1, \dots, g_s\} \subseteq k[x_1, \dots, x_n]$  is a Gröbner basis when  $\text{Syz}(\text{lt}(g_1), \dots, \text{lt}(g_s))$  has a generating set  $\mathcal{B}$  which has the property that for any  $b \in \mathcal{B}$  we have  $b \cdot (g_1, \dots, g_s) \xrightarrow{G}_+ 0$ . Proposition 5.2.7 tells us that one of these generating sets is  $\{\tau_{ij} \mid 1 \leq i < j \leq s\}$ , and by Remark 5.2.3 we can now see that for  $\tau_{ij} \in \mathcal{B}$  for some  $i < j \in \{1, \dots, s\}$  we have  $\tau_{ij} \cdot (g_1, \dots, g_s) = S(g_i, g_j) \xrightarrow{G}_+ 0$ . As a corollary we have recovered Buchberger's Theorem (Theorem 4.2.6), this time in terms of modules.

**COROLLARY 5.2.9.** (*Buchberger's Theorem for modules*) [1, Corollary 3.2.6]. *Let  $G = \{g_1, \dots, g_t\}$  be a set of non-zero polynomials in  $k[x_1, \dots, x_n]$ . Then  $G$  is a Gröbner basis if and only if for all  $i \neq j \in \{1, \dots, t\}$  we have that  $S(g_i, g_j) \xrightarrow{G}_+ 0$ .*

**PROOF.** Assume that  $G$  is a Gröbner basis. We have  $S(g_i, g_j) \in \langle g_1, \dots, g_t \rangle$  and so by Theorem 4.1.2,  $S(g_i, g_j) \xrightarrow{G}_+ 0$ .

Conversely, assume that for each  $i \neq j \in \{1, \dots, t\}$  we have  $S(g_i, g_j) \xrightarrow{G}_+ 0$ . Using Proposition 5.2.7 we have that

$$\mathcal{B} = \{\tau_{ij} \mid 1 \leq i < j \leq t\} \subseteq k[x_1, \dots, x_n]^t$$

is a homogeneous generating set for  $\text{Syz}(\text{lt}(g_1), \dots, \text{lt}(g_t))$ . Each element of  $\mathcal{B}$  gives rise to an  $S$ -polynomial:

$$\begin{aligned} \tau_{ij} \cdot (g_1, \dots, g_t) &= \left(0, \dots, \frac{X_{ij}}{\text{lt}(g_i)}, 0, \dots, -\frac{X_{ij}}{\text{lt}(g_j)}, \dots, 0\right) \cdot (g_1, \dots, g_t) \\ &= \frac{X_{ij}}{\text{lt}(g_i)} g_i - \frac{X_{ij}}{\text{lt}(g_j)} g_j \\ &= S(g_i, g_j) \end{aligned}$$

and we have assumed these reduce to zero modulo  $G$ . Thus, by Theorem 5.2.8,  $G$  is a Gröbner basis  $\square$

### 5.3. The second new criterion

In the previous section we developed a new equivalent condition for a Gröbner basis in terms of syzygies. This is what will form the basis of our second new criterion.

LEMMA 5.3.1. [1, Lemma 3.3.2]. *Let  $n, s \in \mathbb{N}$ , let  $X_1, \dots, X_s \in P_n$  and let  $c_1, \dots, c_s \in k \setminus \{0\}$ . Using the notation of Definition 5.2.2, for polynomials  $f_i = c_i X_i$  and each distinct  $i, j, l \in \{1, \dots, s\}$  we have*

$$\frac{X_{ijl}}{X_{ij}} \tau_{ij} + \frac{X_{ijl}}{X_{jl}} \tau_{jl} + \frac{X_{ijl}}{X_{li}} \tau_{li} = 0.$$

Furthermore, if  $X_l$  divides  $X_{ij}$ , then  $\tau_{ij}$  is in the submodule of  $k[x_1, \dots, x_n]^s$  generated by  $\tau_{jl}$  and  $\tau_{li}$ .

PROOF. We have

$$\begin{aligned} \frac{X_{ijl}}{X_{ij}} \tau_{ij} + \frac{X_{ijl}}{X_{jl}} \tau_{jl} + \frac{X_{ijl}}{X_{li}} \tau_{li} &= \frac{X_{ijl}}{X_{ij}} \left( \frac{X_{ij}}{c_i X_i} e_i - \frac{X_{ij}}{c_j X_j} e_j \right) + \frac{X_{ijl}}{X_{jl}} \left( \frac{X_{jl}}{c_j X_j} e_j - \frac{X_{jl}}{c_l X_l} e_l \right) \\ &\quad + \frac{X_{ijl}}{X_{li}} \left( \frac{X_{li}}{c_l X_l} e_l - \frac{X_{li}}{c_i X_i} e_i \right) \\ &= \frac{X_{ijl}}{c_i X_i} e_i - \frac{X_{ijl}}{c_j X_j} e_j + \frac{X_{ijl}}{c_j X_j} e_j - \frac{X_{ijl}}{c_l X_l} e_l + \frac{X_{ijl}}{c_l X_l} e_l - \frac{X_{ijl}}{c_i X_i} e_i \\ &= 0. \end{aligned}$$

Now, if  $X_{ij} | X_l$  then  $X_{ijl} = X_{ij}$  and so

$$\tau_{ij} + \frac{X_{ijl}}{X_{jl}} \tau_{jl} + \frac{X_{ijl}}{X_{li}} \tau_{li} = 0$$

meaning that  $\tau_{ij}$  is in the submodule of  $k[x_1, \dots, x_n]^s$  generated by  $\tau_{jl}$  and  $\tau_{li}$ .  $\square$

COROLLARY 5.3.2. [1, Corollary 3.3.3] *Using the notation of Definition 5.2.2. Let  $n, s \in \mathbb{N}$ , let  $c_1, \dots, c_s \in k$  and let  $X_1, \dots, X_s \in P_n$ . Let  $\mathcal{B} \subseteq \{\tau_{ij} | 1 \leq i < j \leq s\}$  be a generating set for  $\text{Syz}(c_1 X_1, \dots, c_s X_s)$ . With  $f_i = c_i X_i$  for each  $i \in \{1, \dots, s\}$ , suppose we have three distinct indices  $i, j, l$  such that  $\tau_{ij}, \tau_{jl}, \tau_{li} \in \mathcal{B}$ , and such that  $X_l$  divides  $X_{ij}$ . Then  $\mathcal{B} \setminus \{\tau_{ij}\}$  is also a generating set for  $\text{Syz}(c_1 X_1, \dots, c_s X_s)$ .*

What we have here in Corollary 5.3.2 is a condition that lets us make a generating set for a syzygy module smaller, while still keeping it a generating set for that syzygy module. This is the second criterion we use to improve Algorithm 4.2.7.

### 5.4. Improving Buchberger's Algorithm

Lemma 5.3.1 and Corollary 5.3.2 give us two criteria that let us avoid having to compute and reduce redundant  $S$ -polynomials, as we know they will reduce to zero. We now detail how they will be used to improve Buchberger's Algorithm.

The first criterion, referred to as *crit1* (Algorithm 5.4.1) below, is easy to implement. During Buchberger's Algorithm, before we reduce an  $S$ -polynomial, we first check whether the lead products of the two polynomial arguments are disjoint and, if they are, we needn't reduce their  $S$ -polynomial, saving us from performing a lengthy calculation.

The second criterion, *crit2* (Algorithm 5.4.2), is a little bit trickier to implement. We keep track of all pairs of polynomials for which we have not yet computed the associated  $S$ -polynomial in a list  $\mathcal{NC}$ . We would like to, during Buchberger's Algorithm, remove as many pairs of polynomials from  $\mathcal{NC}$  as we can before computing and reducing their  $S$ -polynomials. From one iteration of the while loop in Buchberger's Algorithm (Algorithm 4.2.7) to the next, a new polynomial might be added to the basis and all the corresponding pairs are also added to  $\mathcal{NC}$ . Before we iterate through the loop again, we use Corollary 5.3.2 to remove all the pairs from  $\mathcal{NC}$  we can. We can do this because Corollary 5.3.2 tells us that we will still have a generating set for the syzygy module of lead terms of our polynomials if we remove the pairs that meet the condition of Corollary 5.3.2. So the  $S$ -polynomials of the pairs that are removed are never reduced and we are saved from, possibly, a very large amount of costly reduction computations.

These two criteria together save us a lot of computation time because it is quicker to check these various divisibility and disjointness conditions than it is to reduce polynomials modulo other polynomials. We now give the improved version of Buchberger's Algorithm, and *crit1* and *crit2*.

ALGORITHM 5.4.1. [1, p. 128]. *crit1*.

Input: Two polynomials  $f, g \in k[x_1, \dots, x_n]$

Output: True or False

Implementation:

If  $\gcd(\text{lp}(f), \text{lp}(g)) = 1$ :

    Return True

Else:

    Return False

ALGORITHM 5.4.2. [1, Algorithm 3.3.2]. *crit2*.

(Using the notation of Definition 5.2.2)

Input:  $\mathcal{NC}$  and  $\mathcal{C}$  from Algorithm 5.4.3

Output:  $\mathcal{NC}$  with some elements removed

Implementation:

For all distinct indices  $i < j < k$  that appear in  $\mathcal{NC} \cup \mathcal{C}$ :

    If  $\text{lcm}(X_i, X_j) \mid X_k$  and  $(f_i, f_j) \in \mathcal{NC}$ :

$\mathcal{NC} = \mathcal{NC} \setminus \{(f_i, f_j)\}$

If  $\text{lcm}(X_i, X_k) | X_j$  and  $(f_i, f_k) \in \mathcal{NC}$ :  
 $\mathcal{NC} = \mathcal{NC} \setminus \{(f_i, f_k)\}$   
 If  $\text{lcm}(X_j, X_k) | X_i$  and  $(f_j, f_k) \in \mathcal{NC}$ :  
 $\mathcal{NC} = \mathcal{NC} \setminus \{(f_j, f_k)\}$   
 Return  $\mathcal{NC}$

ALGORITHM 5.4.3. [1, Algorithm 3.3.1] *Improved Buchberger Algorithm*  
 (Using the notation of Definition 5.2.2)

Input:  $F = \{f_1, \dots, f_s\}$  a list of non-zero polynomials in  $k[x_1, \dots, x_n]$

Output:  $G$ , a Gröbner basis for  $\langle F \rangle$ .

Initialisation:

$G := F$   
 $\mathcal{NC} := \{\tau_{ij} \mid 1 \leq i < j \leq s\}$   
 $\mathcal{C} := \emptyset$   
 $t := s$

Implementation:

$\mathcal{NC} := \text{crit2}(\mathcal{NC}, \mathcal{C})$

While  $\mathcal{NC} \neq \emptyset$ :

Choose a pair  $(f_i, f_j) \in \mathcal{NC}$   
 $\mathcal{NC} := \mathcal{NC} \setminus \{(f_i, f_j)\}$   
 $\mathcal{C} := \mathcal{C} \cup \{(f_i, f_j)\}$

If  $\text{crit1}(f_i, f_j) = \text{False}$ :

Compute remainder  $S(f_i, f_j) \xrightarrow{G}_+ h$

If  $h \neq 0$ :

Add new pairs  $\{(u, h) \mid \text{for all } u \in G\}$  to  $\mathcal{NC}$   
 Add  $h$  to  $G$   
 $\mathcal{NC} := \text{crit2}(\mathcal{NC}, \mathcal{C})$

Return  $G$

PROPOSITION 5.4.4. [1, Proposition 3.3.4]. *Given a set of non-zero polynomials  $F = \{f_1, \dots, f_s\}$ , Algorithm 5.4.3 terminates and produces a Gröbner basis for the ideal  $I = \langle f_1, \dots, f_s \rangle$ .*

PROOF. Let  $G = \{f_1, \dots, f_t\}$  ( $t \geq s$ ) be the output of the algorithm. We note that upon termination all the  $S$ -polynomials of the pairs of polynomials in  $\mathcal{C}$  will necessarily reduce to 0 modulo  $G$ . This is because the remainder of each  $S$ -polynomial modulo  $G$  is computed and if it is not 0 that remainder is added to  $G$ . The  $S$ -polynomial then trivially reduces to 0 modulo this updated  $G$ . Also note that  $\mathcal{C} \subsetneq \{(f_i, f_j) \mid 1 \leq i < j \leq t\}$  because the  $\text{crit2}$  algorithm removes some of these pairs from  $\mathcal{NC}$  before they have a chance to be chosen, reduced and added to  $\mathcal{C}$ .

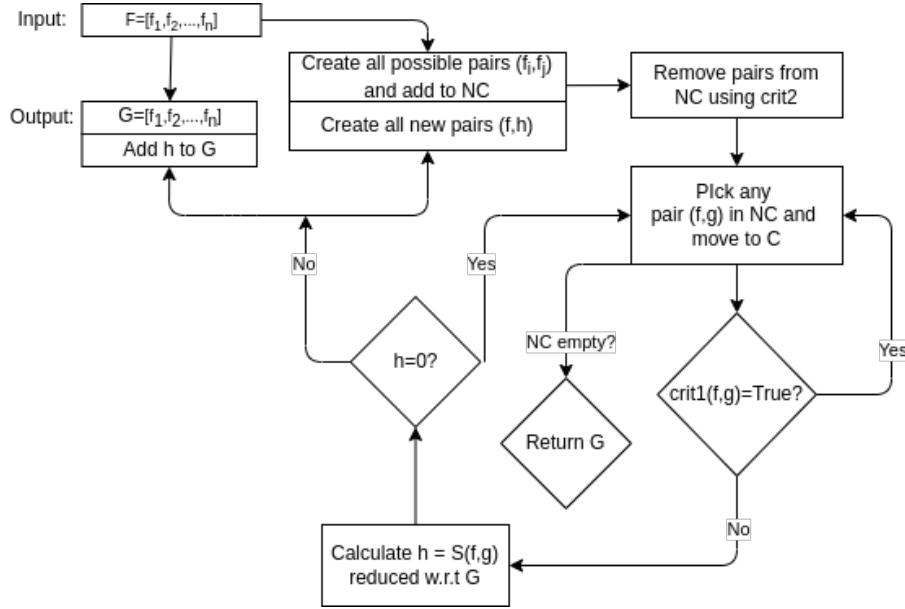


FIGURE 5.4.1. A flow diagram for Algorithm 5.4.3

Thus, if we show that the set  $\{\tau_{ij} \mid (f_i, f_j) \in \mathcal{C}\}$  is a generating set for  $\text{Syz}(\text{lt}(f_1), \dots, \text{lt}(f_t))$  then we will have that  $G$  is a Gröbner basis for  $I$ . For this, it suffices to show that at any stage of the algorithm,  $\{\tau_{ij} \mid (f_i, f_j) \in \mathcal{NC} \cup \mathcal{C}\}$  is a generating set for the syzygy module of the lead terms of the polynomials in the current value of  $G$ .

Upon initialisation, we have  $\{\tau_{ij} \mid (f_i, f_j) \in \mathcal{NC} \cup \mathcal{C}\} = \mathcal{NC} = \{\tau_{ij} \mid 1 \leq i < j \leq s\}$  and  $G = \{f_1, \dots, f_s\}$  so by Proposition 5.2.7 we have that  $\{\tau_{ij} \mid (f_i, f_j) \in \mathcal{NC} \cup \mathcal{C}\}$  generates  $\text{Syz}(\text{lt}(f_1), \dots, \text{lt}(f_s))$ . Before the while loop begins,  $\mathcal{NC}$  is made smaller using  $\text{crit2}$  and, by Corollary 5.3.2,  $\{\tau_{ij} \mid (f_i, f_j) \in \mathcal{NC} \cup \mathcal{C}\}$  remains a generating set for  $\text{Syz}(\text{lt}(f_1), \dots, \text{lt}(f_s))$ .

Now assume that the algorithm has iterated  $l \geq 1$  times, let  $G_l, \mathcal{NC}_l, \mathcal{C}_l$  denote the values of  $G, \mathcal{NC}, \mathcal{C}$  respectively during the  $l + 1$ -th iteration and assume that  $\{\tau_{ij} \mid (f_i, f_j) \in \mathcal{NC}_l \cup \mathcal{C}_l\}$  generates  $\text{Syz}(\text{lt}(f) \mid f \in G_l)$ . A pair  $(f_m, f_n)$  is chosen from  $\mathcal{NC}_l$  and moved to  $\mathcal{C}_l$ , renaming  $\mathcal{C}_l$  to  $\mathcal{C}_{l+1}$ . The pair  $(f_m, f_n)$  is checked with  $\text{crit1}$  and if it fails this check then we are not assured that  $S(f_m, f_n) \xrightarrow{G_l} 0$ . So we calculate  $S(f_m, f_n) \xrightarrow{G_l} h$ . If  $h \neq 0$  then we add  $h$  to  $G_l$  to form  $G_{l+1}$  and we update  $\mathcal{NC}$  with  $\{(f, h) \mid f \in G_l\}$ . Thus all of the pairs in  $\{\tau_{ij} \mid (f_i, f_j) \in \mathcal{NC}_{l+1} \cup \mathcal{C}_{l+1}\}$  generate  $\text{Syz}(\text{lt}(f_1), \dots, \text{lt}(f_s), \text{lt}(h))$ .  $\text{crit2}$  is applied again to  $\mathcal{NC}_{l+1}$ , possibly making  $\mathcal{NC}_{l+1}$  smaller, and  $\mathcal{NC}_{l+1} \cup \mathcal{C}_{l+1}$  still forms a generating set for  $\text{Syz}(\text{lt}(f_1), \dots, \text{lt}(f_s), \text{lt}(h))$ . So when the algorithm terminates,  $\mathcal{NC} = \emptyset$  and  $\mathcal{C}$  forms a generating set for  $\text{Syz}(\text{lt}(f_1), \dots, \text{lt}(f_t))$ , making  $G$  a Gröbner basis.

That the algorithm terminates follows the same way as in the proof of Theorem 4.2.9. □

Again, we also include a flow diagram to help understand the workings of Algorithm 5.4.3.



## Bibliography

1. W. Adams and P. Loustau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, RI, 1994. MR 1287608
2. B. Buchberger, *An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal*, J. Symbolic Comput. **41** (2006), no. 3-4, 475–511, Translated from the 1965 German original by Michael P. Abramson. MR 2202562
3. T. Fernique, *Compact packings of space with two sizes of spheres*, Discrete Comput. Geom. **65** (2021), no. 4, 1287–1295. MR 4249904
4. N. Gunther, *Sur les modules des formes algébriques*, Trav. Inst. Math. Tbilissi [Trudy Tbiliss. Mat. Inst.] **9** (1941), 97–206. MR 0007553
5. H. Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero. I, II*, Ann. of Math. (2) **79** (1964), 109–203; *ibid.* (2) **79** (1964), 205–326. MR 0199184
6. F. S. MacAulay, *Some Properties of Enumeration in the Theory of Modular Systems*, Proc. London Math. Soc. (2) **26** (1927), 531–555. MR 1576950
7. M. Penn, *A tricky geometry problem!*, <https://www.youtube.com/watch?v=xgEhkM6m-7o>.
8. B. Renschuch, H. Roloff, and G. G. Rasputin, *Beiträge zur konstruktiven Theorie der Polynomideale. XXIII. Vergessene Arbeiten des Leningrader Mathematikers N. M. Gjunter zur Theorie der Polynomideale*, Wiss. Z. Pädagog. Hochsch. “Karl Liebknecht” Potsdam **31** (1987), no. 1, 111–126. MR 928797