Groebner Bases and an Improvement on Buchberger's Algorithm

Dessalegn Yizengaw Melesse (dessalegn@aims.ac.za)
African Institute for Mathematical Sciences (AIMS)

Supervised by Cornelia Naude
University of Stellenbosch

June 5, 2007

Abstract

In the computation of Groebner bases using Buchberger's Algorithm, a key issue for improving the efficiency is to create techniques to help us avoid as many unnecessary pairs of polynomials from the non-computed set of pairs as possible. A good solution would be to avoid those pairs that can be easily ignored without computing their S-polynomials, and hence to process only on the set of pairs of generators of the module generated by syzygies. This paper details an improvment of Buchberger's Algorithm for computing Groebner bases by defining the module of solutions of a homogeneous linear equation with polynomial coefficients (called the syzygy module). As a consequence, we use these syzygy modules to give another equivalent condition for a set to be a Groebner basis for an ideal. As a result we demonastrate that this new condition can significantly improve the Buchberger's Algorithm to compute Groebner bases.

KEY WORDS: *Improvement on Buchberger's Algorithm, Computing Groebner bases, syzygy modules, S-polynomials*.

ጭብጥ

የቡችበርገር የመስሪያ ወይም ማስያ ዘዴ (Buchberger`s Algorithm) የግሮብነር ሳቢያን (Groebner Basis) ለመፈለግ ወይም ለማስላት የምንጠቀምበት ዋነኛ መንገድ ነዉ። ይህም ማለት የሳቢያዉ መሰረት ወይም ምንጭ (basis) የሆኑትን ኤስ-ፖሊኖሚያሎች (S-polynomials) በዘዴዉ በመጠቀም ማስላት (compute) ሲሆን የሚሰሉት ሁሉ ግን የሳቢያው ስብስብ አባላት ስለማይሆኑ የሚሆኑትን ብቻ ለይቶ ለማስላት እንዲረዳን ከዚህ በፊት የነበረዉን የቡችበርገር የመስሪያ ዘዴ ብቃት ማሻሻል የስሌቱን ዉስብስብነት ከመቀነሱም በላይ ጊዜን ይቆጥባል። ስለሆነም የሳቢያው አባል የማይሆኑትን ያለምንም ስሌት በቀላሉ ለይቶ ለመተዉና የሚሆኑትን ኤስፖሊኖሚያሎች ብቻ ለማስላት የሲዚጂ ሞጁል ጽንሰ ሃሳብን በመጠቀም የቡችበርገር የማስያ ዘዴን በሁለት መሰረታዊ መስፈርቶች ብቃቱን ከፍ ማድረግና የግሮብነር ሳቢያ አባል የማይሆኑትን ኤስ-ፖሊኖሚያሎች በመፈለግ ሊጠፉ ይችል የነበረዉን ጊዜ ከመቆጠቡም በላይ የስሌቱን ዉስብስብነት በእጅጉ መቀነስ እንደምንችል ጽሁፉ በጥልቀት ያትታል።

Contents

1. Introduction

The algorithmic theory of Groebner bases was introduced in 1965 by Bruno Buchberger in his PhD thesis. He named the basis after his PhD advisor, Wolfgang Groebner (1899-1980)) [fCM]. A problem of particular interest was the development of algorithms for computing Groebner bases. The standard algorithm for computing Groebner bases is Buchberger's Algorithm. The first algorithm, proposed by Buchberger, has a time complexity that is doubly exponential in the number of variables [JS06]. Since then several improvements have been proposed. The most time consuming parts of the algorithm are the increased number of S-polynomials to be computed, the difficulty to check the reduction of S-polynomials and the coefficient growth of S-polynomials. The improvements were mainly focused on addressing these problems. The optimized Buchberger's Algorithm proposed in [JS06] is an example of method that seeks to minimize the number of S-polynomials to be computed.

The algorithm computes, for a given finite basis, say $G = \{g_1, \ldots, g_s\}$ of an ideal $I = \langle G \rangle$, a Groebner basis by computing the so called S-polynomials, by reducing them modulo G as far as possible, and by adding these S-polynomials into G if they are irreducible and non-zero. If the computation eventually terminates, and all S-polynomials become zero modulo G, G is a Groebner basis of I. This means that
$G = \{g_1, ..., g_s\} \subset I$ *is a Groebner basis for I if and only if the S-polynomial* $\overline{S(g_i, g_j)}^G$ *is 0 for all* $1 \leq i, j \leq s$.

If these S-polynomials reduce modulo G to the zero polynomial, it is ignored and has no contribution to the final Groebner basis. So, we need a criteria that helps us to determine this reduction, and two basic criteria were in fact developed by Buchberger [AL96]. A a practical implementation and interpretation of one kind of Buchberger's criteria in terms of syzygies can be found in [GM88].

The involvement of the concept of syzygies is crucial in detecting the zero reductions, since it considers every pair of computed and non-computed sets of the S-polynomials. It also has the power to optimize the performance of Buchberger's Algorithm in minimizing the number of S-polynomials to be computed, which forms the main theme of this paper.

The reduction of a polynomial to zero means a linear dependence of this polynomial on the polynomials employed in the reduction procedure. Since all polynomials to be considered are of type $t_i f_i$, $f_i \in F$ if $F = \{f_1, \ldots, f_s\}$, t_i a power product, and the linear dependence relation can be written as a syzygial relation

$$\sum_{f_i \in F} g_i f_i = 0,$$

where the g_i are linear combinations of some power products t_{ij}, i.e they are polynomials, and hence the vector $(g_1, \ldots, g_s) \in A^s$, where $A = k[x_1, \ldots, x_n]$ is a commutative ring over a field k, is called a syzygy with respect to $(f_1, \ldots, f_s)$.

Among ideal bases, Groebner bases are especially well suited for constructively solving problems in commutative algebra, and a recent and exciting development is seen in its applications in computational biology and engineering. For instance see [fCM] and [JS06].

The most well-known algorithms to calculate Groebner bases, aside from Buchberger's Algorithm, are the recently introduced $F4$ [Fau99] and $F5$ [Fau02] algorithms. This paper introduces Groebner bases and the Improvement of Buchberger's Algorithm to compute the Groebner bases, but doesn't address these other algorithms.

The paper describes the connection between modules, Groebner bases, syzygies and the improvement of the Buchberger's Algorithm. The second Chapter next to this introduction reviews modules of a cartesian product A^s of a commutative ring $A = k[x_1, \ldots, x_n]$ over a field k. This is the background for the next Chapter in which we describe modules of syzygies. The third Chapter discusses the connection between Groebner bases and syzygies. A description of the basic concepts is given and it is shown how the performance of the Buchberger's Algorithm is improved by using syzygies.

In general, the main aim of this paper is to introduce the improvement of Buchberger's Algorithm. The last Chapter addresses this using two powerful commands (criteria), namely criterion 1 and criterion 2 denoted as $Crit1$ and $Crit2$ respectively, to improve the algorithm and compute Groebner bases. Finally, two solved examples are given to show how the algorithm's performance is improved in computing Groebner bases.

2. Modules

This Chapter contains the basic definitions and constructions in connection with modules, submodules and homomorphism of modules are also briefly discussed.

The notion of modules over a ring is the analogue of the notion of a vector space over a field,say k, in the sense that a module is defined by the same axioms, except that we allow ring elements as scalars and not just field elements. Just as vector spaces appear naturally as the solution sets of systems of linear equations over a field, modules appear as solutions sets of systems over a ring [GP02]. However, the underlying structure of the commutative ring can be considerably more complicated and unpleasant than the structure of the field. To give an example, the fact that some of the non-zero elements of a commutative ring may not have an inverse means that we cannot expect the ideas of linear independence and linear dependence to play as significant role in module theory as they do in the theory of vector spaces [Sha90]. For instance, the submodule (or ideal) $M = \{0, 2\}$ in the ring $\mathbb{Z}_4$ does not have a complement. This means that there is no other proper non-zero submodules, since 1 and 3 are invertible in the ring, and therefore can not belong to a proper submodule.

2.1 Preliminaries:

2.1.1 Basic Concepts of Ideals

Let A be a ring, for instance , let $A = k[x_1, \ldots, x_n]$, k is a field.

Definition 2.1.1. *A subset $I \subset k[x_1, \ldots, x_n]$ is an ideal if it satisfies:*

1. $0 \in I$.
2. *If $f, g \in I$, then $f + g \in I$.*
3. *If $f \in I$ and $h \in A$, then $hf \in I$.*

Definition 2.1.2. *Let $f_1, \ldots, f_s$ be polynomials in A. Then we set*
$\langle f_1, \ldots, f_s\rangle = \sum_{i=1}^{s} h_i f_i \ : h_1, \ldots, h_s \in A$.
Here it is important to note that $\langle f_1, \ldots, f_s\rangle$ is an ideal.

Lemma 2.1.1. *If $f_1, \ldots, f_s \in A = k[x_1, \ldots, x_n]$, then $\langle f_1, \ldots, f_s\rangle$ is an ideal of A. We call $\langle f_1, \ldots, f_s\rangle$ the ideal generated by $f_1, \ldots, f_s$.*

Proof. It is clear that $0 \in \langle f_1, \ldots, f_s\rangle$ since $0 = \sum_{i=1}^{s} 0 \cdot f_i$, for $0 \in A$.
Next, suppose that $f = \sum_{i=1}^{s} h_{1i} f_i$ and $g = \sum h_{2i} f_i$ and $h \in A$. Then

$$f + g = \sum_{i=1}^{s} (h_{1i} + h_{2i}) f_i$$
$$hf = \sum_{i=1}^{s} (hh_{1i}) f_i = \sum_{i=1}^{s} p_i f_i, \text{ for } p_i = hh_{1i} \in A.$$

which implies that $\langle f_1, \ldots, f_s\rangle$ is an ideal. □

We say that an ideal I is finitely generated if there exists $f_1, \ldots, f_s \in A$ such that $I = \langle f_1, \ldots, f_s \rangle$ and we say that $\{f_1, \ldots, f_s\}$ is a basis of I. Every ideal of $A = k[x_1, \ldots, x_n]$ is finitely generated (by Hilbert Basis Theorem 2.1.1)[CLO97]. Here note that a given ideal may have many different bases but one can choose an especially useful type of basis called *Groebner Basis* [Sha90]. This basis is going to be discussed in the next chapter.

2.1.2 Basic Concepts of Modules

Definition 2.1.3. *Let A be a ring with unity 1, and M be a non-empty set such that M is an additive abelian group with scalar multiplication by elements of A (i.e; if $x \in M$ and $a \in A$, then ax is a uniquely determined element of M). The set M is called an A-module (or a module over A) if the following conditions are satisfied:*

1. $a(m + m') = am + am'$, *for all* $a \in A$ *and* $m, m' \in M$
2. $(a + a')m = am + a'm$, *for all* $a, a' \in A$ *and* $m \in M$
3. $a(a'm) = (aa')m$, *for all* $a, a' \in A$ *and* $m \in M$
4. $1m = m$, *for all* $m \in M$.

Example 2.1.1. *[Sha90] Let A be a commutative ring, and let I be an ideal of A.*

1. *Then A is, of course, an abelian group and the scalar multiplication in A satisfies the ring axioms which turns A into an A-module. Thus a very important example of the A-module is A itself.*
2. *Since I is closed under addition and scalar multiplication by an arbitrary element of A, it follows that I is an A-module under the addition and multiplication of A.*
3. *The quotient ring A/I can also be viewed as an A-module. Of course, A/I has a natural abelian structure, so we need to provide it with a scalar multiplication by elements of A. Let $a, a' \in A$ such that $a + I = a' + I \in A/I$. Let $r \in A$. Thus $a - a' \in I$, and so $ra - ra' = r(a - a') \in I$. Hence $ra + I = ra' + I$. This can also be demonstrated by defining it as*

$$\begin{aligned} A \times A/I &\longrightarrow A/I \\ (r, s + I) &\longmapsto rs + I. \end{aligned}$$

One can easily show that A/I becomes an A-module with respect to this scalar multiplication. This concept of an A-module A/I will be discussed later in a cartesian product A^s.

Definition 2.1.4. *Let M be a module over a commutative ring A, and let M' be a subset of M. We say that M' is a submodule of M precisely when M' is itself an A module with respect to the operation for M.*

A non-empty subset M' of M will be a submodule of M if and only if it is closed under addition and $am \in M'$ for $m \in M'$ and $a \in A$.

The following remark can be taken as the criterion to determine whether a given A-module M' is a submodule of an A-module M.

Remark 2.1.1. *(The Submodule Criterion)[Sha90]: Let A be a commutative ring and let M' be a subset of the A-module M. Then M' will be a submodule of M if and only if the following conditions hold:*

1. $M' \neq \emptyset$.
2. *Whenever* $m, m' \in M'$, *and* $a, a' \in A$, *then* $am + a'm' \in M'$.

If $a_1, \ldots, a_s$ are elements of the A-module M, an element of M of the form

$$b_1a_1 + ... + b_sa_s, \text{ where each } b_i \in A$$

may naturally be called a linear combination of $a_1, \ldots, a_s$. The set of all linear combinations of $a_1, \ldots, a_s$ is a submodule of M [MB97]. Note that a submodule of M is an abelian subgroup of the additive group M, and so must have the same zero element as M. Furthermore, M itself is a submodule of M and also the set $\{0\}$; the latter is known as the *zero submodule of* M [Sha90].

Consider any submodule N of an A-module M defined by

$$M/N = \{m + N | m \in M\}$$

Then M/N is the quotient abelian group and can be made an A-module by defining

$$a(m + N) = am + N, \text{ for all } a \in A, m \in M$$

This multiplication is well defined such that for $a \in A$ and $m \in M$, and by using definition 2.1.3; we also let $m, m' \in M$ and $a, a' \in A$.

1. We can easily show that M/N is an abelian group.
2. $a((m + N) + (m' + N)) = (am + N) + (am' + N)$, where $am, am' \in M$ since M is an A-module.
3. $(a + a')(m + N) = a(m + N) + a'(m + N)$.
4. $a(a'(m + N)) = aa'(m + N)$.
5. $1(m + N) = 1.m + N = m + N$, since M is an A-module.
   Hence, M/N has the structure of an A-module and is called *the quotient module* of M by N.

A function $\phi : M \longrightarrow M'$ is called an A-module homomorphism provided that it is an abelian group homomorphism and scalar multiplication is also preserved, that is

$$\phi(m + m') = \phi(m) + \phi(m'), \text{ for all } m, m' \in M.$$

which satisfies

$$a\phi(m) = \phi(am), \text{ for all } a \in A, m \in M.$$

For the two A-modules M and M' given above, if there exists an A-homomorphism ϕ of M onto M', we say that M' is an A-homomorphic image of M. If ϕ is one-to-one, the homomorphism ϕ called an *isomorphism* and we write $M \cong M'$.
Let $N = ker(\phi) = \{\phi(m) = 0 | m \in M\}$. Then it can be easily shown that N and $\phi(M)$ are submodules of M and M' respectively. From the theory of abelian groups we know that $M/N \cong \phi(M)$ under the map

$$\begin{aligned} M/N &\longrightarrow \phi(M) \\ m + N &\longmapsto \phi(m) \end{aligned}$$

which is an A-module isomorphism as discussed above and referred to as *The First Isomorphism Theorem of modules*.

Theorem 2.1.1. *(Hilbert's Basis Theorem)[AL96] Let k be a field. In the ring $A = k[x_1, \ldots, x_n]$ we have the following :*

1. *If I is an ideal of A, then there exist polynomials $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ such that*

$$I = \langle f_1, \ldots, f_s \rangle$$

2. *If $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq \cdots$ is an ascending chain of ideals of $k[x_1, \ldots, x_n]$, then there exists an N such that $I_N = I_{N+1} = I_{N+2} = \cdots$.*

For the proof and related concepts see [AL96] and [CLO97]. The ideal I which satisfies condition (1) is said to be *finitely generated*. Further the ring A which satisfies condition (2), referred to as the *ascending chain condition*, is called a *Noetherian ring*.

Theorem 2.1.2. *[AL96] For a commutative ring A, the two conditions stated in Hilbert's Basis Theorem 2.1.1 are equivalent.*

Proof. Assume that condition (1) holds true. Let $I_1 \subseteq I_2 \subseteq ... \subseteq I_n \subseteq ...$ be an ascending chain of ideals of A. Consider the set $I = \bigcup_{n=1}^{\infty} I_{n_i}$. Since the ideals I_n are increasing, it is easy to see that I is an ideal of A. In addition, by condition (1), $I = \langle f_1, \ldots, f_s \rangle$ for some $f_1, \ldots, f_s \in A$. Since for $i = 1, \ldots, s$, f_i is in I, there exists N_i such that $f_i \in I_{N_i}$. Now let $N = \max_{1 \leq i \leq s} N_i$; then $f_i \in I_N$ for all $i = 1, \ldots, s$, and so $I \subseteq I_N$, which implies that $I = I_N$ and thus condition

(2) is satisfied.
To show that condition (2)$\Longrightarrow$ condition(1), assume that the contrary holds true: there exists an ideal of A that is not generated by a finite set of elements of A. Let $f_1 \in I$. Then there exists $f_2 \in A$ with f_2 not an element of $\langle f_1 \rangle$. Thus $\langle f_1 \rangle \subsetneqq \langle f_1, f_2 \rangle$. Continuing the same procedure which results an infinite sequence $f_1, \ldots, f_s$ of polynomials in I such that $\langle f_1 \rangle \subsetneqq \langle f_1, f_2 \rangle \subsetneqq \ldots \subsetneqq I$ which is an ascending chain of ideals of A which contradicts condition (2). □

2.2 Modules in a Cartesian Product of the Form A^m

Let A be the commutative ring $k[x_1, \ldots, x_n]$, k is a field. Having discussed some elementary aspects of modules, let us now shift a gear to address modules of a commutative ring A of the form A^m.

Definition 2.2.1. *Consider the cartesian product*

$$A^m = \left\{ \begin{bmatrix} a_1 \\ \vdots \\ a_m \end{bmatrix} | a_i \in A, i = 1, \ldots, m \right\}, \tag{2.1}$$

where A^m consists of all column vectors with coordinates in A of length m. The set A^m is called a free A-module [AL96] since every element $\mathbf{a} = (a_1, \ldots, a_m) \in A^m$ can be uniquely written as

$$\mathbf{a} = \textstyle\sum_{i=1}^{m} a_i \mathbf{e}_i, \text{ where } a_i \in A$$

with $\mathbf{e}_1 = (1, 0, \ldots, 0), \ldots, \mathbf{e}_m = (0, 0, \ldots, 1)$ which are called the standard basis of A^m.

Note: Bold letters will be used to refer to column vectors.

Definition 2.2.2. *In a given cartesian product of a ring A, the set $M \subseteq A^m$ is called an A-module provided that M is an additive abelian group undergoing scalar multiplication by elements of A. All the elements should satisfy conditions given in definition 2.1.3 with the difference that in this case elements of M are column vectors. Moreover, the scalar multiplication in this definition is done component wise.*

For instance, for vectors $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_s$ elements of an A-module, A^m, we have

$$M = \{b_1\mathbf{a}_1 + \cdots + b_s\mathbf{a}_s | b_i \in A, i = 1, \ldots, s\} \subseteq A^m.$$

M is a submodule of A^m denoted by $\langle \mathbf{a}_1, \ldots, \mathbf{a}_s \rangle \subseteq A^m$, and the set $\{\mathbf{a}_1, \ldots, \mathbf{a}_s\}$ is called the *generating set of* M. If there is a single element $\mathbf{a}$ of M such that $M = \langle \mathbf{a} \rangle$, we say that M is *cyclic module* with generator $\mathbf{a}$.

A finite set $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_s$ of elements of the A-module is said to be independent if

$$b_1\mathbf{a}_1 + b_2\mathbf{a}_2 + ... + b_s\mathbf{a}_s = \mathbf{0}, \text{ for all } \mathbf{b}_i \in A,$$

which implies that $b_i = 0$ (for $i = 1, \ldots, s$). If $\mathbf{a}_1, \ldots, \mathbf{a}_s$ is *independent* and generates M, then $\mathbf{a}_1, \ldots, \mathbf{a}_s$ are said to be *bases* of M (see [AL96] and [MB97]).
The concept of an A-module and a vector space is similar except that the set of scalars in the module case is in the ring A, which is not necessarily a field. Submodules of A^m are used for a linear algebra in A^m in the same way that subspaces of k^m are used for linear algebra in k^m [AL96].

Theorem 2.2.1. *[AL96] Every submodule M of A^m has a finitely generating set.*

Proof. Let M be a submodule of A^m. By induction, if $m = 1$, then M is a finitely generated ideal of A by Hilbert Basis Theorem.
If $m > 1$, let

$$I = \{a \in A | \text{a is the first coordinate of an element of } M\}.$$

Then I is an ideal of A and therefore finitely generated by the Hilbert's Basis Theorem. We are interested in showing that the module M has a finitely generated set.
Let

$$I = \langle a_1, \ldots, a_t \rangle.$$

Let $\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_t \in M$, with a_i being the first coordinate of $\mathbf{m}_i$.
Assume that the theorem holds true for submodules of A^{m-1}. Now consider $M' \in A^{m-1}$ such that $M' = \{(b_2, \ldots, b_m) | (0, b_2, \ldots, b_m) \in M\}$. Then we can note that M' is a submodule of A^{m-1} and by induction, is finitely generated (due to our assumption).
Suppose $\mathbf{n}'_1, \ldots, \mathbf{n}'_l \in M' \subseteq A^{m-1}$ are the generators of M', for $i = 1, \ldots, l$.
Let $\mathbf{n}_i \in A^m$, with 0 in the first coordinate, and $\mathbf{n}'_i$ is the vector with the remaining $m - 1$ coordinates. Note that $\mathbf{n}_i \in M$. We show that $M = \langle \mathbf{m}_1, \mathbf{m}_2, .., \mathbf{m}_t, \mathbf{n}_1, \ldots, \mathbf{n}_l \rangle$.
Let $\mathbf{m} \in M$. Now let m_1 be the first coordinate of $\mathbf{m}$. Then

$$m_1 = \textstyle\sum_{i=1}^{t} d_i a_i.$$

Again consider $\mathbf{m}' = \mathbf{m} - \sum_{i=1}^{t} d_i \mathbf{m}_i$. This implies that $\mathbf{m}' \in M$ with first coordinate equal to zero. Hence, $\mathbf{m}' = \sum_{i=1}^{l} c_i \mathbf{n}_i$ which leads us to the end of the proof that:

$$\mathbf{m} = \mathbf{m}' + \textstyle\sum_{i=1}^{t} d_i \mathbf{m}_i = \sum_{i=1}^{l} c_i \mathbf{n}_i + \sum_{i=1}^{l} d_i \mathbf{m}_i.$$

Hence, M is finitely generated. □

Now, consider an A-module M with $\mathbf{m}_1, \ldots, \mathbf{m}_s \in M$ and consider an A-module homomorphism $\phi : A^s \longrightarrow M$ defined by:

$$\phi(a_1, \ldots, a_s) = \sum_{i=1}^{s} a_i \mathbf{m}_i. \tag{2.2}$$

Then for **a=**$(a_1, \ldots, a_s)$, **a'** $= (a'_1, \ldots, a'_s) \in A^s$ and $c \in A$, we can easily show that

1. $\phi(\mathbf{a} + \mathbf{a}') = \phi(\mathbf{a}) + \phi(\mathbf{a}')$, for all $\mathbf{a}, \mathbf{a}' \in A^s$
2. $c\phi(\mathbf{a}) = \phi(c\mathbf{a})$, for all $\mathbf{a} \in A^s$ and $c \in A$.

Then by 1) and 2) ϕ is an A-module homomorphism. Moreover, the image of ϕ is the submodule of M generated by $\mathbf{m}_1, \ldots, \mathbf{m}_s$. Hence, if $\mathbf{m}_1, \ldots, \mathbf{m}_s$ generate M, then ϕ is onto.
Let $\mathbf{e}_1, \ldots, \mathbf{e}_s$ denote the standard basis elements in A^s, we note that ϕ is uniquely defined by specifying the image of each $\mathbf{e}_i \in A^s$, namely by specifying $\phi(\mathbf{e}_i) = \mathbf{m}_i$. We will often define a homomorphism ϕ from A^s by simply specifying $\phi(\mathbf{e}_i)$, for $i = 1, \ldots, s$ [AL96].

Now let $M = \langle \mathbf{m}_1, \ldots, \mathbf{m}_s \rangle$ and $N = ker(\phi) = \{\mathbf{a} \in A^s | \phi(\mathbf{a}) = \mathbf{0}\}$ and the map $\phi : A^s \longrightarrow M$ is defined as:

$$\phi(a_1, \ldots, a_s) \longmapsto \textstyle\sum_{i=1}^{s} a_i \mathbf{m}_i$$

Then,

1. we can easily show that the map is a homomorphism.
2. Since $\mathbf{m}_1, \ldots, \mathbf{m}_s$ generates M, we see that ϕ is onto and consider elements $\mathbf{a}, \mathbf{a}' \in A^s$, and $\mathbf{m}_i \in M$. We can then easily verify that if $\phi(\mathbf{a}+N) = \phi(\mathbf{a}'+N)$, then $\mathbf{a}+N = \mathbf{a}'+N$ which implies that ϕ is one-to-one. Then by these steps or generally by the First Isomorphism Theorem for modules, we have
$$M \cong A^s/N. \tag{2.3}$$

We therefore can conclude that

Lemma 2.2.1. *[AL96] Every finitely generated A-module M is isomorphic to A^s/N for some positive integer s and some submodule N of A^s.*

Here we note that for a submodule M of A^s, if we have $\mathbf{m}_1, \ldots, \mathbf{m}_t \in A^s$ for $t < s$ such that $M = \langle \mathbf{m}_1, \ldots, \mathbf{m}_t \rangle$ and for another submodule N of M , the module M/N can be explicitly given as $M/N = \langle \mathbf{m}_1 + N, \ldots, \mathbf{m}_t + N \rangle$ which is a submodule of A^s/N.

2.3 Noetherian Rings and Modules

Consider a non-empty partially ordered set $(V, \preceq)$; we say that $(V, \preceq)$ satisfies the ascending chain condition whenever $(v_i)_{i \in \mathbb{N}}$ is a family of subsets of V such that $v_1 \preceq v_2 \preceq ... \preceq v_i \preceq v_{i+1} \preceq \cdots$ then there exists $k \in \mathbb{N}$ such that $v_k = v_{k+i} \forall_{i \in \mathbb{N}}$ and we say that $(V, \preceq)$ satisfies the maximal condition if every non-empty subset of V contains a maximal element (with respect to $\preceq$) [Sha90].

Definition 2.3.1. *A module A is said to satisfy the ascending chain condition (ACC) on submodules (or to be Noetherian) if for every chain $A_1 \preceq A_2 \preceq A_3 \preceq \cdots$ of submodules of A, there is an integer n such that $A_i = A_n$ for all $i \geqslant n$.*
A submodule B is said to satisfy the descending chain condition (DCC) on submodules (or to be Artinian) if for every chain $B_1 \succeq B_2 \succeq B_3 \succeq \cdots$ of submodules of B, there is an integer m such that $B_i = B_m$ for all $i \geqslant m$ [Hun74].

Proposition 2.3.1. *[Sha90] Let A be the ring and M be an A-module. The following conditions are equivalent.*

1. *Every submodule of M is finitely generated.*
2. *Every ascending chain $M_1 \preceq M_2 \preceq \cdots$ of submodules of M is eventually stationary.*
3. *Every non-empty set of submodules of M has a maximal element (with respect to inclusion).*

Let $(A, \preceq)$ be a partially ordered set. Then an element $m \in A$ is said to be maximal if, for all $a \in A$ we have $a \preceq m$. Alternatively, an element m in A is maximal if $m \preceq a$ for any $a \in A$, implies that $m = a$.

Definition 2.3.2. *An A-module M is called Noetherian if it satisfies the equivalent conditions of Proposition 2.3.1.*

Definition 2.3.3. *[Hun74] The commutative ring A is Noetherian if and only if every ideal in A has a finite generating set.*

Hence,theorem 2.1.1 states that $A = k[x_1, \ldots, x_n]$ is Noetherian. It now follows from Theorem 2.2.1 that A^m is a Noetherian module for all $m \geq 1$.

Corollary 2.3.1. *Let $A = k[x_1, \ldots, x_n]$ be the ring and M be an A-module. Then every finitely generated A-module M is Noetherian.*

From the above Lemma 2.2.1, we have $M \cong A^s/N$ for some positive integer s and submodule N. Then the submodules of A^s/N will be of the form L/N provided that L is the submodule of A^s containing N. Now recall Theorem 2.2.1; i.e every submodule N of A^s is finitely generated. As A^s is Noetherian, this implies that every submodule of A^s/N is finitely generated 2.2.1. Hence, M is also Noetherian (See [AL96]).

3. Groebner Bases and Syzygies

Let $A = k[x_1, \ldots, x_n]$ and $M = \langle \mathbf{m}_1, \ldots, \mathbf{m}_s \rangle$. We define the map $\phi : A^s \longrightarrow M$, as given in equation 2.2. We have seen that ϕ satisfies the First Isomorphism Theorem, and hence $A^s/N \cong M$ where $N = ker(\phi)$. This isomorphic map will be considered in this Chapter to define syzygies, and the concept of S-polynomials used to determine generating sets of syzygies.

In the first section of this Chapter we will discuss preliminary concepts that will be used to develop the concept of Groebner bases and syzygies. In the last section of the Chapter we will briefly discuss modules of homogeneous linear equations with polynomial coefficients, syzygy modules, and we will briefly discuss the use of these modules in determining the Groebner bases of ideals.

3.1 Preliminary Concepts

Before we briefly deal with the connection between Groebner bases and syzygies let us review some important preliminary concepts.

3.1.1 Basic Concepts of Groebner Bases

Definition 3.1.1. *Monomial ordering on $k[x_1, \ldots, x_n]$ is any relation $>$ of $\mathbb{Z}^n_{\geq 0}$, or equivalently; a relation on the set of monomials $x^\alpha, \alpha \in \mathbb{Z}^n_{\geq 0}$, satisfying:*

1. *The relation $>$ is a total (or linear) ordering on $\mathbb{Z}^n_{\geq 0}$.*
2. *If $\alpha > \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma > \beta + \gamma$.*
3. *The relation $>$ is a well ordering on $\mathbb{Z}^n_{\geq 0}$. This means that every nonempty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under $>$.*

We have three basic monomial orderings, namely Lexicographical, Graded Lex and Graded Reverse Lex order (see [CLO97]).

Definition 3.1.2. *Let $f = \sum_\alpha a_\alpha x^\alpha$ be a non-zero polynomial in $k[x_1, ...x_n]$ and let $>$ be a monomial order:*

1. *the multidegree of f is multideg$(f) = \max(\alpha \in \mathbb{Z}^n_{\leq 0} : a_\alpha \neq 0)$ (the maximum is taken with respect to $>$).*
2. *the leading coefficient of f is lc$(f) = a_{\text{multideg}(f)} \in k$.*
3. *the leading power product of f is lp$(f) = x^{\text{multideg}(f)}$ (with coefficient 1).*
4. *the leading term of f is lt(f) = lc(f)lp(f).*

For instance, let $f(x,y,z) = 2xy^5z^2 + 3x^2y^3z^3 + 4x^3$. Then,

with respect to lex:	with respect to grlex:	with respect to grevlex
multideg$(f) = (3,0,0)$	multideg$(f) = (2,3,3)$	multideg$(f) = (1,5,2)$
lc$(f) = 4$	lc$(f) = 3$	lc$(f) = 2$
lp$(f) = x^3$	lp$(f) = x^2y^3z^3$	lp$(f) = xy^5z^2$
lt$(f) = 4x^3$	lt$(f) = 3x^2y^3z^3$	lt$(f) = 2xy^5z^2$

Definition 3.1.3. *A set of non-zero polynomials $G = \{g_1, \ldots, g_t\}$ contained in an ideal I, is called a Groebner basis for I if and only if for every $f \in I$ such that $f \neq 0$, there exists some $i \in \{1, \ldots, t\}$ such that* lp(g_i) *divides* lp(f).

This definition tells us that if G is the Groebner basis for an ideal I, then there is no non-zero polynomial in I reduced with respect to G ([AL96]).

Theorem 3.1.1. *Let I be a non-zero ideal of $k[x_1, \ldots, x_n]$. The following statements are equivalent for a set of non-zero polynomials $G = \{g_1, \ldots, g_t\} \subseteq I$.*

1. *G is a Groebner basis for I.*
2. *$f \in I$ if and only if $f \xrightarrow{G}_+ 0$.*
3. *$f \in I$ if and only if $f = \sum_{i=1}^{t} h_i g_i$ with* lp$(f) = \max_{1 \leq i \leq t}(lp(h_i)lp(g_i))$.*
4. *lt$(G) =$ lt(I).*

The theorem is proved in [AL96]. Based on this we have the following corollary that sometimes is considered as an alternative definition of Groebner bases.

Corollary 3.1.1. *[Hun74] Let $G = \{g_1, \ldots, g_t\}$ be a Groebner basis for an ideal $I \subset A = k[x_1, \ldots, x_n]$ and let $f \in A$. Then $f \in I$ if and only if the remainder on division of f by G is zero.*

Every non-zero ideal I of $A = k[x_1, \ldots, x_n]$ has a Groebner basis and using the condition of Groebner bases given in Theorem 3.1.1, we can detect whether a given basis is a Groebner basis for an ideal I.

Proposition 3.1.1. *Let $G = \{g_1, \ldots, g_t\}$ be a Groebner basis for an ideal I in A and let f be a polynomial in A. Then there is a unique r in A such that*

1. *r is completely reduced with respect to G. This is to mean that no term of r is divisible by* lt(g_1), ..., lt(g_t).
2. *there is $g \in A$ such that $f = g + r$.*

In particular, r is the remainder on division of f by G no matter how the elements of G are listed, when using the division algorithm (bear in mind that the "quotients" a_i produced by the algorithm in $f = a_1g_1 + a_2g_2 + ... + a_tg_t + r$ may change if we rearrange the g_i).

3.2 S-polynomial and Buchberger's Algorithm

We have seen that every non-zero polynomial ideal I of $k[x_1, \ldots, x_n]$ has a Groebner basis but we have not yet touched any of the techniques by which Groebner bases are constructed. So, now we can ask the question given an ideal $I \subset k[x_1, \ldots, x_n]$, say, how can we actually construct a Groebner bases for I? Answering this question will lead us to come up with Buchberger's Algorithm and the use of S-polynomials in computing Groebner bases.

Definition 3.2.1. *Fix a monomial ordering. Let f and g be two polynomials in A and let $J = lcm(lp(f), lp(g))$. The S-polynomial of f and g is the combination*

$$S(f,g) = \frac{J}{lt(f)} f - \frac{J}{lt(g)} g.$$

Note that J is computed in such a way that if multideg$(f) = \alpha$ and multideg$(g) = \beta$, then let $\gamma = (\gamma_1, \ldots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i. We call $J = x^\gamma$ the least common multiple of lp(f) and lp(g), written $J = x^\gamma = lcm(lp(f), lp(g))$.

Since $\frac{J}{\mathrm{lt}(f)}$ and $\frac{J}{\mathrm{lt}(g)}$ are monomials, then $S(f,g)$ belongs to the same ideal to which f and g belong. S-polynomials are constructed to cancel lt(f) and lt(g). In fact the two terms, from the S-polynomial obtained from f and g, are equal and cancel each other. We now illustrate this with an example.

Example 3.2.1. *Let $f = xy^3z - xy^3$ and $g = x^2yz - x^2z + z$ in $\mathbb{R}[x,y,z]$ with grlex order $x > y > z$. Then*
lt$(f) = xy^3z$, lt$(g) = x^2yz$ and $\gamma = (2,3,1)$ which implies that $J = x^\gamma = x^2y^3z$. Hence,

$$\begin{aligned} S(f,g) &= x(xy^3z - xy^3) - y^2(x^2yz - x^2z + z) \\ &= \underbrace{x^2y^3z} - x^2y^3 - \underbrace{x^2y^3z} + x^2y^2z - y^2z, \end{aligned}$$

Here we see that the underbraced elements cancel each other. We have seen that the S-polynomial was introduced as a means to cancel the leading terms but here we can further use the practical concept of S-polynomials to compute the Groebner bases.

Theorem 3.2.1. *(Buchberger[AL96])*
Let $G = \{g_1, \ldots, g_t\}$ be a set of non-zero polynomials in $k[x_1, \ldots, x_n]$. Then G is a Groebner basis for the ideal I=$\langle g_1, \ldots, g_t \rangle$ if and only if for all $i \neq j$,

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

This theorem is the basic driving force behind construction of Groebner bases. Hence, for a set G in A we can immediately test G for being a Groebner basis by checking whether

$$S(g_i, g_j) \xrightarrow{G}_+ 0 \text{ for all } g_i, g_j \in G,\ g_i \neq g_j.$$

If $S(g_i, g_j) \xrightarrow{G}_+ r$ and $r = 0$, nothing will be added to G because r is already in $\langle G \rangle$. If $r \neq 0$, we add r to G without changing the ideal, since $\langle G \rangle = \langle G, r \rangle$. We now consider $G \bigcup r$, and we continue finding S-polynomials until the new remainder r of $S(g_i, g_j) \xrightarrow{G}_+ 0$ for each pair of g_i and g_j is 0.

Definition 3.2.2. *Fix a monomial order. Let $G = \{g_1, \ldots, g_s\}$ be a finite set of polynomials in $k[x_1, \ldots, x_n]$. A polynomial g is completely reduced with respect to G (or modulo G) if no monomial of g is divisible by any of the $lp(g_i)$ for all $1 \leq i \leq s$.*

A polynomial g cannot have an infinite chain of reductions with respect to G: we must end up with a completely reduced polynomial which is called the *NormalForm of* g. To show that a polynomial h is a normal form of g with respect to G, we write $g \xrightarrow{G}_+ h$ or $h = \text{NormalForm}(g, G)$[Fab].

Theorem 3.2.2. *Given $F = \{f_1, \ldots, f_s\}$ with $f_i \neq 0 (1 \leq i \leq s)$, Buchberger's Algorithm given below will produce a Groebner basis for the ideal $I = \langle f_1, \ldots, f_s \rangle$.*

INPUT: A polynomial set $F = \{f_1, \ldots, f_t\} \subseteq K[x_1, \ldots, x_n]$ with $f_i \neq 0 (1 \leq i \leq t)$.
OUTPUT: A Groebner basis $G = \{g_1, \ldots, g_t\}$ that generates $I = \langle f_1, \ldots, f_t \rangle$
INITIALISATION: $G = F,\ G' = \{\{f_i, f_j\} \,|f_i \neq f_j \in G\}$
WHILE $G' \neq \emptyset$ **DO**
    choose any $\{f, g\} \in G'$
    $G' = G' - \{\{f, g\}\}$
    $S(f, g) \xrightarrow{G}_+ h$, where $h = \text{NormalForm}(S, G)$, i.e. h is reduced with respect to G
IF $h \neq 0$ **THEN**
        $G' = G' \cup \{\{u, h\} \,|\text{for all } u \in G\}$
        $G = G \cup \{h\}$

Algorithm 3.2.1. *Buchberger's Algorithm for Computing Groebner Basis [AL96].*

Example 3.2.2. *Consider an ideal generated by F such that*
$I = \langle F \rangle = \{f_1 = x^2 + 2xy^2, f_2 = xy + 2y^3 - 1\}$ with lex order $x > y$ in $\mathbb{R}[x, y]$. Find the Groebner basis for I. To find the basis we have to apply the algorithm as follows.
INITIALISING: we first set $G = F = \langle x^2 + 2xy^2, xy + 2y^3 - 1 \rangle$ and $G' = \{\{f_1, f_2\}\}$. This is the first assumed Groebner basis for the ideal for which an S-polynomial is to be computed. After initialising we have to apply the WHILE loop in order to determine the rest elements of the basis provided that the S-polynomial of f and g is not zero.
Apply the WHILE loop:
$G' \neq \emptyset$. Then choose $f_1, f_2 \in G$ to determine the S-polynomial for these two elements of G. $S(f_1, f_2) \xrightarrow{G}_+ x$ and NormalForm$(x, G) = x = h$ (Reduced with respect to G). So, since $h \neq 0$ add x, say $f_3 = x$, to G and update G'.
So, $G = \{f_1, f_2, f_3\}$ and $G' = \{\{f_1, f_3\}, \{f_2, f_3\}\}$
Then take $\{f_2, f_3\}$ and $S(f_2, f_3) \xrightarrow{G}_+ 2y^3 - 1$ and NormalForm$(2y^3 - 1, G) = 2y^3 - 1$.

Let $f_4 = 2y^3 - 1$. Add f_4 to G and update G' since f_4 is completely reduced modulo G or NormalForm$(f_4, G) = 2y^3 - 1$ (see Definition 3.2.2).
Then update $G = \{f_1, f_2, f_3, f_4\}$ and $G' = \{\{f_1, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$.
Following the same procedure for each pair of elements of G' in finding S-polynomials, we can get the following.
$S(f_1, f_3) = 2xy^2 = 2y^2 f_3$ *and* NormalForm$(S(f_1, f_3), G) = 0$.
$S(f_1, f_4) = \frac{1}{2}x^2 + 2xy^5 = \frac{1}{2}f_1 + xy^2 f_4$ *and* NormalForm$(S(f_1, f_4), G) = 0$.
$S(f_2, f_4) = \frac{1}{2}x + 2y^5 - y^2 = \frac{1}{2}f_3 + y^2 f_4$ *and* NormalForm$(S(f_2, f_4), G) = 0$.
$S(f_3, f_4) = \frac{1}{2}x = \frac{1}{2}f_3$ *and* NormalForm$(S(f_3, f_4), G) = 0$.
Now the WHILE loop stops since we have $G' = \emptyset$ and our job of finding Groebner basis stops here as S-polynomials of all pairs reduce to zero and so G becomes
$G = \{f_1, f_2, f_3, f_4\} = \{x^2 + 2xy^2, xy + 2y^3 - 1, x, 2y^3 - 1\rangle$.

Remark 3.2.1. *The steps we used to solve the above example are beyond what is necessary for a new S-polynomial; say $S(f_i, f_j) \xrightarrow{G}_+ h \neq 0$ (if $h = 0$, our computation would stop and no basis would be added to G) with lt(h) divisible by any of the $g_i \in G$ we had before. We eliminate h, and G is still a Groebner basis.*

Example 3.2.3. *Referring to the previous Example 3.2.2 since lt(f_1) and lt(f_2) are both multiples of f_3, we can eliminate f_1 and f_2 and then $G = \{f_3, f_4\} = \{x, 2y^3 - 1\}$.*
Furthermore, if we adjust constants to make all leading coefficients 1, we get a Groebner basis called the minimal Groebner basis[Fab].

3.2.1 Buchberger's Refined Algorithm

Under this subsection we will see some improvements on the basic Buchberger's Algorithm for computing Groebner bases. We see that the most expensive operation in the algorithm is the reduction of the S-polynomials modulo G. So, Buchberger developed two criteria for the reduction of polynomials. In addition, he also formulated another strategy that can help us to improve the speed of the calculations.

Let $G = \{f_1, \ldots, f_s\}$ be a Groebner basis.

- **Buchberger's Criterion 1:**
  If lcm(lp(f_i), lp(f_j)) = lp(f_i)lp(f_j), then
  $S(f_i, f_j) \xrightarrow{G}_+ 0$
  This criterion tells us that we can ignore calculating the S-polynomials of a pair whose leading power products are relatively prime.

- **Buchberger's Criterion 2:**
  When we consider $\{f_i, f_j\}$ in order to compute the S-polynomial, and if there is another element, say $f_t \in G$, with $f_i, f_j \neq f_t$ such that lcm(lp(f_i), lp(f_j)) is a multiple of the lp(f_t) and $S(f_i, f_t)$ and $S(f_j, f_t)$ have already been considered, then

$$S(f_i, f_j) \xrightarrow{G}_+ 0$$

This means that we can skip the calculation of $S(f_i, f_j)$.

Furthermore, Buchberger designed a strategy in selecting pairs for the computation of S-polynomials. It can be shown that if we always select a pair $\{f_i, f_j\}$ such that lcm(lp(f_i), lp(f_j)) is as small as possible with respect to the chosen monomial ordering (the so called *normal selection strategy*), then criteria 1 and 2 are good in the sense that all possible reductions of $S(f_i, f_j)$ will yield 0 [Fab].

So, based on the above two basic criteria the Buchberger's Algorithm can further be improved as follows:

INPUT: *A polynomial set* $F = \{f_1, \ldots, f_t\} \subseteq K[x_1, \ldots, x_n]$ *with* $f_i \neq 0 (1 \leq i \leq t)$.
OUTPUT: *A reduced Groebner basis* $G = \{g_1, \ldots, g_t\}$ *that generates* I.
Set: $G = F$
    (optionally) Reduce G
    $G' = \{\{f_i, f_j\}; 1 \leq i < j \leq s\}$
WHILE $(G' \neq \emptyset)$ **DO**
    $\{f_i, f_j\}$ = *a pair in* G' *such that lcm*(*lp*(f_i), *lp*(f_j)) *is minimal degree*
    $G' = G' - \{\{f_i, f_j\}\}$
    IF *(Criterion 1* $(\{f_i, f_j\})$ **AND NOT** *(Criterion 2* $(\{f_i, f_j\}, G, G'))$ **THEN**
        S=S-polynomial $\{f_i, f_j\}$
        $h =$ *NormalForm*(S, G)
        IF $(h \neq 0)$ **THEN**
            $G' = G' \bigcup \{\{g, h\} \text{ for all } g \in G\}$
            $G = G \bigcup \{h\}$

Algorithm 3.2.2. *Improved construction of Reduced Groebner Bases [Fab]*

Example 3.2.4. *I would like to refer to the previous example 3.2.2 under this subsection where an ideal* I *was given such that* $I = \langle F \rangle = \{f_1 = x^2 + 2xy^2, f_2 = xy + 2y^3 - 1\}$ *with lex order* $x > y$ *in* $\mathbb{R}[x, y]$.
In the example we obtained $G = \{f_1, f_2, f_3, f_4\}$ *and* $G' = \{\{f_1, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$. *with* $f_1 = x^2 + 2xy_2$, $f_2 = xy + 2y^3 - 1$, $f_3 = x$ *and* $f_4 = 2y^3 - 1$. *Then we have:*

lcm(*lp*(f_1), *lp*(f_3)) $= x^2$,

lcm(*lp*(f_1), *lp*(f_4)) $= x^2y^3$,

lcm($lp(f_2)$, *lp*(f_4)) $= xy^3$, *and*

lcm($lp(f_3)$, *lp*(f_4)) $= xy^3$

We can choose either of $\{f_2, f_4\}$ *or* $\{f_3, f_4\}$. *The reason why we prefer these from other pairs, is because of the strategy proposed by Buchberger and to apply Criterion 2 if Criterion 1 fails. But we*

can skip $\{f_3, f_4\}$ and $\{f_1, f_4\}$ by Criterion 1. Then let us look at $\{f_2, f_4\}$. But lcm(lp(f_2), lp(f_4)) is a multiple of f_3 and $S(f_2, f_3)$ was already considered which implies that $S(f_2, f_4) \xrightarrow{G}_+ 0$. Moreover, when we compute $S(f_1, f_3)$ we have NormalForm$(S(f_1, f_3), G)) = 0$. So, no more basis elements will be added. This implies that $G = \{f_1, f_2, f_3, f_4\}$. But we can reduce G into $\{f_3, f_4\}$ because we can cancel f_1 and f_2 from G, since their leading terms are both multiples of the leading term of f_3. Hence, $G = \{f_3, f_4\} = \{x, y^3 - 1/2\}$ (by normalising f_3 and f_4).

3.3 Groebner Bases and Syzygies

We now looked at the basic concepts in computing Groebner bases, which can be found using Buchberger's Algorithm for polynomial ideals as done in the preliminary section of this paper. In this section we are going to define the module of solutions of homogeneous linear equations with polynomial coefficients, called the syzygy module, which will be of course taken as an equivalent condition for a set to be Groebner basis for an ideal [AL96].

Definition 3.3.1. *Let A be a ring, M be an A-module, and $G = (f_1, \ldots, f_s)$ a tuple of elements of M. Then*

1. *A syzygy of G is a tuple $(h_1, \ldots, h_s) \in A^s$ that satisfies*

$$h_1 f_1 + \cdots + h_s f_s = \sum_{i=1}^{s} h_i f_i = 0. \tag{3.1}$$

2. *The set of all syzygies of $G = (f_1, \ldots, f_s)$ forms an A-module which we call the syzygy module of G denoted as Syz(G) or Syz$(f_1, \ldots, f_s)$.*

Example 3.3.1. *Let $A = \mathbb{Q}[x, y, z]$ with lex term ordering. Then consider the ideal $M = \langle g_1, g_2 \rangle$ generated by $g_1 = x^2 - y^2 - x$ and $g_2 = xy^2 - z^2$, and the pair $G = (g_1, g_2)$. The syzygy module of G is the submodule of*
Syz$(G) = \{(f_1, f_2) \in A^2 | f_1 g_1 + f_2 g_2 = 0\} = \{(f_1, f_2) \in A^2 | f_1(x^2 - y^2 - x) + f_2(xy^2 - z^2) = 0\}$ of A^2. Here we see that the Syz$(G) = \langle g_2, -g_1 \rangle$ since $f_1 = g_2$ and $f_2 = -g_1$ satisfies equation 3.1.

Let $A = k[x_1, \ldots, x_n]$ be a Noetherian ring with certain term ordering such that $(f_1, \ldots, f_s) \in A^s$ and let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal of A.

Consider the A-module homomorphism ϕ defined by:

$$\begin{array}{ll} \phi : A^s \longrightarrow I & \text{given by} \\ (h_1, \ldots, h_s) \longmapsto \sum_{i=1}^{s} h_i f_i & \end{array}$$

From the isomorphism given in equation 2.3 it follows that $I \cong A^s / ker(\phi)$, and from the definition of ϕ, that the kernel of ϕ is the syzygy module of the $1 \times s$ matrix $[f_1 \cdots f_s]$. So $(h_1, \ldots, h_s) \in A^s$

is in Syz$(f_1, \ldots, f_s)$ if it satisfies $h_1 f_1 + \cdots + h_s f_s = 0$.
We can introduce the elements of Syz$(f_1, \ldots, f_s)$ with a matrix multiplication such that $\phi(h_1, \ldots, h_s) = [f_1 \cdots f_s] \begin{bmatrix} h_1 \\ \vdots \\ h_s \end{bmatrix} = \sum_{i=1}^{s} h_i f_i$. We let $F = [f_1 \cdots f_s]$ and $\mathbf{h} = \begin{bmatrix} h_1 \\ \vdots \\ h_s \end{bmatrix} \in A^s$, then $\phi(h_1, \ldots, h_s) = F\mathbf{h}$, and Syz$(f_1, \ldots, f_s)$ is the solutions of the linear equation $F\mathbf{h} = \mathbf{0}$.

Example 3.3.2. *Let $A = \mathbb{Q}[x, y, z, w]$, and $I = \langle x^2 - yw, xy - wz, y^2 - xz \rangle$.*
Let $f_1 = x^2 - yw$, $f_2 = xy - wz$ and $f_3 = y^2 - xz$. Let $\phi : A^3 \longrightarrow I$ defined by

$$(h_1, h_2, h_3) \longmapsto \sum_{i=1}^{3} h_i f_i, \text{ where } (h_1, h_2, h_3) \in A^3 \text{ and } f_i \in I.$$

We need to find Syz(f_1, f_2, f_3). This is in fact the same as finding parameters h_1, h_2, and h_3 which satisfy the equation

$$h_1 f_1 + h_2 f_2 + h_3 f_3 = 0. \tag{3.2}$$

We can see that equation 3.2 is satisfied for $(h_1, h_2, h_3) = (y, -x, w)$ and $(h_1, h_2, h_3) = (-z, y, -x)$. This means $yf_1 - xf_2 + wf_3 = 0$ and $-zf_1 + yf_2 - xf_3 = 0$.
Then we observe that

$$\text{Syz}(f_1, f_2, f_3) = \text{Syz}(x^2 - yw, xy - wz, y^2 - xz) = \langle (y, -x, w), (-z, y, -x) \rangle \subseteq A^3$$

Because of $I \cong A^s / ker(\phi)$ (isomorphism) for the map $\phi : A^s \longrightarrow I$, the ideal I can be described as a quotient of a free A-module and Syz$(f_1, \ldots, f_s)$.

Syz$(f_1, \ldots, f_s)$ plays an important role in the theory of Groebner bases, and in particular, its use will lead us to improvements of Buchberger's Algorithm. Note that Syz$(f_1, \ldots, f_s) \subseteq A^s$ is finitely generated, since it is a submodule of A^s (by Theorem 2.2.1). The main aim of this section is to find a way to compute the generators of Syz$(f_1, \ldots, f_s)$ and then to compute Groebner bases. So, let us start with the following proposition, which is a special case of computing generators of Syz$(f_1, \ldots, f_s)$.

Proposition 3.3.1. *[AL96] Let $c_1, \ldots, c_s \in k - \{0\}$ and let $X_1, \ldots, X_s$ be power products in A. For $i \neq j \in \{1, \ldots, s\}$, we define $X_{ij} = lcm(X_i, X_j)$. Then the module Syz$(c_1 X_1, \ldots, c_s X_s)$ is generated by*

$$\left\{ \frac{X_{ij}}{c_i X_i} \mathbf{e}_i - \frac{X_{ij}}{c_j X_j} \mathbf{e}_j \in A^s | 1 \leq i < j \leq s \right\},$$

where $\mathbf{e}_1, \ldots, \mathbf{e}_s$ are the standard basis of A^s.

Proof. We can see that $\frac{X_{ij}}{c_i X_i} \mathbf{e}_i - \frac{X_{ij}}{c_j X_j} \mathbf{e}_j$ for $i \neq j$ is a syzygy of $[c_1 X_1 \cdots c_s X_s]$, since

$\frac{X_{ij}}{c_iX_i}\mathbf{e}_i - \frac{X_{ij}}{c_jX_j}\mathbf{e}_j = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \frac{X_{ij}}{c_jX_j} \\ 0 \\ \vdots \\ 0 \\ -\frac{X_{ij}}{c_jX_j} \\ 0 \\ \vdots \\ 0 \end{bmatrix}$. Then $[c_1X_1 \cdots c_iX_i \cdots c_jX_j \cdots c_sX_s]\,(\frac{X_{ij}}{c_iX_i}\mathbf{e}_i - \frac{X_{ij}}{c_jX_j}\mathbf{e}_j) = 0.$

Note that the standard basis $\mathbf{e}_i$ is a column vector.Therefore,

$$\left\langle \frac{X_{ij}}{c_iX_i}\mathbf{e}_i - \frac{X_{ij}}{c_jX_j}\mathbf{e}_j | 1 \le i < j \le s \right\rangle \subseteq \mathrm{Syz}(c_1X_1, \ldots, c_sX_s).$$

To prove the converse, let $(h_1, \ldots, h_s)$ be a syzygy of $[c_1X_1 \cdots c_sX_s]$, that satisfies

$$h_1c_1X_1 + ... + h_sc_sX_s = 0.$$

Then we need to show that $(h_1, \ldots, h_s)$ is a linear combination of elements of the form $\left\langle \frac{X_{ij}}{c_iX_i}\mathbf{e}_i - \frac{X_{ij}}{c_jX_j}\mathbf{e}_j \right\rangle$. Now let X be a power product. Then the coefficient of X in $h_1c_1X_1 + \cdots + h_sc_sX_s$ must be zero. Thus it suffices to consider the case for which $h_i = c_i'X_i'$ for $i = 1, \ldots, s$, and where $c_i' = 0$ or $X_iX_i' = X$ for a fixed power product X such that

$$c_1'c_1X_1X_1' + \cdots + c_i'c_iX_iX_i' + \cdots + c_s'c_sX_sX_s' = 0 \tag{3.3}$$

Then it is clear that equation 3.3 is satisfied if $c_i' = 0$. Let $X_iX_i' = X$, and suppose that there exists a subset J such that $c_{i_j} \neq 0$ for any $i_j \in J$ (that is $J = \{c_{i_1}, \ldots, c_{i_t}\}$, where $i_1 < \cdots < i_t$ with non-zero $c_{i_j}'s$). Then we have

$$c_1'c_1 + \cdots + c_s'c_s = c_{i_1}'c_{i_1} + \cdots + c_{i_t}'c_{i_t} = 0. \text{ Hence,}$$

$$\begin{aligned}
(h_1, \ldots, h_s) &= (c_1'X_1', \ldots, c_s'X_s') = c_{i_1}'X_{i_1}'\mathbf{e}_{i_1} + \cdots + c_{i_t}'X_{i_t}'\mathbf{e}_{i_t} \\
&= c_{i_1}'c_{i_1}\frac{X}{c_{i_1}X_{i_1}}\mathbf{e}_{i_1} + \cdots + c_{i_t}'c_{i_t}\frac{X}{c_{i_t}X_{i_t}}\mathbf{e}_{i_t}, \text{where } X_{i_1}' = \frac{X}{X_{i_1}} \\
&= c_{i_1}'c_{i_1}\frac{X}{X_{i_1i_2}}(\frac{X_{i_1i_2}}{c_{i_1}X_{i_1}}\mathbf{e}_{i_1} - \frac{X_{i_1i_2}}{c_{i_2}X_{i_2}}\mathbf{e}_{i_2}) + (c_{i_1}'c_{i_1} + c_{i_2}'c_{i_2})\frac{X}{X_{i_2i_3}}(\frac{X_{i_2i_3}}{c_{i_2}X_{i_2}}\mathbf{e}_{i_2} - \frac{X_{i_2i_3}}{c_{i_3}X_{i_3}}\mathbf{e}_{i_3}) \\
&+ \cdots + (c_{i_1}'c_{i_1} + \cdots + c_{i_{t-1}}'c_{i_{t-1}})\frac{X}{X_{i_{t-1}i_t}}(\frac{X_{i_{t-1}i_t}}{c_{i_{t-1}}X_{i_{t-1}}}\mathbf{e}_{i_{t-1}} - \frac{X_{i_{t-1}i_t}}{c_{i_t}X_{i_t}}\mathbf{e}_{i_t}) + k\frac{X}{c_{i_t}X_{i_t}},
\end{aligned}$$

where $k = c_{i_1}'c_{i_1} + ... + c_{i_t}'c_{i_t} = 0$. This implies that every term of the syzygy is a linear combination of the $\frac{X_{ij}}{c_iX_i}\mathbf{e}_i - \frac{X_{ij}}{c_jX_j}\mathbf{e}_j$ and the proof ends here. □

From what we have seen above, we observe that if $c_1X_1, \ldots, c_sX_s$ are leading terms of the polynomials $f_1, \ldots, f_s$, and if $(h_1, \ldots, h_s) \in \mathrm{Syz}(c_1X_1, \ldots, c_sX_s)$, then we have $\sum_{i=1}^{s} h_i f_i$. This sum has a leading term strictly smaller than $\max_{1<i<s} \mathrm{lp}(h_i)\mathrm{lp}(f_i)$.
In particular the syzygy $\frac{X_{ij}}{c_iX_i}\mathbf{e}_i - \frac{X_{ij}}{c_jX_j}\mathbf{e}_j$ of $[c_1X_1 \cdots c_sX_s] = [lt(f_1) \cdots lt(f_s)]$ give rise to an S-polynomial of f_i and f_j, since

$$[f_1, \ldots, f_s]\,(\frac{X_{ij}}{c_iX_i}\mathbf{e}_i - \frac{X_{ij}}{c_jX_j}\mathbf{e}_j) = \frac{X_{ij}}{c_iX_i}f_i - \frac{X_{ij}}{c_jX_j}f_j = S(f_i, f_j) \tag{3.4}$$

Definition 3.3.2. *Let $X_1, \ldots, X_s$ be power products and $c_1, \ldots, c_s \in k - \{0\}$. Then for a power product X, we call a syzygy $\mathbf{h}=(h_1, \ldots, h_s) \in$ Syz$(c_1X_1, \ldots, c_sX_s)$ homogeneous of degree X provided that each h_i is a term (that is , lt$(h_i) = h_i$ for all i) and $X_i$lp$(h_i) = X$ for all i such that $h_i \neq 0$. We say that $h \in$ Syz$(c_1X_1, \ldots, c_sX_s$ is homogeneous if it is homogeneous degree X for some power product X.*

This last conclusion (equation 3.4) indicates that the syzygy module of $[\mathrm{lt}(f_1) \cdots, lt(f_s)]$ will be important in computing the Groebner basis for $\langle f_1, \ldots, f_s \rangle$.

Remark 3.3.1. *The generating set in Proposition 3.3.1 consists of a finite set of homogeneous syzygies.*

Theorem 3.3.1. *[AL96] Let $G = \{g_1, \ldots, g_t\}$ be a set of non-zero polynomials in A. Let B be a homogeneous generating set of Syz(lt$(g_1), \ldots,$ lt$(g_t))$. Then G is Groebner basis for the ideal $\langle g_1, \ldots, g_t \rangle$ if and only if for all $(h_1, \ldots, h_t) \in B$, we have*

$$h_1g_1 + \cdots + h_tg_t \xrightarrow{G}_{+} 0.$$

The proof is in [AL96] and for more, see [CLO97]).

The corollary given below tells us about the Groebner basis and the relation with the S-polynomial; it has the same argument as the preliminary Theorem of Buchberger (theorem 3.2.1) we saw previously.

Corollary 3.3.1. *Let $G = \{g_1, \ldots, g_t\}$ be a set of non-zero polynomials in A. Then G is a Groebner basis if and only if for all $i, j = 1, \ldots, t$*

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

from

Proof. 1. ($\Rightarrow$) Let G be a Groebner basis. Then since $S(g_i, g_j)$ is an element of an ideal $\langle g_1, \ldots, g_t \rangle$, we have $S(g_i, g_j) \xrightarrow{G}_{+} 0$.

2. ($\Leftarrow$) By Theorem 3.3.1 we have the set,

$$B = \left\{ \frac{X_{ij}}{\mathrm{lt}(g_i)}\mathbf{e}_i - \frac{X_{ij}}{\mathrm{lt}(g_j)}\mathbf{e}_j | i < j \text{ and } i, j = 1, \ldots, t \right\} \subseteq A^t$$

a homogeneous generating set of the syzygy module of $[\mathrm{lt}(g_1)\cdots\mathrm{lt}(g_t)]$. Then by the remark after Proposition 3.3.1 that resulted in 3.4, every element of B gives rise to an S-polynomial which reduces to zero.

Hence, G is a Groebner basis. □

Example 3.3.3. *Consider the set $G = \{g_1, g_2\}$, where $g_1 = x+y, g_2 = x+1 \in \mathbb{Q}[x,y]$ with lex order $x > y$. Then we need to prove that the set $\{(x+1,-x-1),(x,-x)\}$ is the generating set for Syz(lt(g_1), lt(g_2)).*
To prove let us start with Syz(lt(g_1), lt(g_2)) = Syz(x,x) and lt(g_1) = lt(g_2) = x. Then by proposition 3.3.1 we have generators $\frac{x}{x}\mathbf{e}_1 - \frac{x}{x}\mathbf{e}_2 = (1,-1) \subseteq A^2$
Let $(h_1,h_2) \in$ Syz(x,x). Then $(h_1,h_2) \in \langle(1,-1)\rangle$ which implies that $h_1 = -h_2$. Then $(h_1,h_2) = h_1(x+1,-x-1)+h_2(x,-x))$ which implies that $(h_1,h_2) \in \langle(x+1,-x-1),(x,-x)\rangle$.
Moreover, we can see that $h_1g_1 + h_2g_2 \xrightarrow{\{g_1,g_2\}}_+ 0$ although G is not a Groebner basis since the leading term of the one divides the other.

4. Improvements on Buchberger's Algorithm

So far we have seen how the ordinary Buchberger's Algorithm is used to compute Groebner bases of ideals. We also reviewed the refined Buchberger's Algorithm and the strategy proposed to speed up calculations in computing Groebner bases. We can now use this knowledge to simplify our procedures. However, the computational complexity of Buchberger's Algorithm often makes the computation difficult for even small problems.

In this Chapter we will investigate more improvements in the algorithm. We can observe that the algorithm has two principal steps: the computation of the S-polynomials and their reduction. What makes the algorithm complex is the increment of the number of S-polynomials that has to be computed and hence as the computation progresses, the number of bases gets larger and larger. In addition we need to be careful in manipulating the algorithm, because of the fact that the bases are finite and our computation should terminate somewhere. In fact, at some point before the algorithm terminates, the desired Groebner basis is obtained but we do not "know" it. At that point the computation of S-polynomials and their reductions are all together useless except for the fact that they verify that we do have a Groebner basis [AL96]. So, one way to solve such a problem is to predict that some S-polynomials will reduce to zero, without reducing them by computation.

4.1 Concepts to Improve Buchberger's Algorithm

In Chapter 2 we presented the basic concepts of Buchberger's Algorithm and the refined version of the algorithm that can be used to compute Groebner basis for an ideal I. In this section we are going to address how the concepts of syzygies can be used to improve Buchberger's Algorithm to compute Groebner bases.

Lemma 4.1.1. *[AL96] Let $f, g \in A = k[x_1, \ldots, x_n]$, both non-zero , and let $d = \gcd(f, g)$. The following statements are equivalent:*

1. *lp$(\frac{f}{d})$ and lp$(\frac{g}{d})$ are relatively prime.*

2. $S(f, g) \xrightarrow{\{f,g\}}_+ 0$.
   In particular, $\{f, g\}$ is a Groebner basis if and only if lp$(\frac{f}{d})$ and $lp(\frac{g}{d})$ are relatively prime.

This lemma is proved in [AL96] and is taken as one of the criteria of Buchberger's Algorithm that determine whether the S-polynomial is reduced or not. Having f and g such that lp$(\frac{f}{d})$ and lp$(\frac{g}{d})$ are relatively prime implies that it is not necessary to compute $S(f, g)$, since $S(f, g)$ will reduce to zero using f and g alone. Hence, an S-polynomial will not be created and added to the basis. This idea is used in the basic commands of Buchberger's Algorithm, and is given as $Crit1$ in the next section of this chapter.

Lemma 4.1.2. *[AL96] Let $X_1, \ldots, X_s$ be power products in $A = k[x_1, \ldots, x_n]$ and let $c_1, \ldots, c_s \in k - \{0\}$. For $i, j = 1, \ldots, s$ define $X_{ij} = lcm(X_i, X_j)$, and let*

$$\tau_{ij} = \frac{X_{ij}}{c_i X_i}\mathbf{e}_i - \frac{X_{ij}}{c_j X_j}\mathbf{e}_j \in Syz(c_1X_1, \ldots, c_sX_s) \subseteq A^s,$$

where $\mathbf{e}_1, \ldots, \mathbf{e}_s$ is the standard basis for A^s. For each $i, j, l = 1, \ldots, s$ let $X_{ijl} = lcm(X_i, X_j, X_l)$. Then we have

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

More over, if X_l divides X_{ij}, then τ_{ij} is in the submodule of A^s generated by τ_{jl} and τ_{il}.

Proof. To prove the lemma we let $\tau_{ij} = \frac{X_{ij}}{c_i X_i}\mathbf{e}_i - \frac{X_{ij}}{c_j X_j}\mathbf{e}_j$.
Then we have

$$\begin{aligned}\frac{X_{ijl}}{X_{ij}}\tau_{ij} + \frac{X_{ijl}}{X_{jl}}\tau_{jl} + \frac{X_{ijl}}{X_{li}}\tau_{li} &= \frac{X_{ijl}}{X_{ij}}\left(\frac{X_{ij}}{c_i X_i}\mathbf{e}_i - \frac{X_{ij}}{c_j X_j}\mathbf{e}_j\right) + \frac{X_{ijl}}{X_{jl}}\left(\frac{X_{jl}}{c_j X_j}\mathbf{e}_j - \frac{X_{jl}}{c_l X_l}\mathbf{e}_l\right) + \frac{X_{ijl}}{X_{il}}\left(\frac{X_{il}}{c_i X_i}\mathbf{e}_i - \frac{X_{il}}{c_l X_l}\mathbf{e}_l\right)\\ &= \frac{X_{ijl}}{c_i X_i}\mathbf{e}_i - \frac{X_{ijl}}{c_j X_j}\mathbf{e}_j + \frac{X_{ijl}}{c_j X_j}\mathbf{e}_j - \frac{X_{ijl}}{c_l X_l}\mathbf{e}_l + \frac{X_{ijl}}{c_l X_l}\mathbf{e}_l - \frac{X_{ijl}}{c_i X_i}\mathbf{e}_i = 0.\end{aligned}$$

If X_l divides X_{ij}, then $X_{ijl} = X_{ij}$, and we have

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

Hence, τ_{ij} is in the submodule of A^s generated by τ_{jl} and τ_{li}. □

4.2 Improvements on Buchberger's Algorithm

We can now proceed with the improvement of Buchberger Algorithm by using syzygies. We will use the notation that we have used in Lemma 4.1.2. We first look at the following corollary.

Corollary 4.2.1. *[AL96] Let $B \subseteq \{\tau_{ij} | 1 \leq i < j \leq s\}$ be a generating set for Syz$(c_1X_1, \ldots, c_sX_s)$. Suppose we have three distinct indices i, j, l such that $\tau_{ij}, \tau_{jl}, \tau_{li} \in B$, and such that X_l divides $X_{ij} = lcm(X_i, X_j)$. Then $B - \{\tau_{ij}\}$ is also a generating set for Syz$(c_1X_1, \ldots, c_sX_s)$.*

Now let us set $\{f_1, \ldots, f_s\}$ to be generators for the ideal I in $k[x_1, \ldots, x_n]$ and $c_iX_i = \mathrm{lt}(f_i)$. We will use the same notation as given in the corollary and eliminate as many $\tau_{ij} \in B$ as possible (by applying Corollary 4.2.1) to obtain a smaller set of generators for Syz$(\mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s))$. Then we need to find the S-polynomial $S(f_i, f_j)$, corresponding to one of the τ_{ij} remaining in B and reduce it. We then add the reduced S-polynomial, say f_{s+1}, to the set $\{f_1, \ldots, f_s\}$ if $f_{s+1} \neq 0$; otherwise we ignore it. Now the generating set B is enlarged to $\{\tau_{i,s+1} | 1 \leq i \leq s.\}$ which generates Syz$(\mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s), \mathrm{lt}(f_{s+1}))$. Again we apply the steps in Corollary 4.2.1 to eliminate as many $\tau'_{ij}s$ from the new set, to obtain a smaller generating set for Syz$(\mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s), \mathrm{lt}(f_{s+1}))$. Then find S-polynomial, $S(f_i, f_j)$, corresponding to a τ_{ij} remaining in B and reduce it. We have to keep doing this until all S-polynomials are reduced to zero. If all these S-polynomials are reduced to zero, then we maintain the set B as a basis of the current syzygy module.

The main objective of the algorithm is to reduce the S-polynomials either to zero, and ignore the pairs or reduce it and add the new polynomial to the set. So, we need to have techniques to do this. Now let us see how the algorithm is set to compute these S-polynomials and reduce them. We first subdivide the set of indices $\{\{i,j\}, \tau_{ij} \in B\}$ into two subsets: the computed set C= $\{\{i,j\}, \tau_{ij} \in B \text{ for which an S} - \text{polynomial has been computed}\}$ and the non-computed set $NC = \{\{i,j\}, \tau_{ij} \in B \text{ for which an S} - \text{polynomial has not been computed}\}$.

Here we note that at any time in the algorithm after NC has been initialised, $\{\tau_{ij} | \{i,j\} \in NC \bigcup C\}$ is the generating set of the syzygy module of the current set of leading terms. We continue the algorithm until $NC = \emptyset$.

With these ideas acting as foundation, we can now introduce the improved version of Buchberger Algorithm to compute Groebner bases using syzygies. The improvement of the performance of the algorithm is based on the following two main criteria, $Crit1(i,j)$ and $Crit2(i,j)$, given below:

1. $Crit1(i,j)$:
   It turns "TRUE" if and only if lp(f_i) and lp(f_j) are relatively prime.
   If $Crit1(i,j)$=TRUE, we can ignore computing $S(f_i, f_j)$ since $S(f_i, f_j)$ reduces to zero modulo G by Lemma 4.1.1 . So, nothing is added to the basis and $\{i,j\}$ is added to C . We pick a pair of $\{f_i, f_j\}$ such that lp(f_i) and lp(f_j) are not relatively prime.

2. $Crit2(NC, C, s)$:
   This command is given as an algorithm 4.2.2 and is used to eliminate pairs from the set NC with out computing their S-polynomial. It is the implementation of the ideas in Corollary 4.2.1. As it will be seen from algorithm 4.2.2, the basic idea is to find triples of indices ν, μ, ρ such that the three pairs $\{\nu,\mu\}, \{\mu,\rho\}, \{\mu,\rho\}$ are in $NC \bigcup C$ and X_ν divides lcm(X_μ, X_ρ) [AL96].

Since we are interested in doing the first main WHILE loop of algorithm 4.2.2, we only need to consider one of ν, μ, ρ is equal to s. This is because the cases of all triples with ν, μ, ρ all less than s were checked before. Since μ and ρ are interchangeable, it is enough to consider the cases $\rho = s$ and $\nu = s$ in order to go through that eliminate pairs from the set NC without computing the S-polynomial. Moreover, we note that a pair of the form $\{i,s\}$ cannot lie in C (this explains why checking membership in $NC \bigcup C$ was often done by just checking membership in NC). Finally, we only check, in the second main WHILE loop, whether $\{i,j\}$ is in NC since we are only interested in eliminating it from NC [AL96].

First of all we take (NC, C, s) from algorithm 4.2.1 as an input for algorithm 4.2.2, to allow us to eliminate pairs from the set NC which were not already eliminated by algorithm 4.2.1. Consider a pair $\{i,s\} \in NC (i < s)$ to check whether this pair is to be eliminated from NC or not. We start with a pair $\{l,s\}$ where $1 \leq l < s$. Then if we have $\{l,s\} \in NC$ and the pairs $\{i,l\} \in NC \bigcup C$ with $\{i,s\} \in NC$, then we are supposed to check only whether X_l divides lcm(X_i, X_s) such that the pair $\{i,s\}$ can be eliminated from NC and NC will be updated to $NC - \{\{i,s\}\}$; otherwise that pair $\{i,s\}$ will remain in the set NC. We proceed checking for different $i, l < s$ until checking for every pair of the form $\{i,s\}$ is completed.

The second main WHILE loop starts to check whether the pair $\{i,j\}$, where $i,j < s$, will be

eliminated from the set NC or not. Here we note that since $i, j < s$, the pair was checked before but not eliminated. Now consider the pair $\{i, s\} \in NC$. In fact, the pair can not lie in C. Hence, for $j < s$ and if the pairs $\{j, s\}$ and $\{i, j\}$ are both in NC, and X_s divides $\mathrm{lcm}(X_i, X_j)$, then the pair $\{i, j\}$ will be eliminated from the set NC otherwise it will be updated as an element of NC. We proceed checking for pairs of $\{i, j\}$ with $i, j < s$ and update the set.

Finally, after we had finished going through the loops and determining which pairs are to be eliminated, and if we still have pairs in the set, we compute the S-polynomial of a pair from the set NC based on the strategy proposed by Buchberger, and update the set NC. Actually, In algorithm 4.2.1 we do not give a rule for choosing the pair $\{i, j\} \in NC$, for which we compute the corresponding S-polynomial. Buchberger proposed a strategy to speed up our calculation. Often the S-polynomials are computed in such a way that $S(f_i, f_j)$ is computed first if $\mathrm{lcm}(\mathrm{lp}(f_i), \mathrm{lp}(f_j))$ is least (with respect to the current term order) among the $\mathrm{lcm}(\mathrm{lp}(f_i), \mathrm{lp}(f_j))$. This process is called the *normal selection strategy*. This strategy is used to speed up the calculation that regards the procedure to select a pair. It can be shown that if we always select a pair $\{f_i, f_j\}$ such that $\mathrm{lcm}(\mathrm{lp}(f_i), \mathrm{lp}(f_j))$ is as small as possible with respect to the chosen term ordering, then $Crit1$ and $Crit2$ are "good" in the sense that all possible reductions of $S(f_i, f_j)$ will yield zero. Finally, if the degree ordering is used, this strategy seems to lead to simpler polynomials than other possible choices.

INPUT: $F = \{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n]$
OUTPUT: *A Groebner basis* G *for* $\langle f_1, \ldots, f_s \rangle$
INITIALISATION: $G = F$
$C = \emptyset$
$NC = \{\{1, 2\}\}$
$i = 2$
WHILE $i < s$ **DO**
$NC = NC \bigcup \{\{j, i+1\} \,|\, 1 \leq j \leq i\}$
$NC = Crit2(NC, C, i+1)$
$i = i + 1$
WHILE $NC \neq \emptyset$ **DO**
choose $\{i, j\} \in NC$
$NC = NC - \{\{i, j\}\}$
$C = C \bigcup \{\{i, j\}\}$
IF $Crit1(i, j) =$ *FALSE* **THEN**
$S(f_i, f_j) \xrightarrow{G}_+ h$, *where* h *is reduced with respect to* G
IF $h \neq 0$ **THEN**
$f_{s+1} = h$
$G = G \bigcup \{f_{s+1}\}$
$s = s + 1$
$NC = NC \bigcup \{\{i, s\} \,|\, 1 \leq i \leq s - 1\}$
$NC = Crit2(NC, C, s)$

Algorithm 4.2.1. *Improved Buchberger's Algorithm[AL96]*

Proposition 4.2.1. *[AL96] Given a set of non-zero polynomials $F = \{f_1, \ldots, f_s\}$,the Improved Buchberger's Algorithm (given in Algorithm 4.2.2) will produce a Groebner basis for the ideal $I = \langle F \rangle$.*

Proof. Similar to Buchberger's Algorithm seen in the previous Chapter, we start with $F = G$ and when we compute S-polynomials the number of elements may increase. So, let us assume that we have t elements where $t \geq s$. Let $G = \{f_1, \ldots, f_t\}$ $(t \geq s$ be the output of the algorithm we have in Algorithm 4.2.1. We see that every S-polynomial corresponding to every pair in C reduces to zero. It then suffices to show that $\{\tau_{ij} | \{i, j\} \in C\}$ is a generating set for Syz(lt$(f_1), \ldots,$ lt$(f_t))$, and since at any time in the algorithm after NC has been initialised, it suffices to show that $\{\tau_{ij} \{i, j\} \in NC \bigcup C\}$ is a generating set for the syzygy module of current leading terms.

So, at each stage of the algorithm, we can have either the S-polynomial reducing to zero, and $NC \bigcup C$ doesn't change, or a polynomial being added to G. This latter option will lead to other relevant pairs being added to $NC \bigcup C$, and so that the set of τ_{ij}'s corresponding to this update $NC \bigcup C$ is a generating set for the syzygy module of the new set of leading terms. And then $Crit2$ is to be applied to the new set of NC, which will not alter this last statement, according to Corollary 4.2.1 [AL96]. □

INPUT: (NC, C, s) *from Algorithm 4.2.1*
OUTPUT: NC *with pairs deleted using Corollary 4.2.1*
INITIALISATION: $l = 1$
WHILE $l < s$
  IF $\{l, s\} \in NC$ **THEN**
    $i = 1$
    WHILE $i < s$ **DO**
      IF $\{i, l\} \in NC \bigcup C$ **AND** $\{i, s\} \in NC$ **THEN**
        IF X_l *divides lcm*(X_i, X_s) **THEN**
          $NC = NC - \{\{i, s\}\}$
      $i = i + 1$
  $l = l + 1$
$i = 1$
WHILE $i < s$ **DO**
  IF $\{i, s\} \in NC$ **THEN**
    $j = i + 1$
    WHILE $j < s$ **DO**
      IF $\{j, s\} \in NC$ **AND** $\{i, j\} \in NC$ **THEN**
        IF X_s *divides lcm*(X_i, X_j) **THEN**
          $NC = NC - \{\{i, j\}\}$
      $j = j + 1$
  $i = i + 1$

Algorithm 4.2.2. $Crit2(NC, C, s)$ *[AL96]*

Example 4.2.1. *1. Let $I = \langle x^2y + z, xz + y\rangle \subseteq \mathbb{Q}[x, y, z]$ using grlex with $x > y > z$. We need to compute the Groebner basis for the ideal I using the improved Buchberger Algorithm.*

Let $f_1 = x^2y + z$ and $f_2 = xz + y$ and $G = \{f_1, f_2\}$; $C = \emptyset$ and $NC = \{\{f_1, f_2\}\}$. Then we have $NC = Crit2(NC, C, 2) = \{\{f_1, f_2\}\}$. We need to find the S-polynomial of f_1 and f_2; $S(f_1, f_2) = -xy^2 + z^2$ and let $f_3 = -xy^2 + z^2$ which is reduced with respect to G and add it to G. Then we have $NC = \{\{1, 3\}, \{2, 3\}\}$ and $C = \{\{1, 2\}\}$. Now apply $Crit2$ but it is easy to show that no pair is eliminated from NC. We compute $S(f_1, f_3)$, and we see that $S(f_1, f_3) \xrightarrow{G}_+ 0$. We then update $NC = \{\{2, 3\}\}$, $C = \{\{1, 2\}, \{1, 3\}\}$. Then we again compute $S(f_2, f_3) = y^3 + z^3 = f_4$ which is reduced with respect to G. Then we update $NC = \{\{1, 4\}, \{2, 4\}, \{3, 4\}\}$ and $C = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$. We apply $Crit2$ to compute the new NC, and we see that for $l = 3$, the pairs $\{1, 4\}$ will be eliminated from NC since $\{1, 4\} \in NC, \{1, 3\}\, NC \bigcup C$, $\{3, 4\} \in NC$ and lp(f_3) divides lcm$(lp(f_1), lp(f_4))$. And also the pair $\{2, 4\}$ will be eliminated since $\{2, 4\} \in NC, \{2, 3\} \in NC \bigcup C$ and $\{3, 4\} \in NC$ with lp(f_3) divides lcm$(lp(f_2), lp(f_4))$. We update NC such that $NC = \{\{3, 4\}\}$ and $C = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$. When we find the S-polynomial of the pair $\{3, 4\}$, we have $S(f_3, f_4) \xrightarrow{G}_+ 0$. Finally, when we update NC such that $NC = \emptyset$. Hence, the Groebner basis $G = \{f_1, f_2, f_3, f_4\}$.

Example 4.2.2. *Consider the polynomials $f_1 = x^2y^2 - z^2$, $f_2 = xy^2z - xyz$, and $f_3 = xyz^3 - xz^2 \in \mathbb{Q}[x, y, z]$ with term order grlex such that $x < y < z$. We need to find the Groebner basis using the improved Buchberger's Algorithm. We follow Algorithm 4.2.1 and 4.2.2 with the proposed strategy, called the normal strategy, to speed up our computation in selecting pairs to compute S-polynomials.*
We start with the assumption that $G = \{f_1, f_2, f_3\}, C = \emptyset$ and $NC = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$. We have lcm(lp$(f_1)$, lp$(f_3)$) is divisible by lp$(f_2)$ which implies that we do not consider $\{1, 3\}$. Then we have $NC = Crit2(NC, C, 3) = \{\{1, 2\}, \{2, 3\}\}$.

- *Using the strategy proposed by Buchberger to choose and compute the S-polynomial from NC, we choose pair $\{1, 2\}$ and compute the S-polynomial that brings $NC = \{\{2, 3\}\}$ and $C = \{\{1, 2\}\}$ with $S(f_1, f_2) = x^2yz - z^3$ which is reduced with respect to G. Now we let $f_4 = x^2yz - z^3$ to be added to G and then NC will be updated as*
  $NC = \{\{2, 3\}, \{1, 4\}, \{2, 4\}, \{3, 4\}\}$ and $C = \{\{1, 2\}\}$

- *Apply $Crit2$ and for $l = 1$, we eliminate $\{2, 4\} \in NC$ since $\{1, 2\} \in NC \bigcup C$, $\{1, 4\}$, and lp(f_1) divides lcm(lp(f_2), lp(f_4)). But we do not have any to eliminate for $l = 2$ and $l = 3$. Then the new $NC = \{\{2, 3\}, \{1, 4\}, \{3, 4\}\}$. We choose $\{1, 4\}$ to calculate the S-polynomial by the normal selection strategy such that $S(f_1, f_4) = yz^3 - z^3$, say $f_5 = yz^3 - z^3$, which brings $NC = \{\{2, 3\}, \{3, 4\}\}$ and $C = \{\{1, 2\}, \{1, 4\}\}$. Then we update NC to include pairs of f_5 and*
  $NC = \{\{2, 3\}, \{3, 4\}, \{1, 5\}, \{2, 5\}, \{3, 5\}, \{4, 5\}\}$ and $C = \{\{1, 2\}, \{1, 4\}\}$.

- *Apply $Crit2$: for $l = 2$, we eliminate $\{1, 5\}$ since $\{1, 2\} \in NC \bigcup C, \{2, 5\} \in NC$, and lp$(f_2)$ divides lcm$(lp(f_1),$ lp$(f_5))$. For $l = 3$ we eliminate $\{2, 5\}$ since $\{2, 3\} \in NC \bigcup C, \{3, 5\} \in NC$, and lp$(f_3)$ divides lcm(lp(f_2), lp$(f_5))$ and similarly for $l = 4$ we*

eliminate $\{4,5\}$. *But we have no pair that can be eliminated for* $l = 1$. *Then we have* $NC = \{\{2,3\},\{3,4\},\{3,5\}\}$. *We apply normal selection strategy to choose* $\{3,5\}$ *and compute the S-polynomial such that* $S(f_3, f_5) = xz^3 - xz^2$, *say* $f_6 = xz^3 - xz^2$. *Then we update*
$NC = \{\{2,3\},\{3,4\},\{1,6\},\{2,6\},\{3,6\},\{4,6\},\{5,6\}\}$ *and*
$C = \{\{1,2\},\{1,4\},\{3,5\}\}$.

- *Apply* $Crit2$: *for* $l = 2$ *we eliminate* $\{1,6\}$ *since* $\{1,2\} \in NC \bigcup C$, $\{2,6\} \in NC$, *and* lp(f_2) *divides* lcm(lp(f_1), lp(f_6)). *For* $l = 3$ *we eliminate* $\{2,6\}$ *since* $\{2,3\} \in NC \bigcup C$, $\{3,6\} \in NC$, *and* lp(f_3) *divides* lcm(lp(f_2), lp(f_6)). *Using the same procedure for* $l = 3$ *we also eliminate* $\{4,6\}$ *and* $\{5,6\}$. *But for* $l = 1$ *and* $l = 5$ *we have nothing to eliminate using* $Crit2$. *Now we are left with* $NC = \{\{2,3\},\{3,4\},\{3,6\}\}$. *We apply the normal selection strategy to choose* $\{3,6\}$ *and compute the S-polynomial such that* $S(f_3, f_6) = xyz^2 - xz^2$, *say* $f_7 = xyz^2 - xz^2$. *We then update*
$NC = \{\{2,3\},\{3,4\},\{1,7\},\{2,7\},\{3,7\},\{4,7\},\{5,7\},\{6,7\}\}$ *and*
$C = \{\{1,2\},\{1,4\},\{3,5\},\{3,6\}\}$.

- *Apply* $Crit2$: *using the same procedure as we used above we can eliminate* $\{1,7\}$ *for* $l = 2$, $\{5,7\}$ *and* $\{6,7\}$ *for* $l = 3$, *and* $\{3,7\}$ *for* $l = 6$. *In addition, using the second main WHILE loop of algorithm 4.2.2 we can eliminate* $\{2,3\}$ *taking* $s = 7, i = 2$ *and* $j = 3$, *since* $\{2,7\} \in NC, \{2,3\} \in NC, \{3,7\} \in NC$ *and* lp(f_7) *divides* lcm(lp(f_2), lp(f_3)). *We also eliminate* $\{3,4\}$ *from* NC *since* $\{3,7\} \in NC$, $\{4,7\} \in NC$, *and* lp(f_7) *divides* lcm(lp(f_3), lp(f_4)). *Hence we have* $NC = \{\{2,7\},\{3,7\},\{4,7\}\}$.
Again using normal selection strategy we choose $\{4,7\}$ *to compute the S-polynomial such that* $S(f_4, f_7) = -z^4 + x^2z^2$, *say* $f_8 = -z^4 + x^2z^2$. *We then update*
$NC = \{\{2,7\},\{3,7\},\{1,8\},\{2,8\},\{3,8\},\ldots,\{7,8\}\}$ *and*
$C = \{\{1,2\},\{1,4\},\{3,5\},\{3,6\},\{4,7\}\}$.

- *Apply* $Crit2$: *we eliminate* $\{1,8\}$ *for* $l = 2$, $\{7,8\}$ *for* $l = 3$, *and* $\{3,8\}$ *for* $l = 5$. *Moreover, when* $S(f_2, f_7) \xrightarrow{G}_+ 0$ *and* $S(f_3, f_7) \xrightarrow{G}_+ 0$ *which leads us to eliminate* $\{2,7\}$ *and* $\{3,7\}$ *results* $NC = \{\{2,8\},\{4,8\},\{5,8\},\{6,8\}\}$. *Using normal selection strategy we also choose* $\{6,8\}$ *to compute the S-polynomial such that* $S(f_6, f_8) = x^3z^2 - xz^3$, *say* $f_9 = x^3z^2 - xz^3$. *We update*
$NC = \{\{2,8\},\{4,8\},\{5,8\},\{1,9\},\{2,9\},\ldots,\{8,9\}\}$ *and*
$C = \{\{1,2\},\{1,4\},\{3,5\},\{3,6\},\{4,7\},\{6,8\}\}$.

- *After applying* $Crit2$ *we have* $NC = \{\{2,8\},\{4,8\},\{4,9\},\{6,9\}\}$. *But the S-polynomial corresponding to the remaining pairs in* NC *all reduce to zero which gives* $NC = \emptyset$.
Thus $G = \{f_1, f_2, , f_3, f_4, f_5, f_6, f_7, f_8, f_9\}$ *is the Groebner basis for the ideal* $I = \langle f_1, f_2, f_3\rangle$.

We noted that the most time consuming part in finding the Groebner basis was computing the S-polynomials and their reduction. But when we apply the improved Buchberger's Algorithm of $Crit2$, we observe that the number of S-polynomials to be computed decreases, resulting in less time to compute them. For instance, in the above example we computed a total of 13 S-polynomials, 6 of which generated elements of the Groebner basis. So, if we had not been using $Crit2$, which is a powerful algorithm for improving Buchberger's Algorithm, we had to compute

$\frac{8.9}{2} = 36$ S-polynomials which is really time consuming and by far unmanageable to compute all these. Moreover, we note that the computation in $Crit2$ is trivial in the sense that we are just checking pairs and eliminating them using the two main WHILE loops of algorithm 4.2.2.

Hence, we conclude by noting that the above two main criteria proposed by Buchberger, $Crit1$ and $Crit2$, are powerful commands that optimise Buchberger's Algorithm to compute S-polynomials. In fact, empirical evidences shows that these two criteria reduce from computing N number of S-polynomials to about $\sqrt{N}$. This represents a significant improvement of the Buchberger's algorithm.

Finally, though this improved Buchberger's Algorithm is efficient in minimising the number of S-polynomials to be computed and saving time to compute the Groebner bases, the algorithm may not address the possible rapid growth of the degree and the coefficient of S-polynomials appearing for even a modest starting polynomials. Hence, a possible future extension of the project may encompass the expansion of the recently introduced algorithms, namely F_4 [Fau99] and F_5 [Fau02], in conjunction with the Buchberger's algorithm, hopefully produce a more efficient algorithm.

5. Conclusion

In this paper we reviewed in detail the improvement of Buchberger's Algorithm using the concept of syzygies. When we compute Groebner bases using the standard algorithm the number of S-polynomials increase and the degrees of the polynomials increase. These factors can make computation of the Groebner bases very complex, and sometimes unmanageable. We can rectify this by employing the improved Buchberger Algorithm based on the concept of syzygies. The improved algorithm imposes two basic basic criteria, following the normal selection strategy proposed by Buchberger, to minimize the complexity of the computation. In this paper we have reviewed the necessary theory and calculations with this algorithm. Therefore, we can see that the algorithm is indeed important for overcoming the increment of certain S-polynomials by ignoring S-polynomials of pairs from a non computed set, since their S-polynomials reduce to zero using either of the criteria.

So, we conclude that the basic criteria proposed by Buchberger really do improve Buchberger's original Algorithm, and acknowldge that the improved algorithm plays a very vital role in computing the Groebner bases.

There are, of course, further problems connected to computing the Groebner bases such as the degree and the coefficients of S-polynomials may possibly grow rapidly even for a modest original polynomials. The improved algorithm may not address these problems of computing Groebner bases. So, we need to have other algorithms in our possession. Hence, a possible future extension to this project may encompass the expansion of the newly introduced algorithms, namely F_4 [Fau99] and F_5 [Fau02], in conjunction with Buchberger's Algorithm to find a more efficient and effective algorithm that can address this difficulty in computing the Groebner bases.

Appendix A. List of Symbols

$\mathbb{N}$	natural numbers
$\mathbb{Z}$	ring of integers
$\mathbb{Z}_n$	ring of integers modulo n
$\mathbb{Q}$	field of rational numbers
k	a field
k^n	affine space
$k[x_1, \ldots, x_n]$	ring of polynomials with variables $x_1, \ldots, x_n$ and coefficients in K
$\langle f_1, \ldots, f_s \}$	ideal generated by $f_1, \ldots, f_s$
$\gcd$	greatest common divisor
lcm	least common multiple
lt(f)	leading tem of f
lp(f)	leading power product of f
lc(f)	leading coefficient of f
x^γ	$x_1^{\gamma_1} \cdots x_n^{\gamma_n}$
$f \xrightarrow{G}_+ h$	f reduces to h modulo G
$S(f, g)$	S-polynomials of f and g
$ker(\phi)$	kernel of the map ϕ
A^m	set of column vectors with entries in the ring A
M/N	quotient modulo M by$N$
$\cong$	isomorphic to
$\mathbf{e}_1, \ldots, \mathbf{e}_s$	standard basis for the free module A^m
Syz$(f_1, \ldots, f_s)$	syzygy module of a $1 \times s$ matrix $[f_1, \ldots, f_s]$

Dedication

This work is dedicated to my lovely wife Fitsum Mengistie, my mother, Feten Workineh, and all beloved sisters and brothers, specially Zelalem Ayichew.

You all are such a blessing in my life. God bless you all abundantly.

To my father,
May his soul rest in Peace.

Acknowledgement

I heartily express my profound gratitude to my supervisor, Dr. Cornelia Naude, to whom I owe a debt of gratitude for her invaluable assistance, for her availability, for the interesting discussion, and for her patience with me.

I would also like to express my sincere gratitude to all academic stuffs, Prof Fritz Hahne, Lecturers and tutors working at the African Institute for Mathematical Sciences (AIMS) for their pleasant support in any ways throughout my stay at AIMS. Specially I would like to acknowledge Paul Razafimandimby and Anahita New for their unreserved help in commenting and editing this paper. Zelalem, Balew and Gashaw, I am thankful for our wonderful time we spent at AIMS. I would also like to express my sincere appreciation to all AIMS management and all non-academic stuff for their support. Dr Sam Webster and Dr Laure Gouba, I thank you very much for your genuine help.

My special gratitude to mum and Zelalem Ayichew, whose endless support I cherish, your unconditional love, care, and encouragement always been of tremendous help. You are the best.

My heartiest appreciation also to all my siblings, and all my indebtedness and best wishes to my dear friend, Assefa Derebe, who is more than a brother to me, for all his worthful deserve. May God bless you all. I also wish to convey my grateful thanks to all my former lecturers at the department of Mathematics at the university of Bahir Dar, Ethiopia, for their unforgettable deserve.

Lastly but not the least, my darling wife, Fitsum, words really fail me on how to thank you for all your caring, giving your unreserved love, and being always with me. Sweetheart, I thank you very much for being there for me, all your patience, understanding, encouragement and most of all your love, and putting up with those long periods when I was away from home. I really love you. I know that it wasn't easy but it was worth it.

Dedication

This work is dedicated to my lovely wife Fitsum Mengistie, my mother, Feten Workineh, and all beloved sisters and brothers, specially Zelalem Ayichew.

You all are such a blessing in my life. God bless you all abundantly.

To my father,
May his soul rest in Peace.

Bibliography

[AL96] Williams W. Adams and Philippe Loustaunau, *An Introduction to Groebner Bases*, Vol.3, American Mathematical Scociety, 1996.

[Ape00] Joachim Apel, *Computational ideal theory in finitely generated extension rings*, Journal of Theoretical Computer ScienceJ **244** (2000), 1–33.

[CLO97] David Cox, John Little, and Donald O'Shea, *Ideals, Variets, and Algorithms*, Springer Science+ Bussines Media, Inc., 1997.

[Fab] Fabrizio, *Available from: http://www.geocities.com/capecanaveral/hall/3131/*, GeoCities.

[Fau99] Jean-Charles Faugere, *A new efficient algorithm for computing groebner bases (f_4)*, Journal of Pure and Applied Algebra **139** (1999), 61–88.

[Fau02] ———, *Efficient algorithm for computing groebner bases without reduction to zero(f_5), proceedings of the 2002 international symposium on symbolic and algebraic computation, ISSAC,*, ACM Press, Italy, 2002.

[fCM] RICAM(Radon Institute for Computational and Applied Mathematics), *Grbner basis implementations*, Radon Institute for Computational and Applied Mathematics(RICAM).

[GM88] R. Gebauer and H.M. Moller, *On an installation of buchberger's algorithm*, Journal of Symbolic computation **6** (1988), 275–286.

[GP02] Gert-Martin Greuel and Gerhard Pfister, *A Singular Inroduction to Commutative Algebra*, Springer-Verlag Berlin Heidelberg, 2002.

[Hun74] Thomas W. Hungerford, *Algebra*, Springer-Verlag New York Heidelberg Berlin, 1974.

[JS06] Winfried Just and Brandilyn Stigler, *Computing groebner bases of ideals of few points in high dimension*, ACM Communication in Computer Algebra **40** (2006).

[KR00] Martin Kreuzer and Lorenzo Robbiano, *Computational Commutative Algebra 1*, Springer-Verlag Berlin Heidelberg, 2000.

[MB97] Neal H. McCoy and Thomas R. Berger, *Algebra: Groups, Rings, and Other topics*, Allyn and Bacon, Inc, 1997.

[MMF01] H. M. Moller, F. Moreau, and Jean-Charles Faugere, *New constructive methods in classical ideal theory*, Transactions of American Methematical Society **353** (2001), 2293–2308.

[Sha90] R. Y. Sharp, *Steps in Computational Algebra*, Springer-Verlag Berlin Heidelberg, 1990.