Muhammad Imran

Gröbner Bases for Decoding Linear Codes

Master Thesis

Thesis Advisor: Prof. S.J. Edixhoven

A thesis presented for the degree of
Master of Science

Date Master Examination: August 05, 2019
Mathematisch Instituut
Universiteit Leiden

Abstract

Gröbner bases are special sets of generators of ideals in multivariate polynomial rings, which provide some powerful theoretical and computational properties for solving problems in many fields such as coding theory, cryptanalysis, optimization, geometric modelling, some problems in control theory, robotics, and statistics.
One of the main ingredients in the construction of Gröbner bases is monomial orderings. In fact, monomial orderings have crucial role which determines the complexity of the computation of Gröbner bases. Different monomial orderings will lead to different levels of complexity in the computation process of a Gröbner basis. The first part of this thesis is devoted to discuss the well-known classification of monomial orderings by Robiano, which represents a monomial ordering on the set of monomials of a multivariate polynomial ring by a certain set of orthogonal vectors in $\mathbb{R}^n$. Furthermore, we give an explicit bijection between the set of all monomial orderings and such family of orthogonal vectors that enables us to construct a monomial ordering from such set of orthogonal vectors and vice versa.
The first algorithm for computing Gröbner bases was formulated by Buchberger. The core of this algorithm is the concept of S-polynomials of pairs of polynomials. However, the major disadvantage of this algorithm is the amount of useless pairs of polynomials that the algorithm has to compute. Hence, the second part of this thesis is devoted to discuss the concept of Gröbner bases and Buchberger's algorithm. Furthermore, we describe some strategies to optimize the computations of Gröbner bases.
The last part of this thesis is devoted for the application of Gröbner bases in decoding problems. We describe how Gröbner bases get involved in solving decoding problems, especially for linear codes. Particularly, we discuss how to translate decoding problems of linear codes into the problem of solving system of multivariate polynomial equations.

Acknowledgements

It is a great pleasure for me to thank those who have helped and encouraged me throughout the long process, that was full of struggle, of completing my master course and finishing my master thesis.

First and foremost, I am wholeheartedly thankful to Prof. Bas Edixhoven for his great supervision, encouragement, guidance and support from the very first I was accepted in this program until he become my thesis supervisor. I appreciate all his contributions of time, ideas, and suggestions to make my study experience in this university more exciting and valuable.

The next, I owe my deepest gratitude to my whole family, especially my mother and my father, who have raised me with love, knowledge, and prayers and who always support me in all my pursuits. There are no suitable words that can fully describe their everlasting love to me.

I would like to thank my other family, Student Association of Indonesia and my fellow Indonesian students, who have made my stay in Leiden so fun and unforgettable. Among them there are Pararawendy Indarjo, Ramadhan Iskandar, and Noly Cristino, who helped me out in my adaptation period here. There are also Rahmat Latif, Ikhwan Dawam, Rumaisha Annida, Tasia Amelia, Aninda Wibowo, Firda Juhairiyah, and Meily Setiawati who showed me how to enjoy the last year of my study.

Using this chance I also would like to thank to all lectures at the group "Algebra, Geometry and Number Theory" for teaching me useful subjects during my study. Among them there are, Dr. David Holmes who is also my study advisor, Prof. Bart de Smit, Prof. Peter Stevenhagen, Dr. Roland van der Veen, Dr. Marco Streng, Dr. Martin Bright and Dr. Peter Bruin.

Last but not least, I would like to express my huge gratitude to the Government of Republic of Indonesia who have empowered me to pursue and finish my study in this world-class university. Without the Lembaga Pengelola Dana Pendidikan (Indonesian Endowment Fund for Education) Scholarship that you hosted, It would not possible for me to achieve all my precious experiences to live and study here.

Contents

Chapter 1

Introduction

1.1 What is a Gröbner Basis

Let I be an ideal of a polynomial ring. A Gröbner basis of the ideal I is a certain set of generators for I which provides some special theoretical and computational properties. In fact, many practical problems in various fields can be solved by Gröbner bases such as decoding problems, cryptanalysis, optimization, geometric modelling, some problems in control theory, robotics, and statistics. The basic idea is translating such problems into polynomial ideals language and then reducing the problems into problems of solving system of polynomial equations or the ideal membership problem. Technically speaking, by applying multivariate division algorithm, any polynomial f has a unique remainder with respect to a Gröbner basis of I. Moreover, any polynomial f in I reduces to zero with respect to a Gröbner basis of I. The basic idea of computing Gröbner bases is based on the divison algorithm, hence in the case of polynomial rings with more than one variable we need multivariate division algorithm which leads us to the notion of monomial orderings. Distinct monomial orderings give different levels of complexity in the computation process of a Gröbner basis.

The notion of Gröbner bases was introduced by Bruno Buchberger during his Ph.D thesis [7] under the supervision of Wolfgang Gröbner, in 1965. Moreover, he formulated an algorithm to compute such bases as well as a proof for the fundamental theorem on which the correctness and termination of the algorithm depends on. Intensive researches in Gröbner bases theory, related algorithms and applications have been developing since then. Nowadays, Gröbner bases becomes one of the important tools in computer algebra. Many computer algebra systems like Maculay2, Magma, Maple, Mathematica, Singular, or Sage have implemented various versions of Buchberger's algorithm. The importance of this concept and the algorithm of computing it is related to the fact that we have a systematic way for computing generators of any ideal. Moreover, most of recent algorithms for computing such bases are still based on Buchberger's algorithm.

1.2 Thesis Overview

In this thesis, we would like to see how monomials ordering are classified which have significant roles in the construction of Gröbner bases, and then discuss some properties of Gröbner bases and how to compute such bases efficiently, and lastly dive in one of the applications of Gröbner bases, particularly, we will discuss in details how the problem of decoding linear codes can be translated into a system of polynomials which can be solved by computing its Gröbner basis.

This thesis is structured into four chapters. In chapter 2: first, we recall some definitions and properties in order theory for multivariate polynomial rings. Then we discuss the classifications of monomial orderings by Lorenzo Robiano, which represents a monomial ordering on the set of monomials of a multivariate polynomial ring by a certain set of orthogonal vectors in $\mathbb{R}^n$, and we give some examples, in the case of polynomial rings with two variables, to describe how such monomial orderings flow on $\mathbb{N}^2$ and divide $\mathbb{Q}^2$ on xy-plane into three parts, i.e., positive, zero and negative part. Moreover, in the last part of the chapter we give an explicit bijection between the set of all monomial orderings and such family of orthogonal vectors that enables us to construct a monomial orderings from such set of orthogonal vectors and vice versa.

In chapter 3: we bring the reader into the notion of Gröbner bases. First, we recall some definitions and properties of multivariate division with respect to a fixed monomial ordering that we need and we give a multivariate division procedure to obtain a unique remainder with respect to the procedure which will be helpful in Buchberger's algorithm. Then, we recall the formal definition of Gröbner bases, its properties and all details of how to construct them. Then, we recall the notion of weight vector from Bernd Sturmfels which will be helpful to optimize the computation of a Gröbner basis. Lastly, we describe various ways to optimize the computational performance of a Gröbner basis, followed by some examples in practice.

In chapter 4: we discuss the application of Gröbner bases in decoding linear codes. First, we recall some definitions and properties of linear codes and one particular class of linear codes, namely cyclic codes, which have special algebraic properties. Then we present some methods of how to translate cyclic codes and linear codes in general into a system of polynomial equations, followed by the application of Gröbner bases in solving decoding problems by using ideals generated by these translations. Lastly, we give some examples to describe these methods in practice.

Chapter 2

Order Theory

2.1 Monomial Ordering

In this chapter we discuss different ways to order the monomials of a polynomial ring. This is needed in order to set up a division algorithm in the case of several variables. A monomial in a polynomial ring $R = \mathbb{F}[x_1, \ldots, x_n]$ over a field $\mathbb{F}$ is a product of the form $x^a = x_1^{a_1} \cdots x_n^{a_n}$ with $a = (a_1, \ldots, a_n) \in \mathbb{N}^n$. We write $\mathrm{Mon}(x)$ for the set of all monomials in R. Firstly, we observe the polynomial ring $\mathbb{F}[x]$ in one variable x over a field $\mathbb{F}$. By Euclidean division algorithm, we have that $\mathbb{F}[x]$ is a principal ideal domain. The most important thing in Euclidean division algorithm is the term of degree of a polynomial, so for every polynomial $f \in \mathbb{F}[x]$ we can rearrange monomials in f in unambiguously descending (or ascending) order with respect to the degree of its monomials. Therefore, we would like to apply this method in polynomial rings with more variables, hence we need to know how we order monomials in polynomial rings over a field with more variables. The definition of a monomial ordering is given below to allow us to do the arrangement.

Definition 2.1.1. A monomial ordering on $R = \mathbb{F}[x_1, \ldots, x_n]$ is a relation $\prec$ on $\mathrm{Mon}(x)$ such that

(a) $\prec$ is a total ordering on $\mathrm{Mon}(x)$, i.e., any two monomials x^a and x^b, we have either $x^a \prec x^b$ or $x^a = x^b$ or $x^b \prec x^a$;

(b) $\prec$ is multiplicative, i.e., for fixed $x^a, x^b \in \mathrm{Mon}(x)$ and for all $x^c \in \mathrm{Mon}(x)$, we have
$$x^a \prec x^b \iff x^a x^c \prec x^b x^c;$$

(c) For all $x^a \in \mathrm{Mon}(x)$ we have $1 \preceq x^a$.

Remark.

- For condition (a): we need this condition in order to rearrange the monomials in a polynomial in unambiguously descending (or ascending) order.

- For condition (b): we need this condition to avoid the effect of the product operation on polynomials. In other words the leading monomial of fg could be different from the product of leading monomials f and g with $f, g \in R$.

Notice that we have a bijection from $\mathrm{Mon}(x)$ onto $\mathbb{N}^n$ via

$$x^a \mapsto a = (a_1, \ldots, a_n).$$

So we can consider a monomial ordering as a non-negative total ordering on $\mathbb{N}^n$ and hence we call $(\mathbb{N}^n, \prec)$ totally ordered non-negative semigroup.

The next lemma shows that the definition of monomial orderings can also be stated in another equivalent way in which we replace the non-negativity property by the well-ordering property, i.e., any nonempty subset of $\mathbb{N}^n$ has a minimal element or equivalently any strictly descending sequence in $\mathbb{N}^n$ terminates. We need this condition in order to have a terminating division algorithm on multivariate polynomial rings.

Lemma 2.1.2. Let $\prec$ be an ordering on $\mathbb{N}^n$ satisfying the following properties:

1. It is a total ordering;
2. It is additive, i.e., for any $a, b, c \in \mathbb{N}^n$ we have
$$a \prec b \iff a + c \prec b + c;$$
3. For all $a \in \mathbb{N}^n$ we have $0 \preceq a$.

Then $\prec$ is a well-ordering.

Proof. Now we prove this lemma by induction on n. Let $n = 1$ and $\prec$ be an ordering on $\mathbb{N}$ satisfying the conditions above. From property 3, we have $0 \prec 1$, and hence from property 2, the only ordering on $\mathbb{N}$ satisfying the properties above is the usual ordering and hence any nonempty subset of $\mathbb{N}$ has a unique minimal element.

Suppose that any ordering on $\mathbb{N}^{n-1}$ satisfying the properties above is a well-ordering. Now let $\prec_n$ be an ordering on $\mathbb{N}^n$ satisfying the properties above and let S be any nonempty subset of $\mathbb{N}^n$. Consider the ordering $\prec_{n-1}$ on $\mathbb{N}^{n-1}$ given by $a = (a_1, \ldots, a_{n-1}) \prec_{n-1} (b_1, \ldots, b_{n-1}) = b$ if and only if $(a_1, \ldots, a_{n-1}, 0) = (a, 0) \prec_n (b_1, \ldots, b_{n-1}, 0) = (b, 0)$ in $\mathbb{N}^n$. Therefore,

- Since $\prec_n$ is a total ordering, any two distinct elements a and b in $\mathbb{N}^{n-1}$, we have either
$$(a, 0) \prec_n (b, 0) \text{ or } (b, 0) \prec_n (a, 0).$$
- For any $a, b, c \in \mathbb{N}^{n-1}$ we have $a \prec_{n-1} b \iff (a, 0) \prec_n (b, 0)$ and also
$$(a, 0) \prec_n (b, 0) \iff (a, 0) + (c, 0) \prec_n (b, 0) + (c, 0).$$
So $a \prec_{n-1} b \iff a + c \prec_{n-1} b + c$.

- For all $a \in \mathbb{N}^{n-1}$ we have $0 \preceq_{n-1} a$, since $0 \preceq_n (a, 0)$.

Therefore the ordering $\prec_{n-1}$ is a well-ordering.

Now consider the set

$$S_1 := \{(a_1, \ldots, a_{n-1}) \in \mathbb{N}^{n-1} \,|\exists\, a_n \in \mathbb{N} \text{ such that } (a_1, \ldots, a_n) \in S\}.$$

By induction hypothesis, S_1 has a unique minimal element with respect to the ordering $\prec_{n-1}$ on $\mathbb{N}^{n-1}$. Let $a = (a_1, \ldots, a_{n-1})$ be the minimal element of S_1. Let $a_n \in \mathbb{N}$ be smallest natural number such that $a' = (a_1, \ldots, a_{n-1}, a_n) \in S$. We claim that for any $b = (b_1, \ldots, b_n) \in S$ with $b_n \geq a_n$ we have $a' \prec_n b$. Indeed, since $(a_1 \ldots, a_{n-1}, 0) \prec_n (b_1, \ldots, b_{n-1}, 0)$, then $(a_1 \ldots, a_{n-1}, b_n) \prec_n (b_1, \ldots, b_{n-1}, b_n)$. On the other hands, since we have $0 \prec_n (0, \ldots, 0, b_n - a_n)$, then $a' \prec_n (a_1, \ldots, a_{n-1}, b_n)$ and hence the claim follows.

Therefore, it is left to consider all elements $b \in S$ where its last coordinate less than a_n. Now For each $0 \leq b_n < a_n$ we have

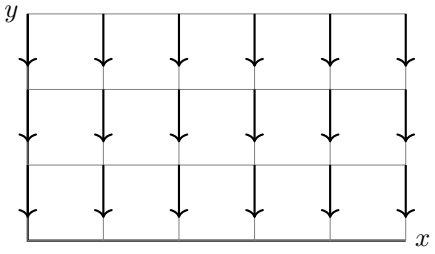
$$S_{b_n} := \{(b_1, \ldots, b_{n-1}) \in \mathbb{N}^{n-1} \,|(b_1, \ldots, b_{n-1}, b_n) \in S\}.$$

Hence again by induction hypothesis, we have a unique minimal element for each S_{b_n}. Therefore, by adding b_n as the last coordinate in the unique minimal element of each set S_{b_n} we have a finite subset S' of S containing a' and all those elements. By the total order property of $\prec_n$ and the finiteness of S', we have a unique minimal element $c = (c_1, \ldots, c_n)$ of S'. We claim that the minimal element of S' is the minimal element of S. Indeed, since any element c of S has last coordinate either $c_n < a_n$ or $a_n \leq c_n$, thus if $a_n \leq c_n$ then $a' \prec_n c$ and if $c_n < a_n$ then c is contained in one of the set S_{b_n}. □

There are some well-known monomial orderings which have been used frequently in computation, some of them are provided below.

Examples of Monomial Ordering:

(1) Lexicographic Order is the ordering $\prec_{lex}$ on $\mathbb{N}^n$ such that for $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ elements in $\mathbb{N}^n$, we have $a \prec_{lex} b$ if and only if the leftmost nonzero coordinate in the difference $b - a \in \mathbb{Z}^n$ is positive. The picture below shows how elements in $\mathbb{N}^2$ are ordered:



Note that:

$\forall m \in \mathbb{N} : (0, m) \prec_{lex} (1, 0)$;

$(1, m) \prec_{lex} (2, 0)$;

$\vdots$

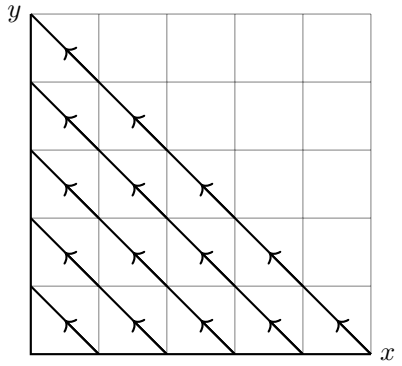
etc.

Figure 1.1

(2) Graded Lexicographic Order is the ordering $\prec$ on $\mathbb{N}^n$ such that for $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ elements in $\mathbb{N}^n$, we have $a \prec b$ if and only if either:

- $|a| = a_1 + a_2 + \cdots + a_n < |b| = b_1 + \cdots + b_n$ or
- $|a| = |b|$ and the leftmost nonzero coordinate in the difference $b - a$ is positive.

The picture below shows how elements in $\mathbb{N}^2$ are ordered:



Note that:
$\forall m, n \in \mathbb{N} : (m, 1-m) \prec (n, 2-n)$;
$(m, 2-m) \prec (n, 3-n)$;
$\vdots$
etc.

Figure 1.2

(3) Block Ordering or Product Ordering. Let $\prec_1$ be an ordering on $\mathbb{N}^j$ and $\prec_2$ be an ordering on $\mathbb{N}^k$ satisfying definition 2.1.1. The block ordering on $\mathbb{N}^n$ with $n = j + k$ is defined as follows: $(a_1, \ldots, a_j, a_{j+1}, \ldots, a_{j+k}) \prec_3 (b_1, \ldots, b_j, b_{j+1}, \ldots, b_{j+k})$ if and only if either:

- $(a_1, \ldots, a_j) \prec_1 (b_1, \ldots, b_j)$ or
- $(a_1, \ldots, a_j) = (b_1, \ldots, b_j)$ and $(a_{j+1}, \ldots, a_{j+k}) \prec_2 (b_{j+1}, \ldots, b_{j+k})$.

(4) Elimination Ordering. Let $\prec$ be an ordering on $\mathbb{N}^{j+k}$, where j and k are nonzero natural numbers with $j + k = n$. The ordering $\prec$ is called an elimination ordering for j, if and only if any element a in $\mathbb{N}^{j+k}$ with nonzero for at least one coordinate in the first j coordinates is greater than any element b in $\mathbb{N}^{j+k}$ with zero at all the first j coordinates. It is easy to verify that such block orderings are elimination orderings.

Definition 2.1.3. An ordering $\prec$ on a commutative group G means an ordering $\prec$ on G such that $(G, \prec)$ is totally ordered group.

The next two lemmas show how a total ordering $\prec$ on the semigroup $\mathbb{N}^n$ extends uniquely on $\mathbb{Z}^n$ such that $(\mathbb{Z}^n, \prec)$ is a totally ordered group and hence extends uniquely on $\mathbb{Q}^n$ such that $(\mathbb{Q}^n, \prec)$ is totally ordered group in which we have more special structure, i.e., we may embed $\mathbb{Q}^n$ into $\mathbb{R}^n$ on which we have the usual inner product and the induced Euclidean topology.

Lemma 2.1.4. Let $\prec$ be a total ordering on $\mathbb{N}^n$ such that $(\mathbb{N}^n, \prec)$ is a totally ordered non-negative semigroup. Then $\prec$ extends uniquely on $\mathbb{Z}^n$ such that $(\mathbb{Z}^n, \prec)$ is a totally ordered group.

Proof. Let $a, b \in \mathbb{Z}^n$ be distinct elements, we say $a \prec b$ if and only if there exists an element $c \in \mathbb{N}^n$ such that $a + c, b + c \in \mathbb{N}^n$ and $a + c \prec b + c$. If $a, b \in \mathbb{N}^n$, then we may choose c to be the zero vector and the order of $a + c = a$ and $b + c = b$ does not change, so $\prec$ extends on $\mathbb{Z}^n$. Moreover, its extension is unique, otherwise there exist $c, c' \in \mathbb{N}^n$ such that $a + c, b + c, a + c', b + c'$ are all in $\mathbb{N}^n$ and satisfying:

$$a + c \prec b + c \text{ and } b + c' \prec a + c'$$

on $\mathbb{N}^n$ and by the property (b) in the definition 2.1.1, we have

$$a + (c + c') \prec b + (c + c') \text{ and } b + (c + c') \prec a + (c + c')$$

which contradicts $\prec$ as a total ordering on $\mathbb{N}^n$. Now it is left to show that its extension is a total ordering on $\mathbb{Z}^n$. Let $a, b, c \in \mathbb{Z}^n$:

- (Antisymmetry): If $a \preceq b$ and $b \preceq a$, then there exist $d, d' \in \mathbb{N}^n$ such that $a+d, b+d, a+d', b+d'$ are all in $\mathbb{N}^n$ and satisfying $a+d \preceq b+d$ and $b+d' \preceq a + d'$. So by the property (b) in the definition 2.1.1, we have

  $$a + (d + d') \preceq b + (d + d') \text{ and } b + (d + d') \preceq a + (d + d').$$

  Since $\prec$ is a total ordering on $\mathbb{N}^n$, we have $a = b$.

- (Transitivity): If $a \prec b$ and $b \prec c$, then there exist $d, d' \in \mathbb{N}^n$ such that $a+d, b+d, b+d', c+d'$ are all in $\mathbb{N}^n$ and satisfying $a+d \prec b+d$ and $b+d' \prec c + d'$. Again by the property (b) in the definition 2.1.1, we have

  $$a + (d + d') \prec b + (d + d') \text{ and } b + (d + d') \prec c + (d + d').$$

  Hence we have $a + (d + d') \prec c + (d + d')$ and $a \prec c$.

- (Connexity): Since for any $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ elements in $\mathbb{Z}^n$, we can always find an element $c \in \mathbb{N}^n$ such that $a + c$ and $b + c$ are in $\mathbb{N}^n$ for example by taking $c = (c_1, \ldots, c_n)$ where $c_i = \max\{|a_i|, |b_i|\}$. So any two elements in $\mathbb{Z}^n$ are comparable.

□

Lemma 2.1.5. Let $\prec$ be a total ordering on $\mathbb{Z}^n$ such that $(\mathbb{Z}^n, \prec)$ is a totally ordered group. Then $\prec$ extends uniquely on $\mathbb{Q}^n$ such that $(\mathbb{Q}^n, \prec)$ is also a totally ordered group.

Proof. Let $a, b \in \mathbb{Q}^n$ be distinct elements, we say $a \prec b$ if and only if there exists $r \in \mathbb{N}^+$ such that ra and rb are in $\mathbb{Z}^n$ and satisfying $ra \prec rb$ in $\mathbb{Z}^n$. If $a, b \in \mathbb{Z}^n$, then we may choose $r = 1$ and the order of $1 \cdot a = a$ and $1 \cdot b = b$ does

not change, so $\prec$ extends on $\mathbb{Q}^n$. Moreover, its extension is unique, otherwise there exists $r, r' \in \mathbb{N}^+$ such that $ra, rb, r'a, r'b$ are all in $\mathbb{Z}^n$ and satisfying:

$$ra \prec rb \text{ and } r'b \prec r'a$$

on $\mathbb{Z}^n$ and since $(\mathbb{Z}^n, \prec)$ is totally ordered group, i.e., $\prec$ is translation-invariant, we have $rr'a \prec rr'b$ and $rr'b \prec rr'a$ which contradicts $\prec$ as a total ordering on $\mathbb{Z}^n$. Now it is left to show that its extension is a total ordering on $\mathbb{Q}^n$. Let $a, b, c \in \mathbb{Q}^n$:

- (Antisymmetry): If $a \preceq b$ and $b \preceq a$, then there exist $r, r' \in \mathbb{N}^+$ such that $ra, rb, r'a, r'b$ are all in $\mathbb{Z}^n$ and satisfying $ra \preceq rb$ and $r'b \preceq r'a$. Since $(\mathbb{Z}^n, \prec)$ is a totally ordered group, i.e., $\prec$ is translation-invariant, thus $rr'a \preceq rr'b$ and $rr'b \preceq rr'a$. Therefore, since $\prec$ is a total ordering on $\mathbb{Z}^n$ we have $rr'a = rr'b$ and hence $a = b$.

- (Transitivity): If $a \prec b$ and $b \prec c$, then there exist $r, r' \in \mathbb{N}^+$ such that $ra, rb, r'b, r'c$ are all in $\mathbb{Z}^n$ and satisfying $ra \prec rb$ and $r'b \prec r'c$. Again since $\prec$ is translation-invariant, we have $rr'a \prec rr'b$ and $rr'b \prec rr'c$ and hence $rr'a \prec rr'c$. So we have $a \prec c$.

- (Connexity): Since for any $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ elements in $\mathbb{Q}^n$, we always can find an element $r \in \mathbb{N}^+$ such that ra and rb are in $\mathbb{Z}^n$ for example by taking r equal to the lowest common multiple of all denominators of all coordinates of a and b. So any two elements in $\mathbb{Q}^n$ are comparable.

□

2.2 Representation of Monomial Orderings

Now we are going to classify all orderings on $\mathbb{N}^n$ satisfying definition 2.1.1 and represent each of monomial orderings as a set of orthogonal vectors which satisfies some given properties. The classification of monomial orderings in this section is mostly based on Robiano in [26], but we provide an explicit map which enables us to see the bijection between the set of all monomial orderings of a polynomial ring and such sets of orthogonal vectors. To simplify, firstly we see the case step by step on $n = 1$ and $n = 2$:

The case $n = 1$. We have seen in the proof of Lemma 2.1.2 that the only ordering on $\mathbb{N}$ satisfying definition 2.1.1 is the usual ordering.

The case with $n = 2$. We have more interesting things to observe in this case because we look at all orderings $\prec$ on the set $\mathbb{N}^2$ satisfying definition 2.1.1. From lemma 2.1.4 and 2.1.5 we may use its extension on $\mathbb{Q}^2$ such that $(\mathbb{Q}^2, \prec)$ is a totally ordered group and we embed $\mathbb{Q}^2$ into $\mathbb{R}^2$ and then examining the orderings we have above.

- The lexicographic ordering: Let $a = (a_1, a_2)$ and $b = (b_1, b_2) \in \mathbb{Q}^2$. Then $a \prec_{lex} b$ if and only if $((a_1 < b_1)$ or $(a_1 = b_1$ and $a_2 < b_2))$. So we can choose a vector $v = (1, 0)$ and $u = (0, 1)$ to describe the above conditions by using the inner product $\langle , \rangle$ in $\mathbb{R}^2$ as follows: $a \prec_{lex} b$ if and only if $((\langle v, a\rangle < \langle v, b\rangle)$ or $(\langle v, a\rangle = \langle v, b\rangle$ and $\langle u, a\rangle < \langle u, b\rangle))$. The picture below shows how these two orthogonal vectors divide the $\mathbb{Q}^2$ into three parts: positive, negative and the zero.

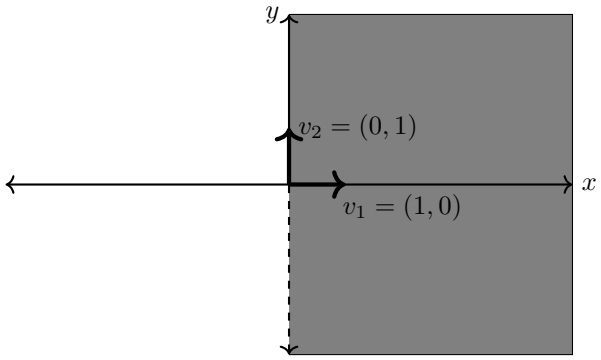


Figure 1.3

The subset of $\mathbb{Q}^2$ on the gray area of the xy-plane is the positive part of $\mathbb{Q}^2$ with respect to the lexicographic ordering given above where the dashed $y-$axis is excluded. While the subset of $\mathbb{Q}^2$ on the other area on the plane excluding the zero vector is the negative part.

- The graded lexicographic ordering: Let $a = (a_1, a_2)$ and $b = (b_1, b_2) \in \mathbb{Q}^2$. Then $a \prec b$ if and only if $((a_1 + a_2 < b_1 + b_2)$ or $(a_1 + a_2 = b_1 + b_2$ and $a_1 < b_1))$. So we can choose a vector $v = (1, 1)$ and $u = (1, -1)$ to describe the above conditions by using the inner product $\langle , \rangle$ in $\mathbb{R}^2$ as follows: $a \prec b$ if and only if $((\langle v, a\rangle < \langle v, b\rangle)$ or $(\langle v, a\rangle = \langle v, b\rangle$ and $\langle u, a\rangle < \langle u, b\rangle))$. The picture below shows how these two orthogonal vectors divide $\mathbb{Q}^2$ into three parts: positive, negative and the zero.

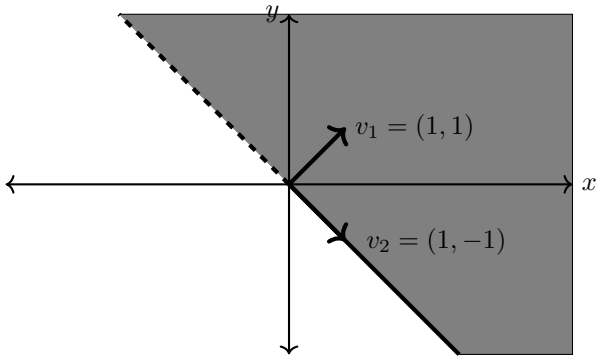


Figure 1.4

The subset of $\mathbb{Q}^2$ on the gray area of the xy-plane is the positive part of $\mathbb{Q}^2$ with respect to the graded lexicographic ordering given above where the dashed line orthogonal to the vector $v_1 = (1, 1)$ is excluded. While the subset of $\mathbb{Q}^2$ on the other area on the plane excluding the zero vector is the negative part.

Therefore, from two examples above we may expect that for any ordering on $\mathbb{N}^n$, we can find at most n (we can find less than n in some cases) orthogonal vectors on $\mathbb{R}^n$ and by using the inner product on $\mathbb{R}^n$ we can describe the ordering. The following we give an example of an ordering on $\mathbb{N}^2$ on which we need only one vector to describe the ordering.

Consider the quadratic field extension $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ of $\mathbb{Q}$, and we have $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}^2$ are isomorphic as $\mathbb{Q}$-vector spaces via $(a, b) \mapsto a + b\sqrt{2}$. Hence we can define an ordering on $\mathbb{N}^2$ as follows: $(a, b) \prec (c, d)$ if and only if $a+b\sqrt{2} < c+d\sqrt{2}$ in $\mathbb{R}$. Hence we need only to choose the vector $(1, \sqrt{2}) \in \mathbb{R}^2$ to describe the ordering on $\mathbb{N}^2$ above. The picture below shows how this vector divides $\mathbb{Q}^2$ into three parts: positive, negative and the zero.

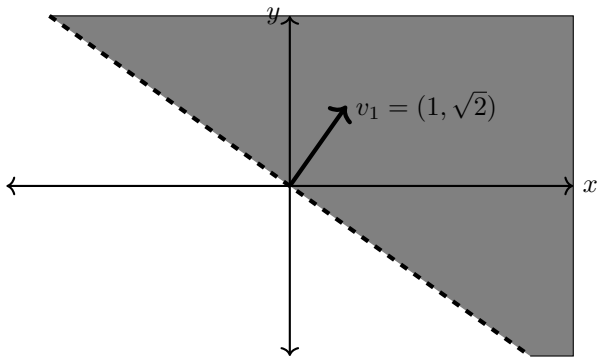


Figure 1.5

The subset of $\mathbb{Q}^2$ on the gray area of the xy-plane is the positive part of $\mathbb{Q}^2$ with respect to the ordering given above. While the subset of $\mathbb{Q}^2$ on the other area on the plane excluding the zero vector is the negative part. The interesting thing happens in this case where we do not need the second vector orthogonal to v_1. The reason is the only element in $\mathbb{Q}^2$ on the line orthogonal to v_1 is the zero vector.

Proposition 2.2.1. Any positive irrational number determines a monomial ordering.

Proof. Let r be any irrational number and $v = (1, \ldots, 1, r) \in \mathbb{R}^n$. For any $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ vectors in $\mathbb{N}^n$, we say $a \prec b$ if and only if $\langle v, a\rangle < \langle v, b\rangle$. Since the usual ordering $<$ on the set of real number satisfies definition 2.1.1, then $\prec$ is a monomial ordering. □

Proposition 2.2.2. Any two distinct positive irrational numbers give two distinct monomial orderings.

Proof. Let r and s be any two distinct irrational numbers. Then there exists a rational number $\frac{p}{q}$ such that $r < \frac{p}{q} < s$. Let $v = (1, \ldots, 1, r)$ and $w = (1, \ldots, 1, s)$. Then for the two vectors $p' = (p, 0, \ldots, 0)$ and $q' = (0, \ldots, 0, q)$ we have

$$\langle v, q' \rangle < \langle v, p' \rangle, \text{ but } \langle w, p' \rangle < \langle w, q' \rangle.$$

Hence any two irrational numbers give two distinct monomial orderings. □

The rest of this section will study the classification of all monomial orderings and the translation of all monomial orderings into vectors as we have done in the three previous examples.

Let $\prec$ be an ordering on $\mathbb{Q}^n$ satisfying definition 2.1.3, and we embed $\mathbb{Q}^n$ into $\mathbb{R}^n$ as previous. Let r be a positive integer and let V be a $\mathbb{Q}$-subvectorspace of $\mathbb{Q}^n$ of dimension r and we denote $V \otimes \mathbb{R}$ the $\mathbb{R}$-subvectorspace of $\mathbb{R}^n$ by $V_{\mathbb{R}}$. By restricting the ordering $\prec$ on V, we denote V^+ and V^- as the positive part and the negative part of V respectively.

Lemma 2.2.3. Let $I = \overline{V^+} \cap \overline{V^-}$ where $\overline{V^+}$ and $\overline{V^-}$ are the closure of V^+ and the closure of V^+ in $V_{\mathbb{R}}$ respectively. Then I is a subvectorspace of $V_{\mathbb{R}}$ of dimension $r - 1$.

Proof. Since any two vector spaces of the same dimension over a field are isomorphic, it is sufficient to show this for $V = \mathbb{Q}^r$. Firstly, we show that I is a $\mathbb{Q}$-subvectorspace of $V_{\mathbb{R}}$. If $\lambda \in \mathbb{Q}_{>0}$, then $\lambda \cdot V^+ = V^+$ and $\lambda \cdot V^- = V^-$ and hence for any $v \in I$ we have $\lambda \cdot v \in I$. If $\lambda \in \mathbb{Q}_{<0}$, then $\lambda \cdot V^+ = V^-$ and $\lambda \cdot V^- = V^+$ and hence for any $v \in I$ we have $\lambda \cdot v \in I$. Now it is left to show that I is closed under addition. So let $v, w \in I$. Since v and w are inside $\overline{V^+}$ and also inside $\overline{V^-}$, there exist $(v_m^+)_{m\geq 0}, (w_m^+)_{m\geq 0}$ in V^+ converging to v and w respectively and also there exist $(v_m^-)_{m\geq 0}, (w_m^-)_{m\geq 0}$ in V^- converging to v and w respectively. Then $(v_m^+ + w_m^+)_{m\geq 0}$ converges to $v + w$ and for all $m \geq 0$ we have $v_m^+ + w_m^+ \in V^+$. The same kind of argument for $(v_m^- + w_m^-)_{m\geq 0}$, the limit is $v + w$ and for all $m \geq 0$ we have $v_m^- + w_m^- \in V^-$. So $v + w \in I$ and hence I is a $\mathbb{Q}$-subvectorspace of $V_{\mathbb{R}}$. Moreover, as multiplication by a real number is continuous, I is closed in $V_{\mathbb{R}}$ and any real number can be approximated by rational numbers, I is closed under scalar multiplication in $\mathbb{R}$ and hence I is $\mathbb{R}-$subvectorspace of $V_{\mathbb{R}}$.

Now it is left to show that $\dim_{\mathbb{R}}(I) = r-1$. Since $V_{\mathbb{R}} - I = (\overline{V^+} - I) \cup (\overline{V^-} - I)$ where $\overline{V^+} - I$ and $\overline{V^-} - I$ are open and disjoint, so $V_{\mathbb{R}} - I$ is disconnected. Let m be a positive integer such that $dim_{\mathbb{R}}(I) = m$. Since any two vector spaces of the same dimension over a field are isomorphic, then $V_{\mathbb{R}} \cong \mathbb{R}^r$ and hence $I \cong \mathbb{R}^m \times \{0\}$. Thus we have

$$V_{\mathbb{R}} - I \cong \mathbb{R}^r - \mathbb{R}^m \times \{0\} = \mathbb{R}^m \times \mathbb{R}^{r-m} - \mathbb{R}^m \times \{0\} = \mathbb{R}^m \times (\mathbb{R}^{r-m} - \{0\})$$

and hence this excludes the possibility $m < r - 1$ otherwise $\mathbb{R}^{r-m} - \{0\}$ is connected and so is $V_{\mathbb{R}} - I$. Furthermore, since V is a totally ordered group we may choose a basis $\{e_1, \ldots, e_r\}$ as a $\mathbb{Q}$-subvectorspace such that $\{e_1, \ldots, e_r\} \subset V^+$. Therefore $e_1 + \cdots + e_r \in V^+$ but it is not inside I since by taking a small

enough open neighbourhood U of $e_1 + \cdots + e_r$, any element of U has positive coordinates. Then we could not have $\dim I = r$. □

Now some definitions stated below are used to classify all monomial orderings on a polynomial ring.

Definition 2.2.4. Let $\prec$ be an ordering on V as before. Then we denote by $H(V)$ the half-line orthogonal to I and contained in $\overline{V^+}$.

Definition 2.2.5. Given a vector $v \in \mathbb{R}^n$, we denote by $d(v)$ the dimension of the $\mathbb{Q}$-subvectorspace of $\mathbb{R}$ spanned by the coordinates of v and we call it the rational dimension of v.

Lemma 2.2.6. Let V and $V_{\mathbb{R}}$ be as before. Let $v \in V_{\mathbb{R}}$. Then $d(v) \leq r = \dim_{\mathbb{Q}} V$.

Proof. Let $v_1, \ldots, v_r$ be a basis of V. Let $v \in V_{\mathbb{R}}$ be any vector and we write as $\sum \lambda_i v_i$ with $\lambda_i \in \mathbb{R}$. Then the vector space over $\mathbb{Q}$ spanned by the coordinates of v is contained in the vector space spanned by $\{\lambda_1, \ldots, \lambda_r\}$. □

Definition 2.2.7. Let $d \in \{1, \ldots, n\}$, we denote by $A(d)$ the quotient set $B(d)/\sim$, where $B(d)$ is the set of all vectors $v \in \mathbb{R}^n$ such that $d(v) = d$ and $\sim$ is the equivalence relation given by $v \sim v'$ if and only if there exists $\lambda \in \mathbb{R}_{>0}$ with $v = \lambda v'$.

Now by using previous definitions, the classification of all monomial orderings on a polynomial ring $R = \mathbb{F}[x_1, \ldots, x_n]$ is given in the following theorem.

Theorem 2.2.8. Let $\mathrm{Ord}(R)$ be the set of all monomial orderings on $\mathrm{Mon}(x)$, the set of monomials in R. Then there is a bijection, given explicitly in the proof below, from $\mathrm{Ord}(R)$ onto the set M defined by

$$\left\{ (t, \rho, u) \;\middle|\; \begin{array}{c} 1 \leq t \leq n, \rho \text{ is a partition of } n \text{ in } t \text{ parts,} \\ \text{and } u = (u_1, \ldots, u_t) \in A(d_1) \times \cdots \times A(d_t) \end{array} \right\}$$

in which

(a) for every $i = 1, \ldots, t-1$, if V_i is the $\mathbb{Q}-$subvectorspace of $\mathbb{Q}^n$ of the vectors orthogonal to $\{u_1, \ldots, u_i\}$, then $u_{i+1} \in V_{i\,\mathbb{R}} = V_i \otimes \mathbb{R}$.

(b) for every $v \in \mathbb{N}^n \setminus \{0\}$, the first non-zero coordinate of $(v \cdot u_1, \ldots, v \cdot u_t)$ is positive.

Proof. Let $\{u_1, \ldots, u_s\}$ is given as above. Then we can construct a monomial ordering on R or equivalently on $\mathbb{N}^n$ with respect to this set of orthogonal vectors as follows: Let $a, b \in \mathbb{N}^n$. Then

$$a \prec b \iff (a \cdot u_1, \ldots, a \cdot u_t) \prec_{lex} (b \cdot u_1, \ldots, b \cdot u_t)$$

where $a \cdot u_i$ is the usual dot product in $\mathbb{R}^n$. Clearly the construction above defines a map from M into $\mathrm{Ord}(R)$ and we claim that the map is surjective. Let

$\prec$ be a monomial ordering on $\mathbb{N}^n$. From lemma 2.1.4 and lemma 2.1.5 we may extend this ordering on $\mathbb{Q}^n$, and hence by embedding $V = \mathbb{Q}^n$ in $V_{\mathbb{R}} = \mathbb{R}^n$ we have I, the $(n-1)-$dimensional $\mathbb{R}$-subvectorspace of $\mathbb{R}^n$, and we have the half-line $H(V)$. Take $u_1 \in H(V)$ and denote d_1 as its rational dimension. Moreover, we denote by V_1 the $\mathbb{Q}-$subvectorspace of $\mathbb{Q}^n$ defined by $V_1 = I \cap \mathbb{Q}^n$. Since $V_1^{\perp} = (I \cap \mathbb{Q}^n)^{\perp} \cong \mathbb{Q}^{d_1}$, $\dim V_1 = n - d_1$ and for every $v \in \mathbb{Q}^n \setminus V_1$, we have $v > 0$ if and only if $v \cdot u_1 > 0$ (as a real number). Hence it is left for us to consider all vectors in V_1. By the same steps as previous we have $(V_1)_{\mathbb{R}} = V_1 \otimes_{\mathbb{Q}} \mathbb{R}$ and the $\mathbb{R}$-vector space I_{V_1} and a vector $u_2 \in H(V_1)$ with $d(u_2) = d_2 \leq n - d_1$. Since the rational dimensions are positive integers then this procedure ends after a finite number of steps and we eventually get the integer t, the partition of n into $\{d_1, \ldots, d_t\}$, and the vectors $u_1, \ldots, u_t$ which satisfy the given properties above. Moreover, the injectivity follows from the constructions of $(u_1, \ldots, u_t)$ above. Indeed, from the proof of the surjectivity of this map, any monomial ordering $\prec$ produces unique $u_1 \in A(d_1)$ as I is of $n-1$ dimensional subspace and hence its orthogonal space is one dimensional space, so by the equivalence class in $A(d_1)$, u_1 is unique. Therefore, the map is injective and hence bijective. $\square$

Corollary 2.2.9. Let $\prec$ be an ordering on $\mathbb{N}^n$ satisfying the properties in 2.1.1. Then there exists a natural number s with $1 \leq s \leq n$ and an $s \times n$ matrix M with real entries such that for any $v, v' \in \mathbb{N}^n$, $v \prec v'$ if and only if $v \cdot M \prec_{lex} v' \cdot M$ on $\mathbb{R}^s$.

Chapter 3

Gröbner Bases

3.1 Multivariate Division

Recall that a polynomial ring over a field with one variable is a principal ideal domain and hence we have an Euclidean division algorithm. By observing the division algorithm on a polynomial ring over a field with one variable we see that we use the term of degree of polynomials to do the algorithm, therefore the same steps we want to apply on any polynomial ring over a field with n variables to get a multivariate division method. By fixing a monomial ordering $\prec$ on the set of monomials in $R = \mathbb{F}[x_1, \ldots, x_n]$ for a fixed field $\mathbb{F}$, it leads us to give the following definitions:

Definition 3.1.1. Let $f = \sum_a c_a x^a$ be a polynomial, we denote $\mathrm{Mon}(f) := \{x^a : c_a \neq 0\}$. Suppose that x^a is the greatest element of $\mathrm{Mon}(f)$ with respect to the monomial ordering $\prec$, then x^a is called the leading monomial of f and denoted by $\mathrm{lm}_\prec(f)$, the coefficient c_a of x^a is called the leading coefficient of f and $\mathrm{lt}_\prec(f) = c_a x^a$ is called the leading term of f.

As we see on the remarks of definition 2.1.1, we need condition b in order to guarantee that for any $f, g \in R$ we have $\mathrm{lm}_\prec(fg) = \mathrm{lm}_\prec(f)\mathrm{lm}_\prec(g)$. Therefore, the lemma below shows this and also gives the effect on the addition of polynomials.

Lemma 3.1.2. Let $f_1, \ldots, f_r$ be nonzero polynomials in R such that $f_1 + \cdots + f_r$ is also nonzero. Then

(i) $\mathrm{lm}_\prec(f_1 \ldots f_r) = \mathrm{lm}_\prec(f_1) \cdots \mathrm{lm}_\prec(f_r)$

(ii) $\mathrm{lm}_\prec(f_1 + \cdots + f_r) \preceq \max\{\mathrm{lm}_\prec(f_1), \ldots, \mathrm{lm}_\prec(f_r)\}$. Moreover, let c_j be the leading coefficient of f_j. The equality holds if and only if the sum taken over c_j for which $\mathrm{lm}_\prec(f_j) \succeq \mathrm{lm}_\prec(f_i)$ for all $1 \leq i \leq r$ is nonzero.

Proof.

(i) By definition, we have $\mathrm{lm}_\prec(f_1)\cdots\mathrm{lm}_\prec(f_r) \succeq u_1u_2\cdots u_r$ for all $u_i \in \mathrm{Mon}(f_i)$ and since all monomials in $\mathrm{Mon}(f_1\cdots f_r)$ are of the form $u_1\cdots u_r$ with $u_i \in \mathrm{Mon}(f_i)$ and since $\mathrm{lm}_\prec(f_1)\cdots\mathrm{lm}_\prec(f_r) \in \mathrm{Mon}(f_1\cdots f_r)$ thus the equality holds if and only if $u_i = \mathrm{lm}_\prec(f_i)$ for all $i = 1,\ldots,r$.

(ii) Note that $\mathrm{Mon}(f_1+\cdots+f_r) \subseteq \bigcup_{i=1}^r \mathrm{Mon}(f_i)$. Therefore, we have

$$\mathrm{lm}_\prec(f_1+\cdots+f_r) \preceq \max\{u | u \in \bigcup_{i=1}^r \mathrm{Mon}(f_i)\}$$

$$\mathrm{lm}_\prec(f_1+\cdots+f_r) \preceq \max\{\mathrm{lm}_\prec(f_1),\ldots,\mathrm{lm}_\prec(f_r)\}.$$

Now let $u = \max\{\mathrm{lm}_\prec(f_1),\ldots,\mathrm{lm}_\prec(f_r)\}$ and suppose that $\sum_j^r c_j \neq 0$, where the sum is taken over those j such that $\mathrm{lm}_\prec(f_j) = u$. Thus it follows that $u \in \mathrm{Mon}(f_1+\cdots+f_r)$ and hence

$$\mathrm{lm}_\prec(f_1+\cdots+f_r) \succeq u = \max\{\mathrm{lm}_\prec(f_1),\ldots,\mathrm{lm}_\prec(f_r)\}.$$

Thus the equality holds.

Conversely, if $\sum_j^r c_j = 0$, then $u \notin \mathrm{Mon}(f_1+\cdots+f_r)$ and hence

$$\mathrm{lm}_\prec(f_1+\cdots+f_r) \neq \max\{\mathrm{lm}_\prec(f_1),\ldots,\mathrm{lm}_\prec(f_r)\}.$$

□

Let $G = \{g_1,\ldots,g_m\}$ be a finite subset of $R = \mathbb{F}[x_1,\ldots,x_n]$ and let $f \in R$ be any polynomial. We say that f is reducible by G if there exists an element $u \in \mathrm{Mon}(f)$ which is divisible by $\mathrm{lm}_\prec(g_i)$ for some i with $1 \leq i \leq m$.

Now suppose that f is reducible by G. Then such element u exists, and we may reduce f into $f - \frac{c\cdot u}{\mathrm{lt}_\prec(g_i)}g_i$ where c is the coefficient of u in f. Therefore, the procedure cancels the term $c \cdot u$ in f and by keep doing this we can see whether f is a linear combination of elements of G or not. Hence it leads us to the following proposition.

Proposition 3.1.3. Let f and $g_1,\ldots,g_m$ be polynomials in R with g_i are nonzero polynomials for $1 \leq i \leq m$. Then there exists polynomials $h_1,\ldots,h_m$ and a polynomial r in R such that $f = g_1h_1+\cdots+g_mh_m+r$ and no element of $\mathrm{Mon}(r)$ is contained in the ideal $\langle \mathrm{lm}_\prec(g_1),\ldots,\mathrm{lm}_\prec(g_m)\rangle$.

Proof. By fixing a monomial ordering $\prec$, we can perform the reduction process as previously described on the biggest element of $u \in \mathrm{Mon}(f)$ which is divisible by $\mathrm{lm}_\prec(g_i)$ for some i with $1 \leq i \leq m$. So we have the reduced form of f is $f - \frac{c\cdot u}{\mathrm{lt}_\prec(g_i)}g_i$ where c is the coefficient of u in f and we can perform again the reduction process on the biggest element of $\mathrm{Mon}(f - \frac{c\cdot u}{\mathrm{lt}_\prec(g_i)}g_i)$ and continued the previous procedures. Clearly this process terminates somehow by the well-ordering property of $\prec$ and we end up either with 0 or a remainder r of f by G. Therefore, the existence of such polynomials $h_1,\ldots,h_m$ and r is guaranteed. □

This remainder r of f by a finite set G is, in general, not unique as it depends on the order of reductions as the following example demonstrate. Let $\prec$ be the lexicographic ordering with $x \prec y$ on $\mathbb{Q}[x, y]$ and let $f = xy + y$, $g_1 = x + 1$, and $g_2 = x$. Then

$$f = yg_1 \text{ as well as } f = yg_2 + y.$$

In the first case we have the remainder of f is 0, but in the other one its remainder is y. Hence we say f reduces to zero by a finite set $G = \{g_1, \ldots, g_m\}$ if it has a remainder with respect to G, which is zero.

Let G be a finite subset of $R = \mathbb{F}[x_1, \ldots, x_n]$ with cardinality m for some field $\mathbb{F}$. In order to get a unique remainder r of a polynomial f by G, we proceed the reduction process as follows:

1. Take m-tuple $(g_1, \ldots, g_m)$ of nonzero distinct elements of G;
2. Take the greatest element $x^a \in \mathrm{Mon}(f)$ with respect to $\prec$ which is divisible by some $\mathrm{lm}_\prec(g_i)$ with $1 \leq i \leq m$. If there is no such element x^a, then $r := f$;
3. Let $g_j \in G$ be the element such that $\mathrm{lm}_\prec(g_j)$ divides x^a and x^a is not divisible by any $\mathrm{lm}_\prec(g_i)$ for $i < j$, then take new $f := f - \frac{c_a x^a}{\mathrm{lt}_\prec(g_j)} g_j$, where c_a is the coefficient of x^a;
4. Back to step 2;

Therefore, by the above procedure, we obtain a unique remainder of f by any tuple of nonzero distinct elements in R and we denote the remainder of f by G under the above procedure with respect to $\prec$ as $\mathrm{Rem}_{(G,\prec)}(f)$. Hence if we apply the above procedure on the previous example $f = xy + y$, $g_1 = x + 1$, and $g_2 = x$ with respect to $x \prec_{lex} y$, then we have $\mathrm{Rem}_{(G,\prec)}(f) = 0$.

3.2 The Notion of Gröbner Bases and Buchberger's Algorithm

Now we are ready to give a definition of a Gröbner basis of an ideal of a polynomial ring over a fixed field $\mathbb{F}$ with respect to a fixed monomial ordering $\prec$. This is a nice set of generators, because a reduction of a polynomial by this set always leads to a unique remainder. Firstly, we fix a monomial ordering $\prec$ on $\mathrm{Mon}(x) \subset \mathbb{R}$.

Definition 3.2.1. Let $I \subset R$ be an ideal. The set of leading monomials of I is the set $\{\mathrm{lm}_\prec(f) : f \in I\}$ with respect to $\prec$. The ideal generated by this set is called the leading monomial ideal of I with respect to $\prec$ and it is denoted by $\mathrm{lm}_\prec(I)$.

Definition 3.2.2. Let $I \subset R = \mathbb{F}[x_1, \ldots, x_n]$ be an ideal. A finite subset $\{g_1, \ldots, g_m\} \subset I$ is a Gröbner basis of I with respect to $\prec$ if and only if $\mathrm{lm}_\prec(I) = \langle \mathrm{lm}_\prec(g_1), \ldots, \mathrm{lm}_\prec(g_m) \rangle$.

Remark. A finite subset G of I is a Gröbner basis if and only if for all $f \in I$ there exists $g \in G$ such that $\mathrm{lm}_\prec(g)$ divides $\mathrm{lm}_\prec(f)$.

The next theorem shows that every ideal of a polynomial ring has a Gröbner basis and that any Gröbner basis of I generates I.

Theorem 3.2.3. Every ideal I in $R = \mathbb{F}[x_1, \ldots, x_n]$ has a Gröbner basis $\{g_1, \ldots, g_m\}$. Moreover, $I = \langle g_1, \ldots, g_m \rangle$.

Proof. Let I be an ideal in R and $\mathrm{lm}_\prec(I)$ is the ideal of its leading monomials. Then by Hilbert's basis theorem $\mathrm{lm}_\prec(I)$ is generated by a finite subset of $\mathrm{lm}_\prec(I)$, i.e., $\mathrm{lm}_\prec(I) = \langle x^{a(1)}, \ldots, x^{a(m)} \rangle$. Therefore, there exist $g_1, ..., g_k \in I$ such that $\mathrm{lm}_\prec(g_i) = x^{a(i)}$ for all $i = 1, \ldots, m$. Now we are going to show that $I = \langle g_1, \ldots, g_m \rangle$. Clearly, $\langle g_1, \ldots, g_m \rangle \subset I$ since every $g_i \in I$. Conversely, let $f \in I$ be any polynomial. By proposition 3.1.3, we can write $f = g_1 h_1 + \cdots + g_m h_m + r$ where $h_i, r \in R$ and there is no element in $\mathrm{Mon}(r)$ divisible by any $\mathrm{lm}_\prec(g_1), \ldots, \mathrm{lm}_\prec(g_m)$. We claim that $r = 0$. Indeed, otherwise $r = f - g_1 h_1 - \cdots - g_m h_m \neq 0$ and $\mathrm{lm}_\prec(r) \in \mathrm{lm}_\prec(I)$. Then there exist $q_1, \ldots, q_m \in R$ such that $\mathrm{lm}_\prec(r) = \sum_{i=1}^{m} q_i x^{a(i)}$ and hence there exists i with $1 \leq i \leq m$ on which $\mathrm{lm}_\prec(r)$ is a monomial in $f_i x^{a(i)}$. So $\mathrm{lm}_\prec(r)$ is divisible by some $x^{a(i)} = \mathrm{lm}_\prec(g_i)$. This contradicts proposition 3.1.3. □

We have introduced the notion of elimination ordering in section 2. By using an elimination ordering we have a powerful property of Gröbner bases that we can use to solve systems of multivariate polynomial equations.

Proposition 3.2.4. Let I be an ideal in $R = \mathbb{F}[x_1, \ldots, x_n]$ and G be a Gröbner basis of I with respect to an elimination ordering $\prec$. Then $G \cap \mathbb{F}[x_1, \ldots, x_i]$ is a Gröbner basis of the ideal $I \cap \mathbb{F}[x_1, \ldots, x_i]$ with respect to the induced ordering on $\mathbb{F}[x_1, \ldots, x_i]$.

Proof. Let $G = \{g_1, \ldots, g_m\}$ with g_i's are distinct. Assume that $G \cap \mathbb{F}[x_1, \ldots, x_i] = \{g_1, \ldots, g_s\}$, then $\mathrm{lm}_\prec(g_j) \notin \mathbb{F}[x_1, \ldots, x_i]$ for all $s < j \leq m$. Now we show that $\langle \mathrm{lm}_\prec(g_1), \ldots, \mathrm{lm}_\prec(g_s) \rangle = \mathrm{lm}_\prec(\langle G_i \rangle)$ where $G_i = G \cap \mathbb{F}[x_1, \ldots, x_i]$.

Let $f \in I$ be a nonzero polynomial. Then $\mathrm{lm}_\prec(f) \in \mathrm{lm}_\prec(I)$ and $\mathrm{lm}_\prec(f)$ is a monomial in the first i-th variables. Hence $\mathrm{lm}_\prec(f)$ is divisible by some $\mathrm{lm}_\prec(g_j)$ for $j \leq s$. Therefore, $\mathrm{lm}_\prec(\langle G_i \rangle) \subseteq \langle \mathrm{lm}_\prec(g_1), \ldots, \mathrm{lm}_\prec(g_s) \rangle$. Because it is obvious that $\langle \mathrm{lm}_\prec(g_1), \ldots, \mathrm{lm}_\prec(g_s) \rangle \subseteq \mathrm{lm}_\prec(\langle G_i \rangle)$, then the result follows. □

Now if we apply a Gröbner basis in proposition 3.1.3, it gives us the results below.

Proposition 3.2.5. Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis for an ideal $I \subset R = \mathbb{F}[x_1 \ldots, x_n]$ and let $f \in I$ be a nonzero polynomial. Then there exists a unique $r \in R$ satisfying:

- No element of $\mathrm{Mon}(r)$ is divisible by any of $\mathrm{lm}_\prec(g_1), \ldots, \mathrm{lm}_\prec(g_m)$;
- There is a $g \in I$ such that $f = g + r$.

This r is the remainder of f by G, we denote by $\mathrm{NF}_{(G,\prec)}(f)$ and it is also called the normal form of f with respect to G.

Proof. From proposition 3.1.3 and theorem 3.2.3, it is left to show that r is unique. Let $f = g + r$ and $f = g' + s$ be two expressions we have after reducing f by G. Since g and g' are in I, then $r - s = g' - g \in I$. Suppose that $r - s \neq 0$. Then $\mathrm{lm}_\prec(r - s) \in \mathrm{lm}_\prec(I) = \langle \mathrm{lm}_\prec(g_1), \ldots, \mathrm{lm}_\prec(g_m) \rangle$, however, no elements of $\mathrm{Mon}(r)$ and $\mathrm{Mon}(s)$ which are divisible by any $\mathrm{lm}_\prec(g_i)$, so it is a contradiction. □

Corollary 3.2.6. Let $I \subset R$ be an ideal and $G = \{g_1, \ldots, g_m\}$ is a finite set of generators of I. Then G is a Gröbner basis of I if and only if for every $f \in I$ we have $f = h_1 g_1 + \cdots + h_m g_m$ for some polynomials $h_i \in R$ such that $\mathrm{lm}_\prec(f) \succeq \mathrm{lm}_\prec(h_i g_i)$ for all $i = 1, \ldots, m$.

Therefore, by using a Gröbner basis of an Ideal $I \subset R = \mathbb{F}[x_1, \ldots, x_n]$, we have a method to check the membership problem of the ideal I as follows.

Corollary 3.2.7. Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis for an ideal $I \subset R$ with respect to the monomial ordering $\prec$ and let $f \in R$ be a polynomial. Then $f \in I$ if and only if the normal form r of f with respect to G is zero.

Note that a Gröbner basis of an ideal $I \subset R$ is not uniquely determined. For example to any Gröbner basis G of I one could add a few more elements of I to G and would obtain another Gröbner basis. But by some additional conditions, a Gröbner basis can be unique. Therefore, we call the unique Gröbner basis of I as reduced Gröbner basis. Before we give the definition of a reduced Gröbner basis, we state the following lemma which will help us to construct a reduced Gröbner basis.

Lemma 3.2.8. Let G be a Gröbner basis of an ideal $I \subset R$. Let f be a polynomial in G such that $\mathrm{lm}_\prec(f) \in \mathrm{lm}_\prec(G \backslash \{f\})$. Then $G \backslash \{f\}$ is also a Gröbner basis for I.

Proof. Since $\mathrm{lm}_\prec(f) \in \mathrm{lm}_\prec(G \backslash \{f\})$ and we have $\mathrm{lm}_\prec(I) = \mathrm{lm}_\prec(G)$, thus it follows that $\mathrm{lm}_\prec(G \backslash \{f\}) = \mathrm{lm}_\prec(G) = \mathrm{lm}_\prec(I)$. □

Therefore a Gröbner basis G of I is called minimal if there is no $f \in G$ with $\mathrm{lm}_\prec(f) \in \mathrm{lm}_\prec(G \backslash \{f\})$.

Definition 3.2.9. Let $I \subset R = \mathbb{F}[x_1, \ldots, x_n]$ be an ideal. Then $G = \{g_1, \ldots, g_m\}$ is reduced Gröbner basis of I, if G is a Gröbner basis for I and satisfying the following conditions:

- The leading coefficient of each g_i is 1;
- For all $i \neq j$, there is no element $u \in \mathrm{Mon}(g_i)$ is divisible by $\mathrm{lm}_\prec(g_j)$.

Theorem 3.2.10. Each ideal $I \subset A$ has a unique reduced Gröbner basis.

Proof. Let $\mathrm{lm}_\prec(I) = \langle u_1, \ldots, u_m \rangle$ and $G = \{g_1, \ldots, g_m\}$ be a finite subset of I such that $\mathrm{lm}_\prec(g_i) = u_i$, then G is a Gröbner basis for I. By lemma 3.2.8 we may assume that G is minimal and by proposition 3.1.3 we may write each $g_i = \sum_{j \neq i} q_j g_j + h_i$, then we have the normal form h_i of each g_i with respect to $G \backslash \{g_i\}$. Therefore, there is no $m_i \in \mathrm{Mon}(h_i)$ which is divisible by $\mathrm{lm}_\prec(g_j)$ for $j \neq i$.

We have $\mathrm{lm}_\prec(g_i) \succeq \mathrm{lm}_\prec(q_j g_j)$ for $i \neq j$. Suppose that $\mathrm{lm}_\prec(g_i) = \mathrm{lm}_\prec(q_j g_j)$ for some j. Then $u_i = \mathrm{lm}_\prec(g_i) = \mathrm{lm}_\prec(q_j) u_j$, which is impossible as G is a minimal Gröbner basis of I. Hence from lemma 3.1.2, we have $\mathrm{lm}_\prec(h_i) = \mathrm{lm}_\prec(g_i) = u_i$ for all i. Therefore by dividing all leading coefficients of all h_i such that all of its leading coefficients are 1, then $H = \{h_1, \ldots, h_m\}$ is a reduced Gröbner basis.

Now it is left to show the uniqueness. Let H and H' be two reduced Gröbner bases for I. Then we have $\mathrm{lm}_\prec(H) = \mathrm{lm}_\prec(H')$ and hence for any $h \in H$ there exists $h' \in H'$ with $\mathrm{lm}_\prec(h) = \mathrm{lm}_\prec(h')$. So we are going to show that $h = h'$. Since $h, h' \in I$, then $h - h' \in I$ and hence $h - h'$ reduces to zero by H. But also we have $\mathrm{lm}_\prec(h) = \mathrm{lm}_\prec(h')$ so these terms cancel in $h - h'$ and the remaining term is not divisible by any element in $\mathrm{lm}_\prec(H) = \mathrm{lm}_\prec(H')$ since both H and H' are reduced. Therefore, this shows that the normal form of $h - h'$ with respect to H is again $h - h'$ and hence $h - h' = 0$. This completes the proof. □

Once the reduced Gröbner basis can be computed, we can decide whether two ideals are equal as they are equal if and only if they have the same reduced Gröbner basis.

So far we only know the existence from theorem 3.2.3 and the usefulness of of such Gröbner bases from corollary 3.2.7. However, the proof of theorem 3.2.3 is not constructive and offers us little insight of how actually to obtain such basis. Therefore, Buchberger constructed a special polynomial to derive a criterion which allows us to answer this question in a finite number of steps.

Definition 3.2.11. Let f and g be nonzero polynomials in $R = \mathbb{F}[x_1, \ldots, x_n]$. The S−polynomial of f and g is defined as

$$\mathrm{S}(f, g) = \frac{x^c}{\mathrm{lt}_\prec(f)} \cdot f - \frac{x^c}{\mathrm{lt}_\prec(g)} \cdot g$$

where $x^c = lcm(\mathrm{lm}_\prec(f), \mathrm{lm}_\prec(g))$. Note that S stands for "syzygy".

Example 3.2.1. Let $I = \langle f, g \rangle$ with $f = xyz - y, g = x^2 y - yz \in \mathbb{Q}[x, y, z]$ and let $\prec$ be the graded lexicographic order with $z \prec y \prec x$. Then

$$\mathrm{S}(f, g) = x \cdot f - z \cdot g = yz^2 - xy.$$

By using the concept of S-polynomial, the following theorem tells us how to see whether a set of generators of an ideal I is a Gröbner basis or not and also the theorem is followed by an algorithm how to compute such Gröbner basis.

Theorem 3.2.12 (Buchberger's Criterion)**.** Let I be an ideal in R. Then $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis for I if and only if for all pairs $i \neq j$, the normal form of $\mathrm{S}(g_i, g_j)$ with respect to G is zero.

Algorithm 1: Buchberger's Algorithm:

Data: A finite set of generators $F = \{f_1, \ldots, f_m\}$ of an ideal I and a monomial ordering $\prec$.

Result: A Gröbner basis G for the ideal I with respect to $\prec$.

```
i := 0;
G_i := F
repeat
    G_{i+1} := G_i ∪ {Rem_{(G_i,≺)}(S(f,g)) ≠ 0 | f, g ∈ G_i}
    i := i + 1;
until G_{i+1} = G_i
Return: G = G_i is a Gröbner basis for I.
```

This algorithm ends in a finite number of steps. Indeed, each time we add a nonzero remainder $\mathrm{Rem}_{(G_i,\prec)}(\mathrm{S}(f,g))$ of an S−polynomial to G_i, the ideal $\langle \mathrm{lm}_\prec(g) : g \in G_i \rangle$ becomes strictly larger and while we repeat the algorithm we have an ascending chain condition because $R = \mathbb{F}[x_1 \ldots, x_n]$ is a Noetherian ring.

Example 3.2.2. Let I be the ideal of $\mathbb{Q}[x, y, z]$ generated by $f = xyz - y$ and $g = x^2y - yz$. Let $G_0 = \{f, g\}$ and let $\prec$ be the graded lexicographic order with $z \prec y \prec x$. From example 3.2.1 we have $\mathrm{S}(f, g) = yz^2 - xy$, and the normal form of $\mathrm{S}(f, g)$ is $\mathrm{NF}_{(G_0,\prec)}(\mathrm{S}(f, g)) = yz^2 - xy \neq 0$. So we add $h = \mathrm{NF}_{(G_0,\prec)}(\mathrm{S}(f, g))$ as an element of new set of generators $G_1 = \{f, g, h\}$. Next we repeat the previous process on G_1:

$$\mathrm{S}(f, h) = g, \text{ and we get } \mathrm{NF}_{(G_1,\prec)}(\mathrm{S}(f, h)) = 0$$

$$\mathrm{S}(g, h) = x \cdot g - z \cdot h = x^3y - yz^3, \text{ and we get } \mathrm{NF}_{(G_1,\prec)}(\mathrm{S}(g, h)) = 0.$$

Hence by Buchberger's criterion in theorem 3.2.12 we have G_1 is a Gröbner basis of the ideal I.

The Gröbner basis is determined by choice of a monomial ordering. The choice of a monomial ordering affects the process of reduction and influence the complexity of Buchberger's algorithm. The following examples shows different monomial orderings give various complexity of Buchberger's algorithm.

Example 3.2.3. Let I be the ideal in $\mathbb{Q}[x, y]$ generated by $f = xy + y^2$ and $g = xy^2 + x^2y + x^2$. Then by using Buchberger's algorithm , we obtain a Gröbner basis $G = \{f, -x^2, -y^3\}$ of I with respect to the lexicographic order with $y \prec x$. On the other hands, if we use the lexicographic order with $x \prec y$, we obtain $G = \{f, -x^2\}$ as a Gröbner basis for I.

Now we denote $\mathrm{Ord}(x)$ the set of all possible monomial orderings on $\mathrm{Mon}(x)$. Furthermore, let $I \subset R = \mathbb{F}[x_1, \ldots, x_n]$ be an ideal. We say that two monomial ordering $\prec_1$ and $\prec_2$ in $\mathrm{Ord}(x)$ are equivalent over the ideal I if and only if $\mathrm{lm}_{\prec_1}(I)$ the ideal of leading monomials of I with respect to $\prec_1$ equals to $\mathrm{lm}_{\prec_2}(I)$ the ideal of leading monomials of I with respect to $\prec_2$. Therefore, V. Ene and J. Herzog, in [15], give the following result.

Proposition 3.2.13. Let I be an ideal in R. The set

$$\mathrm{Ord}(I) := \{lm_{\prec}(I) |\ \prec \in \mathrm{Ord}(x)\}$$

is finite.

Proof. Suppose that the set $\mathrm{Ord}(I)$ is infinite. Let $f_1 \in I$ be a nonzero polynomial. Then for any ideal $J \in \mathrm{Ord}(I)$ there exists $u_1 \in \mathrm{Mon}(f_1)$ such that $u_1 \in J$. Since the set $\mathrm{Mon}(f_1)$ is finite, thus there exists $u_1 \in \mathrm{Mon}(f_1)$ such that the set $S_1 := \{J \in \mathrm{Ord}(I) | u_1 \in J\}$ is infinite. In particular, there exists at least one $J \in S_1$ with $J \neq \langle u_1 \rangle$ and hence from theorem 2.16, monomials which do not belong to $\langle u_1 \rangle$ are linearly dependent modulo I. Therefore, there exists $f_2 \in I$ with $\mathrm{Mon}(f_2) \cap \langle u_1 \rangle = \emptyset$. Moreover, we can repeat previous steps, there exists $u_2 \in \mathrm{Mon}(f_2)$ such that the set $S_2 := \{J \in \mathrm{Ord}(I) | u_2 \in J\}$ is infinite. Since $u_2 \notin \langle u_1 \rangle$, then $\langle u_1 \rangle$ is strictly contained in $\langle u_1, u_2 \rangle$. Again since S_2 is infinite thus there exists $J \in S_2$ with $J \neq \langle u_1, u_2 \rangle$ and so we can construct u_3 as before. By doing the procedures above we have an infinite ascending chain of ideals of $R = \mathbb{F}[x_1, \ldots, x_n]$

$$\langle u_1 \rangle \subset \langle u_1, u_2 \rangle \subset \langle u_1, u_2, u_3 \rangle \subset \ldots.$$

Hence this contradicts the result from commutative algebra that R is a Noetherian ring. □

Therefore, the finiteness of the set $\mathrm{Ord}(I)$ guarantees that we can vary monomials ordering we use in Buchberger's algorithm and it still terminates. Moreover, in [19] P.Gritzmann and B.Sturmfels proved that for any ideal $I = \langle f_1, \ldots, f_m \rangle \subset A$ the set $\mathrm{Ord}(I)$ is in one to one correspondence with the vertices of the affine Newton polytope of the set $\{f_1, \ldots, f_m\}$.

3.3 Weight Vector of Ideals

We have seen that we can correspond a monomial ordering to a set of orthogonal vectors in the previous chapter. However, in case of Gröbner basis, we work mostly with ideals I of a polynomial ring, so in this section we restrict the discussion of representation of monomial orderings on ideals of a polynomial ring instead of the whole polynomial ring. B.Sturmfels also gave a classification of monomial orderings in [28] by using vectors. But instead of describing the set of orthogonal vectors like in the previous section, he showed that for a particular ideal I of a polynomial ring there exists a single vector which describes the monomial ordering on that ideal which is called as weight vector. In the next chapter, in fact, the main role of monomial orderings is as the main tool to find a certain set of generators of an ideal. Therefore, it makes sense to only look how a monomial ordering works on an ideal instead of on the whole polynomial ring.

Definition 3.3.1. Let $v \in \mathbb{R}^n$ be a real vector with non negative entries and $\prec$ be an arbitrary monomial ordering on $\mathrm{Mon}(x) \subset R = \mathbb{F}[x_1, \ldots, x_n]$ for some field $\mathbb{F}$. We define a new ordering $\prec_v$ on $\mathrm{Mon}(x)$ as follows: For any $x^a, x^b \in \mathrm{Mon}(x)$, we say $x^a \prec_v x^b$ if and only if $\langle v, a\rangle < \langle v, b\rangle$ or $\langle v, a\rangle = \langle v, b\rangle$ and $x^a \prec x^b$.

Proposition 3.3.2. Let $\prec$ be an arbitrary monomial ordering and $v \in \mathbb{R}^n$ with non negative entries. Then $\prec_v$ is a monomial ordering.

Proof. This follows directly from the assumption that $\prec$ is a monomial ordering and the fact that for any two vectors $a, b \in \mathbb{N}^n$ we have either $\langle v, a\rangle < \langle v, b\rangle$, $\langle v, a\rangle > \langle v, b\rangle$ or $\langle v, a\rangle = \langle v, b\rangle$. □

Since the preposition above shows that for suitable vector v we have a monomial ordering $\prec_v$, it leads us to the following definitions.

Definition 3.3.3. Let $v \in \mathbb{R}^n$. For any polynomial $f = \sum_a c_a x^a \in R = \mathbb{F}[x_1, \ldots, x_n]$ for some field $\mathbb{F}$ we define the leading form $\mathrm{lm}_v(f)$ of f with respect to the vector v to be the sum of all monomials $C_a x^a$ for which $\langle v, a\rangle$ is maximal in the set $\{\langle v, a\rangle | x^a \in \mathrm{Mon}(f)\}$.

Definition 3.3.4. Let I be an ideal in R and $v \in \mathbb{R}^n$. Then we define the leading form ideal $\mathrm{lm}_v(I)$ of I with respect to the vector v as the ideal generated by the set $\{\mathrm{lm}_v(f) | f \in I\}$.

The following is an example of the leading form of a polynomial f, which is a monomial with respect to some vector v, but it is not a monomial with respect to some other vector v'.

Example 3.3.1. Let $f(x, y) = x^6y^2 + 2x^5y^3 + x^3 - x^2y^4 \in \mathbb{Q}[x, y]$. Let $\prec$ be the lexicographic ordering on the set of monomials of $\mathbb{Q}[x, y]$. We compute the leading form of f with respec to $\prec_v$ and $\prec_{v'}$ where $v = (2, 1)$ and $v' = (1, 1)$ as follows: For $v = (2, 1)$, we have to see the maximal element in the set

$$\{\langle v, (6, 2)\rangle, \langle v, (5, 3)\rangle, \langle v, (3, 0)\rangle, \langle v, (2, 4)\rangle, \} = \{14, 13, 6, 8\}.$$

So we obtain $\mathrm{lm}_v(f) = x^6y^2$.

For $v' = (1, 1)$, we have to see the maximal element in the set

$$\{\langle v', (6, 2)\rangle, \langle v', (5, 3)\rangle, \langle v', (3, 0)\rangle, \langle v', (2, 4)\rangle, \} = \{8, 8, 3, 2\}.$$

So we obtain $\mathrm{lm}_{v'}(f) = x^6y^2 + 2x^5y^3$ which is not a monomial.

Also, Sturmfels showed important results for monomial ordering with respect to weight vector.

Proposition 3.3.5. Let $v \in \mathbb{R}^n$ be a real vector with non negative entries and $I \subset R$ be an ideal. If $\mathrm{lm}_v(I)$ is a monomial ideal, i.e., $\mathrm{lm}_v(I)$ is generated by monomials, then $\mathrm{lm}_v(I)$ is equal to the leading monomial of I with respect to the monomial ordering $\prec_v$.

Proof. Firstly we notice from definition 3.3.1 and 3.3.3 that for any nonzero polynomial $f \in R$, we have the leading monomial of the polynomial $\mathrm{lm}_v(f)$ with respect to $\prec$ is equal to $\mathrm{lm}_{\prec_v}(f)$. Therefore, the ideals $\mathrm{lm}(\mathrm{lm}_v(I))$ and $\mathrm{lm}_{\prec_v}(I)$ contain the same monomials and hence these two ideals are equal. Suppose that $\mathrm{lm}_v(I)$ is a monomial ideal. Then we have

$$\mathrm{lm}_v(I) = \mathrm{lm}_{\prec_v}(\mathrm{lm}_v(I))$$

and hence by the definition of $\prec_v$, the proposition follows. □

Theorem 3.3.6. For any monomial ordering $\prec$ and any ideal $I \subset R$, there exists a vector v with non negative integer entries such that $\mathrm{lm}_v(I)$ is equal to the leading monomial ideal of I.

Sturmfels showed that by taking any $v \in \mathcal{C}_{I,\prec} \cap \mathbb{Z}^n$ where $\mathcal{C}_{I,\prec}$ is the set all non negative vectors $v \in \mathbb{R}^n_{\geq 0}$ such that for all g in the reduced Gröbner basis G of I with respect to $\prec$ we have $lm_v(g) = lm_\prec(g)$. For more details see [28] in proposition 1.11. For $v \in \mathbb{R}^n$ and a monomial ordering $\prec$ such that $\mathrm{lm}_v(I) = \mathrm{lm}(I)$, we call v weight vector representation of I with respect to $\prec$.

Example 3.3.2. Let $I \subset \mathbb{Q}[x, y, z]$ be the ideal generated by $f = xyz - y$ and $g = x^2y - yz$. Let $\prec$ be the graded monomial ordering on the set of monomials of $\mathbb{Q}[x_y, z]$. In example 3.2.1, we obtain $G = \{f, g, h\}$ with $h = yz^2 - xy$ as a Gröbner basis of I. Therefore, by definition 3.2.9, G is the Gröbner basis of I. Now we choose $v = (1, 1, 1)$ and it is obvious that $\mathrm{lm}_v(f) = \mathrm{lm}_\prec(f), \mathrm{lm}_v(g) = \mathrm{lm}_\prec(g)$, and $\mathrm{lm}_v(h) = \mathrm{lm}_\prec(h)$. Moreover, by proposition 3.3.5 and the fact that G is a Gröbner basis of I, we have $\mathrm{lm}_v(I) = \mathrm{lm}_\prec(I)$.

A vector weight from Sturmfels in 3.3.6, in fact, can be obtained from the first vector we achieved in the set of orthogonal vectors representing $\prec$ in theorem 2.2.8.

3.4 Optimization of a Gröbner Basis Computation

In the previous section we have seen Buchberger's algorithm to compute a Gröbner basis of a given ideal I of a polynomial ring $R = \mathbb{F}[x_1, \ldots, x_n]$ for some field $\mathbb{F}$ and in order to make the algorithm works we have to make a prior choice of monomial orderings. Besides of choosing a monomial ordering as the main tool in the algorithm, we also have a notion of S-polynomials which requires us to choose pairs of polynomials in the initial proposed set of generators and we have noticed in section 3.1 that reduced form of a polynomial with respect to a finite set G of polynomials depends on the order of reductions we choose.

Therefore, the choices made in the computational process affects the efficiency of the algorithm such as the number of S-polynomials we have to compute. It might happen that the choices we made obligates us to compute more

S-polynomials which will be eliminated again after reduction process. In this section we discuss some approaches to boost the performance of Gröbner bases computation.

3.4.1 The selection of monomial orderings

The complexity of an algorithm of computing Gröbner basis extreamly relies on the monomial ordering we chose. C.Kollreider showed, in [23], the selection of monomial orderings influences the complexity of Buchberger's algorithm. The following example simply demonstrates how two distinct monomial orderings give different number of computational steps by using Buchberger's algorithm.

Example 3.4.1. Let I be an ideal of $\mathbb{Q}[x, y]$ generated by $f_1 = x + y^2$, $f_2 = x^2 - y^3$, and $f_3 = y^2 - y$. Let $\prec_1$ and $\prec_2$ be the lexicographic order and the graded lexicographic order respectively with $y \prec_i x$ for $i = 1, 2$.

Firstly we compute a Gröbner basis of I with respect to $\prec_1$ by using Buchberger's algorithm: We have $G = \{f_1, f_2, f_3\}$; and we compute $\mathrm{S}(f_1, f_2) = xy^2 + y^3$, $\mathrm{S}(f_1, f_3) = xy + y^4$, and $\mathrm{S}(f_2, f_3) = x^2y - y^5$ which all have zero normal forms with respect to the set G, i.e.,

$$\begin{aligned} \mathrm{S}(f_1, f_2) &= xy^2 + y^3 = y^2 f_1 + y^2 f_3 \\ \mathrm{S}(f_1, f_3) &= xy + y^4 = y f_1 - y^2 f_3 \\ \mathrm{S}(f_2, f_3) &= x^2y - y^5 = y f_2 + y^3 f_3. \end{aligned}$$

So by theorem 3.2.2, G is already a Gröbner basis.

However, by the same algorithm but using $\prec_2$ instead of $\prec_1$, we need more steps and computations to produce $G = \{f_1, f_2, f_3, -x^2 - yx, x + y\}$ as a Gröbner basis of I.

From the example, it might happen that we compute a Gröbner basis with respect to a particular monomial ordering that is computationally less efficient. In the first chapter we have seen that any monomial ordering is related to a matrix and the lexicographic on a finite dimensional real vector space, so it leads us to see the relation between a Gröbner basis of an ideal I with respect to a particular monomial ordering $\prec_1$ and a Gröbner basis of I with respect to another monomial ordering $\prec_2$. In other words, we compute a Gröbner basis of I with respect to some computationally efficient monomial ordering and the transform it into a Gröbner basis of I for the desired monomial ordering.

The algorithm for converting a Gröbner bases was introduced by Collart et al., in [11], in 1997 which is Gröbner walk. Also Gröbner walk is discussed by Amrhein et al. in [1] and by Tran in [29]. Furthermore, if we only focus on finding a Gröbner basis of an ideal ithout any particular monomial ordering required, then we can determine a good monomial ordering to start with as discussed by Tran in [30] and in [31].

3.4.2 Detecting Useless S-polynomials

In Buchberger's algorithm, the process of computing S-polynomials and the reduction process are quite a time-consuming steps that we need to reduce. For instance, computing the S-polynomials of pairs which have zero normal forms, which is unnecessary or even useless process. Therefore, Buchberger, in [6], introduced two criteria to identify pairs of polynomial which have zero normal forms and Gebauer as follows:

- Criterion 1: If two polynomials f and g has property that

$$\gcd(\mathrm{lm}_\prec(f), \mathrm{lm}_\prec(g)) = 1,$$

  then $\mathrm{S}(f, g)$ reduces to zero by the set $\{f, g\}$.

- Criterion 2: Let f, g, h be polynomials in the current basis set G such that $\mathrm{lm}_\prec(h)$ divides $lcm(\mathrm{lm}_\prec(f), \mathrm{lm}_\prec(g))$ and $\mathrm{S}(f, h), \mathrm{S}(g, h)$ reduce to zero, then $\mathrm{S}(f, g)$ reduces to zero by the current basis set G.

The following example shows how to take advantages from these criteria.

Example 3.4.2. Let I be the ideal generated by $f = x^2 + xy^2$, $g = x^2 - y^3$ and $h = y^3 - y^2$. Let $\prec$ be the lexicographic ordering on the set of monomials of $\mathbb{Q}[x, y]$. Therefore, by criterion 1, we do not need to compute $\mathrm{S}(f, h)$ and $\mathrm{S}(g, h)$. Hence we only need to do computation for $\mathrm{S}(f, g)$ and by computing this polynomial we have $\mathrm{S}(f, g) = xy^2 + y^2$ which has nonzero normal form with respect to $G = \{f, g, h\}$. Moreover, since $\mathrm{lm}_\prec(h)$ divides $lcm(\mathrm{lm}_\prec(f), \mathrm{lm}_\prec(h)$ and $lcm(\mathrm{lm}_\prec(g), \mathrm{lm}_\prec(h)$, then by using criterion 2, we have $G' = \{f, g, h, xy^2 + y^2\}$ is a Gröbner basis of I.

3.4.3 Removing Superfluous Polynomials

As we have seen in lemma 3.2.8, we may remove some polynomials from a Gröbner basis we have from the computation which are unnecessary or to make the Gröbner basis into minimal. The removal process is mostly performed after we produce a Gröbner basis, but it is possible to do the removal of superfluous polynomials intermediately at each reduction step. The removal process at each reduction step is as follows:
Let G be a Gröbner basis of an ideal $I \subset R = \mathbb{F}[x_1, \ldots, x_n]$. Let $g, g' \in G$ be distinct elements. If $\mathrm{lm}_\prec(g)$ divides $\mathrm{lm}_\prec(g')$, then g' can be expressed by g and the polynomial $\mathrm{S}(g, g')$. Hence once we reduce $\mathrm{S}(g, g')$ into normal form, we may remove g from our Gröbner basis G, this follows from the second property of reduced Gröbner bases in definition 3.2.9.

The process of removing superfluous polynomials at each reduction step makes the algorithm much more efficient as we only need to compute less S-polynomials.

Chapter 4

Gröbner Bases for Decoding Linear Codes

4.1 Introduction

The problem of information transmission where the information is transmitted through a channel is one of the problems that is encountered in the digital era. For example, if an information source A sends an information to a receiver B where A and B are mobile phones, then the channel is the space where electromagnetic waves propagate. Therefore, we need to consider the case in which some interference or noise appears in the channel where the information transmitted through. Hence the interference in the channel can distort the transmitted information.

The basic idea of coding theory consists of adding some redundancy to the information that the information source A wants to send to a receiver B which we call as an encoding procedure to get a longer word. Because of the appearance of noise, the transmitted information containing additional redundancy can be distorted. If the occurred errors are not too many, the receiver B is able to recover the original word which we call as a decoding procedure.

In this chapter we discuss how to apply Gröbner bases to decode a particular class of codes called linear codes. Therefore, in this section we recall some basic definitions and results from classical coding theory.

Definition 4.1.1. A linear code C is a linear subspace of $\mathbb{F}_q^n$ where $\mathbb{F}_q$ is a finite field with q elements and elements of C are called codewords. The dimension of a linear code is its dimension as a linear subspace over $\mathbb{F}_q$. We write a linear code C over $\mathbb{F}_q$ of length n and dimension k as an $[n, k]_q$ code.

Since any two vector spaces of the same dimension over a field are isomorphic, it is clear that an $[n, k]_q$ code has size q^k. Moreover, the information rate of an $[n, k]_q$ code is k/n and its redundancy is $n - k$. If we have a linear code, we can obtain another linear code by taking its orthogonal space as follows.

Definition 4.1.2. Let C be $[n,k]_q$ code, its dual $\mathrm{C}^\perp$ is the set of vectors orthogonal to C:

$$\mathrm{C}^\perp : \{v \in \mathbb{F}_q^n \,|\forall c \in \mathrm{C}, \langle v, c\rangle = 0\}.$$

Thus $\mathrm{C}^\perp$ is an $[n, n-k]_q$ code.

Now by taking a basis of C as a linear subspace of $\mathbb{F}_q^n$, we can obtain a linear map $\mathcal{E}$ from $\mathbb{F}_q^k$ into $\mathbb{F}_q^n$ and the image of this linear map is the code C. So we can see $\mathbb{F}_q^k$ as the source of words and the process of applying this such linear map is referred to as encoding or coding process.

Definition 4.1.3. Let C be an $[n,k]_q$ code. Then a matrix G whose rows form a basis for C is called a generator matrix for G. If G is of row reduced echelon form then we say G is in a standard form.

Therefore, we can write an encoding process by

$$\begin{aligned} \mathcal{E} : \mathbb{F}_q^k &\to \mathbb{F}_q^n \\ v &\mapsto vG. \end{aligned}$$

A generator matrix G of C is a tool to do encoding. But to do decoding or to check whether a received word is a codeword or not, it is more useful to consider the following matrix.

Definition 4.1.4. A parity-check matrix for an $[n,k]_q$ code C is a generator matrix H for $\mathrm{C}^\perp$.

By the definition above we see that C may be expressed as the null-space of a parity matrix H:

$$\forall x \in \mathbb{F}_q^n,\ Hx^T = 0 \iff x \in \mathrm{C}.$$

Now we give a simple example to describe what could happen during the transmission process. Suppose that the source of words is

$$(\mathbb{F}_2)^2 = \{(0,0),(1,0),(0,1),(1,1)\}$$

and let C be the $[6,2]_2$ code generated by $G = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$. Then we have

$$\mathrm{C} = \{(0,0,0,0,0,0),(1,1,1,0,0,0),(0,0,0,1,1,1),(1,1,1,1,1,1)\}.$$

To send $(1,0)$ we transmit the word $(1,0)G = (1,1,1,0,0,0)$. By our assumption, typically during the transmission the word is distorted by interference and the receiver has to perform some operations to obtain the transmitted word which is referred to a decoding process. Let v be the received vector. There are several different situations may come up:

- $v = (1, 1, 1, 0, 0, 0)$, thus $v \in$ C, so the receiver deduces correctly that no errors have occurred and no correction is needed. It concludes that the word was $(1, 0)$.

- $v = (1, 0, 1, 0, 0, 0) \notin$ C, so the receiver concludes that some errors have occurred. In this case it may "correct" and "detect" the error as follows. It may suppose that the word transmitted was $(1, 1, 1, 0, 0, 0)$ since that is the word that differs in the least number of positions from the received word v.

- $v = (0, 0, 1, 0, 0, 0) \notin$ C, so the receiver correctly reaches the conclusion that there were some errors during the transmission, but if it tries to correct as in the previous case, it concludes that the word "nearest" to v is $(0, 0, 0, 0, 0, 0)$. In this case it corrects in a wrong way.

- $v = (0, 0, 0, 0, 0, 0) \in$ C, then the receiver deduces incorrectly that no errors have occurred.

From the previous example we understand that, when the decoder gets a received vector which is not an element in C, it has to find the element in C which has been sent by the encoder, i.e., among all elements of C, it has to find the one which has the "highest probability" of being sent. To do this we need the following definitions.

Definition 4.1.5. Let $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ be two elements in $\mathbb{F}_q^n$. The weight $\mathrm{wt}(u)$ of u is defined as the number of nonzero coordinate of u and the Hamming distance $d(u, v)$ is defined as the number of coordinates where u and v differ:

$$d(u, v) = |\{i | u_i \neq v_i\}|.$$

By direct verification, one can show that the Hamming distance is a well-defined metric on $\mathbb{F}_q^n$, meaning that it satisfies all properties below:

- For all $x, x' \in \mathbb{F}_q^n$, we have $d(x, x') \geq 0$;

- For all $x, x' \in \mathbb{F}_q^n$, we have $d(x, x') = 0$ if and only if $x = x'$;

- For all $x, x' \in \mathbb{F}_q^n$, we have $d(x, x') = d(x', x)$;

- For all $x, x', y \in \mathbb{F}_q^n$, we have $d(x, x') \leq d(x, y) + d(y, x')$.

Definition 4.1.6. The distance of a linear code C is the minimal distance between distinct words in C:

$$d(\mathrm{C}) := \min\{d(c, c') | c, c' \in \mathrm{C} \text{ and } c \neq c'\}$$

Remark. The distance of C is equal to the minimum weight of nonzero words in C.

We write a linear code of length n and dimension k over $\mathbb{F}_q$ which has distance d as an $[n, k, d]_q$ code.

In the previous example, there is a case where the receiver can detect errors in the transmitted vector but the receiver failed to correct it and also there is a case when the receiver could not detect errors occurred in the transmitted vector. Therefore, the following theorem tells us how many errors occurred can be detected and how many errors occurred can be recovered correctly.

Theorem 4.1.7. Let C be an $[n, k, d]_q$ code. Then

- C has detection capability $l = d - 1$;
- C has correction capability $\tau = \lfloor \frac{d-1}{2} \rfloor$.

Proof. Let $c \in$ C be a transmitted codeword and $v \in \mathbb{F}_q^n$ be the received word. Suppose that $d(c, v) \leq d - 1$. Since d is the minimum distance in C, thus $v \notin$ C and we proved that we can detect errors happened if and only if the number of errors happened is at most $d - 1$. Moreover, we suppose that $d > 2\tau$. Let $c \in$ C be a transmitted codeword and $v \in \mathbb{F}_q^n$ be the obtained word from c with at most τ errors. We need to show that c is closer to v than any other codewords $r \in$ C. Since the Hamming distance is well-defined metric on $\mathbb{F}_q^n$, the triangle inequality holds and hence

$$d(c, v) \leq d(c, r) + d(r, v)$$

$$-d(c, r) + d(c, v) \leq d(r, v)$$

$$\tau + 1 = 2\tau + 1 - \tau \leq d(v, r).$$

Conversely, suppose that c is closer to v than any other codeword $r \in$ C. Then for $r \in$ C$\backslash\{c\}$, we have $d(v, r) \geq \tau + 1$ and again by using the triangle inequality

$$d(v, r) \leq d(v, c) + d(c, r)$$

$$-d(v, c) + d(v, r) \leq d(c, r)$$

$$2\tau + 1 = \tau + 1 + \tau \leq d(c, r).$$

□

Proposition 4.1.8. Let C be an $[n, k, d]_q$ code. Then

$$d \leq n - k + 1.$$

Proof. Let C be a linear code with distance d. Let we consider the projection from $\mathbb{F}_q^n$ to $\mathbb{F}_q^{n-(d-1)}$, say on the last $n - (d - 1)$ coordinates of each codewords of C. Hence the restriction of the projection on C is injective, since all of elements in C have Hamming distance at least d from each other. Therefore, $|\text{C}| = q^k \leq |\, \mathbb{F}_q^{n-(d-1)} \,| = q^{n-d+1}$. So we have $k \leq n - d + 1$ or equivalently $d \leq n - k + 1$. □

A code achieving the equality above is called maximum distance separable (MDS) code.

4.2 Cyclic Codes

Now we give a brief overview of an important class of linear codes that is called cyclic codes which have special algebraic properties.

Definition 4.2.1. An $[n, k, d]_q$ code C is cyclic if and only if the cyclic shift of every codeword $c \in \mathrm{C}$ is again a codeword in C, i.e.,

$$(c_1, \ldots, c_n) \in \mathrm{C} \iff (c_n, c_1, \ldots, c_{n-1}) \in \mathrm{C}.$$

Proposition 4.2.2. The dual of a cyclic code is again cyclic.

Proof. Let C be a cyclic code. Then $\sigma(c) \in \mathrm{C}$ for all $c \in \mathrm{C}$. Then

$$\sigma^{n-1}(c) = (c_1, c_2, \ldots, c_{n-1}, c_0) \in \mathrm{C} \text{ for all } c \in \mathrm{C}.$$

Let $x \in \mathrm{C}^{\perp}$. Then

$$\sigma(x) \cdot c = x_{n-1}c_0 + x_0c_1 + \cdots + x_{n-2}c_{n-1} = x \cdot \sigma^{n-1}(c) = 0$$

for all $c \in \mathrm{C}$. Hence $\mathrm{C}^{\perp}$ is cyclic. □

Now let we consider the quotient ring $\mathrm{C}_{q,n} := \mathbb{F}_q[x]/(x^n - 1)$. Thus the set $\{1, x, x^2, \ldots, x^{n-1}\}$ form a basis for $\mathrm{C}_{q,n}$ over $\mathbb{F}_q$. The following proposition shows that we can consider $\mathbb{F}_q^n$ as $\mathrm{C}_{q,n}$ and cyclic codes $[n, k]_q$ are in one-to-one correspondence with ideals in $\mathrm{C}_{q,n}$.

Proposition 4.2.3. Consider the map ϕ between $\mathbb{F}_q^n$ and $\mathrm{C}_{q,n}$ defined by

$$\phi : v = (v_0, \ldots, v_{n-1}) \mapsto v(x) = v_0 + v_1x + \cdots + v_{n-1}x^{n-1}.$$

Then the map ϕ is an isomorphism of vector spaces. Moreover, cyclic codes in $\mathbb{F}_q^n$ correspond one-to-one to ideals in the ring $\mathrm{C}_{q,n}$.

Proof. The map ϕ is clearly linear and it maps the standard basis of $\mathbb{F}_q^n$ to $\{1, x, x^2, \ldots, x^{n-1}\}$. Hence ϕ is an isomorphism of vector spaces. Let ψ the inverse map of ϕ.

Let I be an ideal in $\mathrm{C}_{q,n}$. Then $\mathrm{C} := \psi(I)$ is a linear code as ψ is a linear map and we can think of I as a subvectorspace of $\mathrm{C}_{q,n}$. Let $c \in \mathrm{C}$. Then $\phi(c) \in I$ and since I is an ideal then $x \cdot \phi(c) \in I$ where

$$x \cdot \phi(c) = c_0x + \cdots + c_{n-1}x^n = c_{n-1} + c_0x + \cdots + c_{n-2}x^{n-1}.$$

Therefore, C is a cyclic code.

Conversely, let C be a cyclic code in $\mathbb{F}_q^n$, and let $I := \phi(\mathrm{C})$. Then I is closed under addition as C is a linear code and ϕ is a linear map. Moreover, if $a \in \mathbb{F}_q^n$ and $c \in \mathrm{C}$, then

$$\phi(a)\phi(c) = \sum_i \sum_j a_i c_{j-i} x^j,$$

where the indices i and j are taken modulo n. Hence

$$\phi(a)\phi(c) = \phi(a_0c + a_1\sigma(c) + \cdots + a_{n-1}\sigma^{n-1}(c)),$$

where σ is the cyclic shift map, i.e., $\sigma(c) = (c_{n-1}, c_0, \ldots, c_{n-2})$. Thus $\phi(a)\phi(c)$ is in I and hence I is an ideal in $\mathrm{C}_{q,n}$. □

Since $\mathbb{F}_q[x]$ is a principal ideal domain as we have Euclidean division algorithm in the ring, thus $\mathrm{C}_{q,n}$ is a principal ideal ring. Therefore, from proposition 4.2.3 any cyclic code corresponds to a principal ideal, meaning that we can obtain a generator polynomial of each cyclic code. Moreover, by looking at the corresponding ideal I as an ideal in $\mathbb{F}_q[x]$ containing the ideal $(x^n - 1)$ rather than as an ideal in the quotient ring $\mathrm{C}_{q,n}$, it leads to the uniqueness of a generator polynomial of any cyclic code, which is the monic polynomial of minimal degree in I.

Definition 4.2.4 (Generator Polynomial)**.** Let C be a cyclic code and let I be the corresponding ideal of C in $\mathbb{F}_q[x]$ containing the ideal $(x^n - 1)$. Then the monic polynomial $g(x) \in I$ of minimal degree is called the generator polynomial of C.

Let ϕ be the isomorphism in theorem 4.2.3 with the inverse map ψ and let φ be the quotient map. Let we consider the following diagram

$$\begin{array}{ccc} \mathbb{F}_q[x] & \xrightarrow{\varphi} & \mathrm{C}_{q,n} \\ & \searrow & \downarrow \psi \\ & & \mathbb{F}_q^n \end{array}$$

From the diagram above, we have a surjective map from $\mathbb{F}_q[x]$ onto $\mathbb{F}_q^n$. Moreover, we have the following result.

Corollary 4.2.5. There exists a bijection between the set of all cyclic codes C over $\mathbb{F}_q$ of length n and the set of all monic factors of $x^n - 1$ in $\mathbb{F}_q[x]$ given by

$$\Phi : \mathrm{C} \longmapsto g(x)$$

where $g(x)$ is the monic minimal degree polynomial in the ideal $\varphi^{-1}(\phi(\mathrm{C}))$ of $\mathbb{F}_q[x]$.

Proof. Let C be a cyclic code over $\mathbb{F}_q$ of length n. From proposition 4.2.3, $\phi(\mathrm{C})$ is an ideal in $\mathrm{C}_{q,n}$. Moreover, by the first isomorphism theorem for rings, $\varphi^{-1}(\phi(\mathrm{C}))$ is an ideal in $\mathbb{F}_q[x]$ containing $(x^n - 1)$. Therefore, since $\mathbb{F}_q[x]$ is a principal ideal domain, we can obtain the monic minimal degree polynomial $g(x)$ which generates $\varphi^{-1}(\phi(\mathrm{C}))$. Furthermore, $g(x)$ divides $x^n - 1$ as $x^n - 1 \in \varphi^{-1}(\phi(\mathrm{C}))$. So the map is well-defined. Moreover, the injectivity and the surjectivity follow from the bijection map ϕ. □

Remark. It is obvious that the minimum distance d of a cyclic code C with generator polynomial $g(x)$ satisfies $d \leq \mathrm{wt}(g(x) \mod x^n - 1)$, and one of a natural goal of coding theory is to construct a code with maximum distance or it is called as maximum distance separable code (MDS). Hence we need a cyclic code with generator polynomial $g(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_0$ with all coefficients $a_j$are nonzero. One subclass of cyclic codes satisfying the criteria is Reed-Solomon codes $RS_k(n, b)$ in definition 4.3.6.

So far we know that to find such generator matrix for a cyclic code C, we need to take the monic generator of its corresponding ideal in $\mathbb{F}_q[x]$ which contains $(x^n - 1)$. But by using a certain generator matrix of C that we have in the previous section we can obtain its generator polynomial and also the corresponding ideal.

Theorem 4.2.6. Let $g(x) = g_0 + g_1x + \cdots + g_mx^m$ be a polyomial $\in \mathbb{F}_q[x]$. Let n be an integer with $m \leq n$. Let $k = n - m$. Let G be the $k \times n$ matrix defined by

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_m & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_m & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \dots & \ddots & 0 \\ 0 & \dots & 0 & g_0 & g_1 & \dots & g_m \end{pmatrix}.$$

(1) If $g(x)$ is the generator polynomial of a cyclic code C, then the dimension of C is equal to k and G is a generator matrix of C.

(2) If $g_m = 1$ and G is a generator matrix of a code C such that

$$(g_m, 0, \dots, 0, g_0, g_1, \dots, g_{m-1}) \in \mathrm{C}$$

then C is cyclic with generator polynomial $g(x)$.

Proof.

(1) Suppose that $g(x)$ is the generator polynomial of a cyclic code C. Then $g = (g_0, \dots, g_m)$ generates the code C and coefficients of each $g(x)$, $xg(x)$, $\dots, x^{k-1}g(x)$ correspond to the rows of the matrix G above. Since $g(x)$ is the generator matrix of C, then $g_m = 1$ and the $k \times k$ submatrix of G consisting the last k columns is a lower diagonal matrix with ones on the diagonal, so the rows of G are linearly independent. Moreover, every polynomial $c(x) \in (g(x))$ with $c = (c_0, \dots, c_n) \in \mathrm{C}$ is equal to $a(x)g(x)$ for some polynomial $a(x) \in \mathbb{F}_q[x]$. Since $g(x)$ divides $x^n - 1$, there exists polynomial $e(x)$ and $f(x)$ in $\mathbb{F}_q[x]$ such that

$$a(x)c(x) = e(x)(x^n - 1) + f(x) \text{ and } \deg(f(x)) < n \text{ or } f(x) = 0.$$

But $x^n - 1$ is divisible by $g(x)$ as $g(x)$ is the generator polynomial of C. So $f(x) = b(x)g(x)$ for some polynomial $b(x) \in \mathbb{F}_q[x]$ with $\deg(b(x) \leq n - m = k$ or $b(x) = 0$. Therefore, $c(x) = a(x)g(x) = b(x)g(x) \bmod (x^n - 1)$. So every codeword $c \in \mathrm{C}$ is a linear combination of rows of the matrix G and k is the dimension of C.

(2) Suppose that $g_m = 1$ and G is a generator matrix of a code C such that $(g_m, 0, \ldots, 0, g_0, g_1, \ldots, g_{m-1}) \in$ C. Then for all $i < k$, we have the cyclic shift of the i-th row of G is the $(i+1)$-th row of G and $(g_m, 0, \ldots, 0, g_0, g_1, \ldots, g_{m-1})$ is the cyclic shift of the k-th row of G. Therefore, as any codeword $c \in$ C is of the linear combination of rows of G and the cyclic shift is a linear transformation, C is a cyclic code of dimension k. Moreover, since any polynomial in the corresponding ideal of the cyclic code C is a linear combination of the polynomials $g(x), xg(x), \ldots, x^{k-1}g(x)$ and also $g(x)$ is monic, thus $g(x)$ is the generator polynomial of C.

□

Consider a cyclic code of length n over $\mathbb{F}_q$ with generator polynomial $g(x)$ and the corresponding generator matrix G as in theorem 4.2.6. Let the word $m = (m_0, \ldots, m_{k-1}) \in \mathbb{F}_q^k$ be mapped to the codeword $c = mG$. Then in terms of polynomials that means that

$$c = \phi(m)g(x) \bmod x^n - 1, \text{ where } \phi(m) = m_0 + m_1 x + \cdots + m_{k-1}x^{k-1}.$$

Proposition 4.2.7. Let $g(x)$ be the generator polynomial of a cyclic code C and $h(x) = \frac{x^n-1}{g(x)}$. Then we have

$$c(x) \in \text{C} \iff c(x)h(x) = 0 \bmod x^n - 1.$$

The polynomial $h(x)$ is called the parity check polynomial of the cyclic code C.

Proof. Let $c \in$ C. Then there exists a polynomial $a(x)$ such that

$$\phi(c) = a(x)g(x).$$

Since $g(x)h(x) = 0 \bmod x^n - 1$, then $c(x)h(x) = a(x)g(x)h(x) = 0 \in \text{C}_{q,n}$.

Conversely, suppose that $c(x)h(x) = 0 \bmod x^n - 1$. Then there exist polynomials $a(x)$ and $b(x)$ such that

$$c(x) = a(x)g(x) + b(x) \text{ and } b(x) = 0 \text{ or } \deg(b(x)) < \deg(g(x)).$$

Since we have $\deg(b(x)h(x))$ is at most $n-1$, thus if $b(x)$ is nonzero, then $b(x)h(x) \neq 0 \bmod x^n - 1$. Hence $b(x) = 0$ and $\phi(c) = a(x)g(x) \in \text{C}_{q,n}$ and $c \in$ C. □

Remark. Since $g_0 \neq 0$ as we have $g(x)h(x) = x^n - 1$, the generator matrix in theorem 4.2.6 is upper diagonal at the first k positions with nonzero entries on the diagonal. So the reduced echelon form of G has $k \times k$ identity matrix at the first k columns and the last row is up to the constant g_0 equal to $(0, \ldots, 0, g_0, \ldots, g_m)$. So we can obtain the monic generator polynomial of any cyclic code from the standard form of generator matrix.

One might expect that if $h(x)$ is the parity check polynomial of the cyclic code C, then $h(x)$ is the generator polynomial of the dual code $\mathrm{C}^{\perp}$. However, this is not the case but the following result shows how we obtain the generator polynomial of the dual code $\mathrm{C}^{\perp}$ from the parity check polynomial $h(x)$ of the cyclic code C.

Proposition 4.2.8. Let $h(x)$ be the parity check polynomial of a cyclic code C. Then the monic reciprocal of $h(x)$, i.e., $g^{\perp}(x) = \frac{x^{\deg(h(x))}h(x^{-1})}{h(0)}$, is the generator polynomial of the code $\mathrm{C}^{\perp}$.

Proof. Let C be a cyclic code of length n and of dimension k with generator polynomial $g(x)$ and parity check polynomial $h(x)$. We are going to show this by using induction on k.

If $k = 0$, then $g(x) = x^n - 1$ and $h(x) = 1$ and similarly if $k = n$, then $g(x) = 1$ and $h(x) = x^n - 1$. Hence this is true for these cases.

Now suppose that $0 < k < n$. Then $h(x) = h_0 + h_1x + \cdots + h_kx^k$. Hence

$$x^k h(x^{-1}) = h_k + h_{k-1}x + \cdots + h_0x^k.$$

The i-th position of $x^k h(x^{-1})$ is h_{k-i}. Let $l = n - k$. Then $g(x) = g_0 + g_1x + \cdots + g_lx^l$ and $g_l = 1$. The elements $x^t g(x)$ generate C. The i-th position of $x^t g(x)$ is equal to g_{i+t}. Hence the inner product of the words $\psi(x^t g(x))$ and $\psi(x^k h(x^{-1})$ is

$$\sum_{i=0}^{k} g_{i+t}h_{k-i},$$

which is the coefficient of the term x^{t+k} in $x^t g(x)h(x)$. But $x^t g(x)h(x)$ is equal to $x^{n+t} - x^t$ and $0 < k < n$, hence this coefficient is zero. So $\sum_{i=0}^{n} g_{i+t}h_{k-i} = 0$ for all t. So $\psi(x^k h(x^{-1})) \in \mathrm{C}^{\perp}$.

Now since $g(x)h(x) = x^n - 1$, so $g(0)h(0) = -1$. Hence the monic reciprocal of $h(x)$ is well-defined, is monic, represents an element of $\mathrm{C}^{\perp}$, has degree k and the dimension of $\mathrm{C}^{\perp}$ is $n - k$. Hence by theorem 4.2.6 $x^k h(x^{-1})/h(0)$ is the generator polynomial of the code $\mathrm{C}^{\perp}$. □

A very interesting case is when $\gcd(q, n) = 1$ as all roots of $x^n - 1$ are simple. Let $\mathbb{F} = \mathbb{F}_{q^m}$ be the splitting field of the polynomial $x^n - 1$ over $\mathbb{F}_q$ and let $\alpha \in \mathbb{F}$ be a root of unity of order n over $\mathbb{F}_q$. We have

$$x^n - 1 = \prod_{i=0}^{n-1}(x - \alpha^i).$$

In this case the generator polynomial of C has powers of α as roots. Recall that given $g \in \mathbb{F}_q[x]$, if $g(\alpha^i) = 0$, then $g(\alpha^{iq}) = 0$.

Definition 4.2.9. Let C be an $[n, k, d]_q$ cyclic code with generator polynomial $g(x)$ with $\gcd(n, q) = 1$. The set

$$S_{\mathrm{C},\alpha} = S_{\mathrm{C}} = \{i \in \mathbb{Z}/n\mathbb{Z} \,|\, g(\alpha^i) = 0\}$$

is called the complete defining set of C.

Any cyclic code C is defined by its complete defining set $S_{\mathrm{C}} = \{i_1, \ldots, i_{n-k}\}$, since

$$\mathrm{C} = \{c(x) \in \mathrm{C}_{q,n} | c(\alpha^i) = 0, \forall i \in S_{\mathrm{C}}\} \iff g(x) = \prod_{i \in S_{\mathrm{C}}} (x - \alpha^i).$$

Conversely, any subset $S \subseteq \mathbb{Z}/n\mathbb{Z}$ which is invariant under multiplication by q gives a cyclic code with generator polynomial $g(x) = \prod_{i \in S}(x - \alpha^i)$. Therefore, by this fact it follows that

$$H = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \ldots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \ldots & \alpha^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{i_{n-k}} & \alpha^{2i_{n-k}} & \ldots & \alpha^{(n-1)i_{n-k}} \end{pmatrix} \tag{4.1}$$

is a parity check matrix of the code C, since

$$Hc^T = \begin{pmatrix} c(\alpha^{i_1}) \\ c(\alpha^{i_2}) \\ \ldots \\ c(\alpha^{i_{n-k}}) \end{pmatrix} = 0 \iff c \in \mathrm{C}.$$

Another interesting case is when n divides $q-1$ as all roots of $x^n - 1$ are in $\mathbb{F}_q$. Hence the splitting field of $x^n - 1$ over $\mathbb{F}_q$ is $\mathbb{F}_q$ itself and such parity check matrix in equation 4.1 is a matrix over $\mathbb{F}_q$.

In coding theory, the minimum distance of a linear code is also crucial as the correction capability of a linear code in theorem 4.1.7 depends on its minimum distance. For cyclic codes we have the following result from Bose, Chaudhuri, and Hocquenghem which gives a bound for the minimum distance of a cyclic code.

Theorem 4.2.10. [BCH Bound] Let C be a cyclic code of length n that has at least $\gamma - 1$ consecutive elements in S_{C} modulo n. Then the minimum distance of C is at least γ.

Proof. See [25], page: 173. □

Now we give some examples of cyclic codes where its minimum distance is equal to the weight of its generator polynomial.

Example 4.2.1. Let C be the $[6, 3]_7$ cyclic code with the generator polynomial $g(x) = x^3 + 3x^2 + x + 6$. Since all roots of $x^6 - 1$ over $\mathbb{F}_q$ are all elements of $\mathbb{F}_q^*$ where 3 generates $\mathbb{F}_q^*$. Then we have $3, 3^2$ and 3^3 are the zeros of $g(x)$ over $\mathbb{F}_q$ and so by BCH bound in theorem 4.2.10 we have $d(\mathrm{C}) \geq 4$. Moreover, since we have $\mathrm{wt}(g(x)) = 4$, $d(\mathrm{C}) = 4$. Hence the code C is an MDS code.

Example 4.2.2. Let C be the $[7, 4]_2$ cyclic code with the generator polynomial $g(x) = x^3 + x + 1$. We know from Galois theory that the splitting field of $x^3 + x + 1$

is isomorphic to $\mathbb{F}_{2^3}$. Suppose that $\alpha \in \mathbb{F}_8$ is a root of $g(x) = x^3 + x + 1$. Hence by the Frobenius morphism, α^2 is also a root of $g(x)$. Hence we have that α^j is a zero of $g(x)$ for two consecutive values of $j = 1, 2$. So by the BCH bound we have $d(\mathrm{C}) \geq 3$ and by the weight of $g(x)$ we have $d(\mathrm{C}) \leq 3$. So we conclude that $d(\mathrm{C}) = 3$.

4.3 Decoding Codes with Gröbner Bases Method

The idea of using Gröbner bases in decoding problems is by associating a certain polynomial system over a finite field to a non codeword such that the solution of the polynomial system of equations corresponds to the error vector.

Let C be a linear code and $v \in \mathbb{F}_q^n$. Decoding problem is the problem of finding the closest codeword $\mathcal{D}(v) \in \mathrm{C}$ to v, if it exists, with respect to the Hamming distance. However, as we have seen in theorem 4.1.7, a linear code only has correction capability up to $\tau := \lfloor \frac{d-1}{2} \rfloor$ errors. Hence we need to restrict the decoding problem for all non codewords v which satisfy

$$d(v, \mathrm{C}) = \min\{d(v, c) | c \in \mathrm{C}\} \leq \tau.$$

If $d(v, \mathrm{C}) \leq \tau$, then there exists a unique codeword $\mathcal{D}(v) \in \mathrm{C}$ such that $d(v, \mathrm{C}) = d(v, \mathcal{D}(v))$.

Definition 4.3.1. Let H be a parity check matrix for a linear code C and let $v \in \mathbb{F}_q^n$. Then the vector $s \in \mathbb{F}_q^{n-k}$ satisfying $s^T = Hv^T$ is called the syndrome of v and it is denoted by $s(v)$.

So the syndrome of v is zero if and only if v is a codeword in C. Otherwise, there are errors occurring during the transmission.

Definition 4.3.2. Two words v and u in $\mathbb{F}_q^n$ are said related if and only their syndromes are equal, i.e., $Hv^T = Hu^T$. If v and u are related we denote it by $v \sim u$.

Lemma 4.3.3. The relation $\sim$ in definition 4.3.2 is an equivalence relation.

Suppose that $v = c + e$ be a received word composed of a codeword $c \in \mathrm{C}$ and an error vector $e \in \mathbb{F}_q^n$ of weight at most τ. So by the property of parity check matrix of C we have the syndromes of v and e are equal. So, given $v \in \mathbb{F}_q^n$ with $s(v) = s$, we have the corresponding equivalence class $[v] = \{u \in \mathbb{F}_q^n \,|s(U) = s\}$. Hence we need to find the vector e of weight at most τ which has syndrome equals to s. The vector e is unique by theorem 4.1.7 and e is the error vector occurred in v. Therefore, to decode a received word v we go through the subset of $\mathbb{F}_q^n$ containing all vectors of weight i, where $i = 1, \ldots$ up to we reach where the vector e lies. The following algorithm shows how we find the vector e and recover the received word v systematically. The algorithm is called syndrome decoding algorithm.

Algorithm 2: Syndrome Decoding Algorithm

Input: A parity check matrix H of a linear code C, a received word $v \in \mathbb{F}_q^n$ of distance to C at most τ.

Output: The unique codeword $\mathcal{D}(v)$.

```
Hv^T := s^T;
i := 1;
if s = 0 then
    v is a codeword and D(v) := v.
else
    Compute:
    E_i := {e ∈ F_q^n | wt(e) = i};
    HE_i^T := {He^T | e ∈ E_i};
    while s^T ∉ HE_i^T do
        i:=i+1;
    Take the element e ∈ E_i such that s^T = He^T and compute
     D(v) := v − e.
```

Remark. The number of elements of $\mathbb{F}_q^n$ of weight i is equal to $\binom{n}{i}(q-1)^i$. Hence if the worst case happens, i.e., the number of errors occurred is equal to τ, then the complexity of the algorithm is $\mathcal{O}(n^\tau(q-1)^\tau)$. Therefore, the algorithm is not really efficient even if we work on binary codes as the complexity is still polynomial in term of the length n of the codes. So we need more efficient methods to solve such decoding problems.

4.3.1 Decoding Cyclic Codes with Gröbner Bases

There are several methods for decoding cyclic codes. One of the first approaches using non-linear system of equations was formulated by Cooper in [12]. Another method for decoding cyclic codes by using Gröbner bases is Newton identities method in [3], [4], [8], and [9]. In this part we discuss Cooper philosophy, and we provide some examples to describe how we use Gröbner bases in this method.

Let $\mathbb{F}_{q^m}$ be the splitting field of $x^n - 1$ over $\mathbb{F}_q$ with $\gcd(n, q) = 1$ and let $\alpha \in \mathbb{F}_{q^m}$ be a root of unity of order n. Let C be the $[n, k, d]_q$ cyclic code with generator polynomial $g(x)$ and complete defining set $S_{\mathrm{C}} = \{i_1, \ldots, i_r\}$ with $r = n - k$ as we have in definition 4.2.9. So

$$H = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \ldots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \ldots & \alpha^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{i_r} & \alpha^{2i_r} & \ldots & \alpha^{(n-1)i_r} \end{pmatrix} \tag{4.2}$$

is a parity check matrix of C. Now we write all codewords and words in terms of polynomials, i.e., for every vector $v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$ we associate it with

$v(x) = \sum_{i=0}^{n-1} v_i x^i$. Let $v = c + e$ be a received word with error vector e of weight at most τ. Then by the equality

$$s^T = Hv^T = He^T,$$

for all $i \in S_{\mathrm{C}}$ we have $s_i = e(\alpha^i)$. Therefore, we have the following $\mathbb{F}_q$-algebra morphism

$$\begin{aligned} \Phi : \mathrm{C}_{q,n} = \mathbb{F}_q[x]/(x^n - 1) &\longrightarrow \mathbb{F}_{q^m}^r \\ f &\longmapsto (f(\alpha^{i_1}), f(\alpha^{i_2}), \ldots, f(\alpha^{i_r})) \end{aligned}$$

with kernel is equal to C. Therefore we have all entries of the syndrome s of v:

$$s_{i_u} = v(\alpha^{i_u}) = e(\alpha^{i_u}) = \sum_{j=0}^{n-1} e_j (\alpha^{i_u})^j, \ 1 \leq u \leq r. \tag{4.3}$$

The $e_j \neq 0$ if and only if there is error occured on the coordinate j of v. Moreover, if $J = \{j_1, \ldots, j_l\}$ with $l \leq \tau$ is the set of indices on which $e_j \neq 0$, then we may reduce the summation in the equations 4.3 to be

$$s_{i_u} = v(\alpha^{i_u}) = e(\alpha^{i_u}) = e_{j_1}(\alpha^{i_u})^{j_1} + \cdots + e_{j_l}(\alpha^{i_u})^{j_l}, \ 1 \leq u \leq r.$$

So $j_1, \ldots, j_l$ refers to the error locations and $e_{j_1}, \ldots, e_{j_l}$ refers to the error values.

Since we assume that the number of errors occured is at most τ, we introduce the variables $x_1, \ldots, x_\tau$ and $z_1, \ldots, z_\tau$, where x_l stands for the error locations and z_l stands for the error values. So $x_l := \alpha^{j_l}$ and $z_l := e_{j_l}$ is a solution to the equations

$$s_{i_u} = \sum_{l=1}^{\tau} z_l x_l^{i_u}, \ 1 \leq u \leq r. \tag{4.4}$$

Now we will show how to find the value of x_l which are the error locations of a received word. After we find the value of the x_l we are able to compute the error values z_l by using Gaussian elimination on the equation 4.4. To find the values of x_l we are going to consider Cooper's philosophy or also know as the power sum method.

In order to specify which values of the variables that are allowed in equations 4.4, we consider some additional equations to the system of equations we have in 4.4:

- Since α is an n-th root of unity, we add $x_l^n = 1$ for all $1 \leq l \leq \tau$;
- Since $e_{j_l} \in \mathbb{F}_q^*$, we add $z_l^q = z_l$ for all $1 \leq l \leq \tau$;
- To ensure that for each distinct pair k and l we have distinct values for x_k and x_l, we add $x_k x_l p(n, x_k, x_l) = 0$ for all $1 \leq k < l \leq \tau$ where

$$p(n, x, y) = \frac{x^n - y^n}{x - y} = \sum_{i=0}^{n-1} x^i y^{n-1-i}.$$

Because we do not know how many errors occurred, we use w as the variable for the number of weight of the error vector e. Therefore we have an ideal in $\mathbb{F}_q[x, z]$ where $x = (x_1, \ldots, x_w)$ and $z = (z_1, \ldots, z_w)$ generated by the following system of equations:

$$\text{Cooper}_{q,r,w}(x, z) = \begin{cases} \sum_{l=1}^{w} z_l x_l^{i_u} = s_{i_u} & 1 \leq u \leq r; \\ x_l^n = 1 & 1 \leq l \leq w; \\ z_l^q = z_l & 1 \leq l \leq w; \\ x_k x_l p(n, x_k, x_l) & 1 \leq k < l \leq w. \end{cases}$$

Hence the decoding problem can be transformed into the problem of finding the reduced Gröbner basis of the ideal generated by the system of equations.

Let I be an ideal in $\mathbb{F}[x_1, \ldots, x_n]$ for some field $\mathbb{F}$ with finitely many zeros and all are defined over $\mathbb{F}$. Let $V = V(I) \subset \mathbb{F}^n$ be the zero set of the ideal I. Then the zero set of $I \cap \mathbb{F}[x_1, \ldots, x_i]$ for some $i < n$ is equal to the projection of V on the first i coordinates. This fact and proposition 3.2.4 lead us to eliminate the variables $z_1, \ldots, z_w, x_2, \ldots, x_w$ in $\text{Cooper}_{q,r,w}(x, z)$ to find error locations of a received word. Indeed, if $(x_1, \ldots, x_w)$ is the x-part of a solution (x, z) to $\text{Cooper}_{q,r,w}(x, z)$, then any permutation of the x_i is also a solution (apply the same permutation on the z-part of the solution). Hence every error-locators will appear as the first coordinate of the x-part of a solution to $\text{Cooper}_{q,r,w}(x, z)$. Therefore, we need an elimination ordering to compute a Gröbner basis of the ideal generated by $\text{Cooper}_{q,r,w}(x, z)$. To do this we choose the lexicographic ordering $\prec$ with $x_1 \prec, \ldots, x_w \prec z_w \prec, \ldots, \prec z_1$. Hence the elimination ideal $(\text{Cooper}_{q,r,w}(x, z)) \cap \mathbb{F}_{q^m}[x_1]$ will contain a unique polynomial g where the roots of g are the error-locators we are looking for.

Proposition 4.3.4. Let v be a received word with the number of errors occured is $t \leq \tau$ and let $g(x_1)$ be the monic generator of the ideal $(\text{Cooper}_{q,r,t}(x, z)) \cap \mathbb{F}_{q^m}[x_1]$. Then the zeros of g are the error-locators of the received word v.

Proof. See [10], proposition 3.6, page: 264. □

The generator we obtained from proposition 4.3.4 will be called the error-locator polynomial and it is denoted as $l(x_1)$.

Theorem 4.3.5. Let v be a received word with the number of errors occured is $t \leq \tau$ and $\text{Cooper}_{q,r,w}(x, z)$ be its corresponding system of equations. Let $l(x_1)$ denote the error-locator polynomial from proposition 4.3.4. Let $g(x_1)$ be the generator of the ideal $(\text{Cooper}_{q,r,w}(x, z)) \cap \mathbb{F}_{q^m}[x_1]$. Then

$$g(x_1) = \begin{cases} 1 & \text{if } w < t; \\ l(x_1) & \text{if } w = t. \end{cases}$$

Proof. See [10], theorem 3.7, page: 264. □

Therefore, to decode a received word v we perform the following algorithm:

Algorithm 3: Cooper Philosophy

Input: A parity check matrix H of a linear code C as in 4.2 , a received word $v \in \mathbb{F}_q^n$ of distance to C at most τ.

Output: The unique codeword $\mathcal{D}(v)$.

Begin
  $vH^T := s$;
  if $s = 0$ **then**
    v is a codeword and $\mathcal{D}(v) := v$.
  else
    $w := 1$;
    $G : \{1\}$
    while $1 \in G$ **do**
      $G := Grobner(\text{Cooper}_{q,r,w}(x, z))$;
      $w := w + 1$;
    Compute the roots of the unique element $g(x_1) \in G \cap \mathbb{F}_{q^m}[x_1]$;
    Apply Gaussian elimination on the system 4.4;
    Find the error vector e from the solution of the system 4.4;
    $\mathcal{D}(v) := v - e$.
  Return $\mathcal{D}(v)$;
End

We give some examples to describe how to use the algorithm above:

Example 4.3.1. Let C be the $[7, 4]_2$ cyclic code as in example 4.2.2. The generator polynomial of C is $g(x) = x^3 + x + 1$ and we have the correction capability is $\tau = 1$. Suppose that $\alpha \in \mathbb{F}_8$ is a root zero of $g(x)$. Then α^2 and α^4 are also zeros of $g(x)$ by Frobenius automorphism. So $S_{\text{C}} = \{1, 2, 4\}$ and we have its parity check matrix:

$$H = \begin{pmatrix} 1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}.$$

Suppose that we the transmitted code is $c = (1, 0, 0, 0, 1, 1, 0))$ but we received $v = (1, 0, 0, 0, 1, 0, 0)$. Then we have

$$\text{Cooper}_{2,3,1}(x, z) = \begin{cases} z_1 x_1 = 1 + \alpha^4; \\ z_1 x_1^2 = 1 + \alpha; \\ z_1 x_1^3 = 1 + \alpha^2; \\ x_1^7 = 1; \\ z_1^2 = z_1. \end{cases}$$

Hence by using SINGULAR we obtain a Gröbner basis for $\text{Cooper}_{7,3,1}(x, z)$ with respect to the lexicographic $\prec$ with $x_1 \prec z_1$ which is an elimination ordering, $G = \{z_1 + 1, x_1 + (\alpha^2 + \alpha + 1\}$. So we can determine the error vector $e = (e_0, e_1, \ldots, e_6)$: Since $x = \alpha^2 + \alpha + 1$, then the error position is the coordinate

j such that $\alpha^j = \alpha^2 + \alpha + 1$ which is $j = 5$ as we have from $\alpha^3 + \alpha + 1 = 0$ and $\alpha^5 = \alpha^3 + \alpha^2$. Since the error value is $z_1 = 1$, the error vector is $e = (0, 0, 0, 0, 0, 1, 0)$ and we get the original code $c = v - e$.

Example 4.3.2. Let C be the $[6, 3]_7$ cyclic code as in example 4.2.1. The generator polynomial of C is $g(x) = x^3 + 3x^2 + x + 6$ with $3, 2$ and 6 are its zeros. Hence $S_{\mathrm{C}} = \{1, 2, 3\}$ and we have its parity check matrix:

$$H = \begin{pmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \end{pmatrix}.$$

Suppose that we have sent $c = (1, 1, 1, 1, 1, 1)$ but we received $v = (1, 1, 2, 1, 1, 1)$. Then we have

$$\mathrm{Cooper}_{7,3,1}(x, z) = \begin{cases} z_1 x_1 = 2; \\ z_1 x_1^2 = 4; \\ z_1 x_1^3 = 1; \\ x_1^6 = 1; \\ z_1^7 = z_1. \end{cases}$$

Hence by using SINGULAR we obtain a Gröbner basis for $\mathrm{Cooper}_{7,3,1}(x, z)$ with respect to the lexicographic $\prec$ with $x_1 \prec z_1$ which is an elimination ordering,, $G = \{z_1 - 1, x_1 - 2\}$. So we can determine the error vector $e = (e_0, e_1, \ldots, e_5)$: Since $x = 2$, then the error position is the coordinate j such that $3^j = 2$ which is $j = 2$ and the error value is 1. So the error vector is $e = (0, 0, 1, 0, 0, 0)$ and the transmitted code is $v - e = c$.

Now in the following example we consider one of subclass of cyclic codes namely Reed-Solomon (RS) codes.

Definition 4.3.6. Let q be a power of some prime p and let α be a primitive element, i.e., a generator of $\mathbb{F}_q^*$. Let $n = q - 1$. Let b and k be non-negative integers with $0 \leq b, k \leq n$. A RS code is a cyclic code with generator polynomial

$$g_{b,k}(x) = (x - \alpha^b) \ldots (x - \alpha^{b+n-k-1})$$

and it is denoted by $RS_k(n, b)$.

Proposition 4.3.7. The code $RS_k(n, b)$ with $n = q - 1$, is MDS of dimension k and $(RS_k(n, b))^{\perp} = RS_{n-k}(n, n - b + 1)$. Moreover, the complete defining set of $\mathrm{C} = RS_k(n, b)$ is $S_{\mathrm{C}} = \{b, b + 1, \ldots, b + n - k - 1\}$

Proof. See [25], page:201. □

Example 4.3.3. Now we consider the code $RS_3(7, 1)$. It is a cyclic code over $\mathbb{F}_8$ with generator polynomial

$$g_{1,3}(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4)$$

where $\alpha^3 = \alpha + 1$. So the minimum distance of $RS_3(7,1)$ is 5 and hence the correction capability is $\tau = 2$. By the generator matrix $g_{1,3}(x)$, we have its corresponding parity check matrix:

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}.$$

Suppose that we the transmitted code is $c = (1,1,1,1,1,1,1)$ but we received $v = (1,1,0,1,1,0,1)$. Then we have

$$\text{Cooper}_{2,3,1}(x,z) = \begin{cases} z_1 x_1 = 1 + \alpha + \alpha^3 + \alpha^4 + \alpha^6; \\ z_1 x_1^2 = 1 + \alpha^2 + \alpha^6 + \alpha + \alpha^5; \\ z_1 x_1^3 = 1 + \alpha^3 + \alpha^2 + \alpha^5 + \alpha^4; \\ z_1 x_1^4 = 1 + \alpha^4 + \alpha^5 + \alpha^2 + \alpha^3; \\ x_1^7 = 1; \\ z_1^2 = z_1. \end{cases}$$

Hence by using SINGULAR we obtain a Gröbner basis for $\text{Cooper}_{7,3,1}(x,z)$ with respect to the lexicographic $\prec$ with $x_1 \prec z_1$ which is an elimination ordering, $G_1 = 1$. So we continue to compute a Gröbner basis G_2 for

$$\text{Cooper}_{2,3,2}(x,z) = \begin{cases} z_1 x_1 + z_2 x_2 = 1 + \alpha + \alpha^3 + \alpha^4 + \alpha^6; \\ z_1 x_1^2 + z_2 x_2^2 = 1 + \alpha^2 + \alpha^6 + \alpha + \alpha^5; \\ z_1 x_1^3 + z_2 x_2^3 = 1 + \alpha^3 + \alpha^2 + \alpha^5 + \alpha^4; \\ z_1 x_1^4 + z_2 x_2^4 = 1 + \alpha^4 + \alpha^5 + \alpha^2 + \alpha^3; \\ x_1^7 = 1; \\ x_2^7 = 1; \\ z_1^2 = z_1; \\ z_2^2 = z_2. \end{cases}$$

Again by SINGULAR we have $G_2 \cap \mathbb{F}_8[x_1] = x_1^2 + (\alpha)x + 1$ with respect to the lexicographic $\prec$ with $x_1 \prec x_2 \prec z_2 \prec z_1$ which is an elimination ordering. Moreover, the roots of $x_1^2 + (\alpha)x + 1$ are α^2 and α^5 which are the error locators. So the error occured at the coordinate e_2 and e_5. By using the roots of $x_1^2 + (\alpha)x + 1$ we obtain the error vector $e = (0,0,1,0,0,1,0)$.

Remark. The decoding process described above requires us to compute a Gröbner bases for $\text{Cooper}_{q,r,w}(x,z)$ every time we receive y. This would certainly take too much time to be practical. Instead of computing a Gröbner bases for every such word, it is nicer to compute a Gröbner basis one time which works for every y we receive. To do this we need to treat all syndromes s_i as variables and work on a bigger polynomial ring, namely the ring $T[s_1, \ldots, s_r]$ where T is the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_w, z_1, \ldots, z_w]$. The advantage is now one only needs to compute a single Gröbner basis for decoding words with exactly $t \leq \tau$ errors. But the disadvantage is an increase time and storage consuming for the computations of Gröbner bases as we work on a bigger polynomial ring. For more detail, see [25].

4.3.2 Decoding Linear Codes with Gröbner Bases

There are several methods for decoding arbitrary linear codes using Gröbner bases as the main tools, namely, Fitzgerald-Lax method in [17], decoding by embedding in MDS code, decoding by normal form computation in [5], etc. In this part we discuss the Fitzgerald-Lax method, and we provide examples to describe how to use this method.

Fitzgerald-Lax Method:

The main idea of this method is representing linear codes as another class of codes which we call affine variety codes.

Definition 4.3.8. Let $q = p^r$ for some prime p and positive integer r. Let $\mathbb{F}_q$ be the finite field with q elements and $\overline{\mathbb{F}}_q$ be the closure of $\mathbb{F}_q$. Let S be a subset of $\mathbb{F}_q[x_1, \ldots, x_m]$. The set of all simultaneous solutions of S in $\overline{\mathbb{F}}_q^m$,

$$V(S) := \{(a_1, \ldots, a_m) \in \overline{\mathbb{F}}_q^m) | \forall f \in S, f(a_1, \ldots, a_m) = 0\},$$

is called the affine variety of S.

Definition 4.3.9. Let Y be a subset of $\overline{\mathbb{F}}_q^n$. The set of all polynomials in $\mathbb{F}_q[x_1, \ldots, x_s]$ which vanish on Y is denoted by $\mathcal{I}(Y)$.

Remark.

- If I is the ideal generated by S, then $V(I) = V(S)$;
- For any subset Y of $\overline{\mathbb{F}}_q^m$, $\mathcal{I}(Y)$ is an ideal in $\mathbb{F}_q[x_1, \ldots, x_m]$;
- By Hilbert's Nullstellensatz, for any ideal I of $\mathbb{F}_q[x_1, \ldots, x_m]$, we have $\mathcal{I}(V(I)) = \sqrt{I}$ and $V(I) = V(\mathcal{I}(V(I))) = V(\sqrt{I})$, where $\sqrt{I}$ denotes the radical of I.

An element $(a_1, \ldots, a_n)$ of $V(S)$ is called a point of $V(S)$ and all points of $V(S)$ whose coordinates lie in $\mathbb{F}_q$ are called the $\mathbb{F}_q$-rational points of $V(S)$.

Proposition 4.3.10. Let I be an ideal of $\mathbb{F}_q[x_1, \ldots, x_m]$. Then the $\mathbb{F}_q$-rational points of $V(I)$ are the points of $V(I_q)$ where $I_q = I + (x_1^q - x_1, \ldots, x_m^q - x_m)$.

Proof. Since $I \subseteq I_q$, we have $V(I_q) \subseteq V(I)$. Let $(a_1, \ldots, a_m) \in V(I_q)$. Since $f_i = x_i^q - x \in I_q$, we have $f_i(a_1, \ldots, a_m) = 0$. Therefore, by the property that $a_i \in \mathbb{F}_q$ if and only if $a_i^q = a_i$ we have $(a_1, \ldots, a_m)$ is an $\mathbb{F}_q$-rational point.

Conversely, let $(a_1, \ldots, a_m)$ be an $\mathbb{F}_q$-rational point of $V(I)$. Therefore, $a_i^q = a_i$ as $a_i \in \mathbb{F}_q$ and hence $f_i(a_1, \ldots, a_m) = 0$ for $f_i = x_i^q - x_i$. Moreover, since $(a_1, \ldots, a_m) \in V(I)$ we have $g(a_1, \ldots, a_m) = 0$ for all $g \in I$. Therefore we have $(a_1, \ldots, a_m)$ is a zero of any polynomial of the form

$$g(x_1, \ldots, x_m)l(x_1, \ldots, x_m) + \sum_{i=1}^{m} h_i(x_1, \ldots, x_m)(x_i^q - x_i).$$

Hence $(a_1, \ldots, a_m) \in V(I_q)$. □

Now we are going to show that the ideals in $\mathbb{F}_q[x_1, \ldots, x_m]$ of the form I_q are radical. The following lemma from Seidenberg is useful to show such ideals I_q are radical.

Lemma 4.3.11. (Seidenberg's Lemma 92) Let $J \subset \mathbb{F}_q[x_1, \ldots, x_m]$ be a zero dimensional ideal, i.e., $V(J)$ is finite, and assume that for $1 \leq i \leq m$, J contains a polynomial $f_i \in \mathbb{F}_q[x_i]$ with $\gcd(f_i, f_i') = 1$. Then J is an intersection of finitely many maximal ideals. Particularly, J is a radical ideal.

Proof. See lemma 92 in [27]. □

Since $\mathbb{F}_q$ consist of q elements, $V(I)$ contains at most q^m $\mathbb{F}_q$-rational points and so $V(I_q)$ is finite.

Corollary 4.3.12. Let I be an ideal of $\mathbb{F}_q[x_1, \ldots, x_m]$. Then I_q is a radical ideal.

Proof. Since $V(I_q)$ is finite, I_q is a zero dimensional ideal. By lemma 92 in [27], it is enough to show that $\gcd(f_i, f_i') = 1$ for $f_i = x_i^q - x_i$, $1 \leq i \leq m$. The formal derivative f_i' is $qx_i^{q-1} - 1 = -1$ as the characteristic of $\mathbb{F}_q$ is p which means $\gcd(f_i, f_i') = 1$. □

We need the following isomorphism of vectors to construct an affine variety code.

Lemma 4.3.13. Let $R := \mathbb{F}_q[x_1, \ldots, x_m]/I_q$ for some ideal I of $\mathbb{F}_q[x_1, \ldots, x_m]$. Let n be the number of points of $V(I_q)$. Then the map ϕ defined by

$$\phi : R \to \mathbb{F}_q^n$$

$$\overline{f} \mapsto (f(P_1), \ldots, f(P_n)),$$

where $\overline{f}$ is the image of f under the quotient map from $\mathbb{F}_q[x_1, \ldots, x_m]$ onto R and P_i are the distinct elements in $V(I_q)$, is an isomorphism of $\mathbb{F}_q$-vector spaces.

Proof. Suppose that $\bar{f}_1 = \bar{f}_2$. Then $f_2 = f_1 + g$ for some $g \in I_q$. Therefore, for every $P \in V(I_q)$ we have $f_2(P) = f_1(P) + g(P) = f_1(P)$ as $g \in I_q$. Then $\phi(\bar{f}_1 = \phi(\bar{f}_2$ and so ϕ is well-defined.

We are going to show that the map is injective. Let $\bar{f}_1$ and $\bar{f}_2$ are in R such that $\phi(\bar{f}_1 = \phi(\bar{f}_2$. Then $\phi(\bar{f}_1 - \bar{f}_2) = 0 \in \mathbb{F}_q^n$ which means $f_1 - f_2$ is zero at every point of $V(I_q)$. By he Nullstellensatz, that implies $f_1 - f_2$ is in $\sqrt{I_q}$, but I_q is radical so $f_1 - f_2 \in I_q$ and $\bar{f}_1 - \bar{f}_2 = 0$.

Furthermore, I_q is the intersection of the n maximal ideals corresponding to each distinct point $P_i \in V(I_q)$ as I_q is radical. By the Chinese Remainder theorem, R is of dimension n as a vector space of $\mathbb{F}_q$ and hence the map is surjective. □

Definition 4.3.14. Let I be an ideal of $\mathbb{F}_q[x_1, \ldots, x_m]$ and let L be an $\mathbb{F}_q$-vector subspace of $R := \mathbb{F}_q[x_1, \ldots, x_m]/I_q$. Let ϕ be the isomorphism in lemma 4.3.13. We define the affine variety code $\mathrm{C}(I, L)$ as the image $\phi(L)$ of L.

Note that different numbering of the points $P_1, \ldots, P_n$ of $V(I_q)$ gives different linear codes. But they are still equivalent, i.e., two codes C_1 and C_2 are equivalent if a generator matrix of C_1 can be obtained by a column permutation of a generator matrix of C_2.

Theorem 4.3.15. (Fitzgerald and Lax in [16]) Let C be any linear code over $\mathbb{F}_q$ of length n of dimension k. Then there exist a positive integer m which is the least integer satisfying $q^m \geq n$, an ideal $I \subset \mathbb{F}_q[x_1, \ldots, x_m]$ and a subspace $L \subset R$ such that $\mathrm{C} = \mathrm{C}(I, L)$.

Proof. Let C be a linear code over $\mathbb{F}_q$ of length n and dimension k. Let $G = [c_{ij}]$ with $1 \leq i \leq k$ and $1 \leq j \leq n$ be a generator matrix of C. Let m be the least integer satisfying $q^m \geq n$. Let $Y = \{P_1, \ldots, P_n\} \subseteq \mathbb{F}_q^m$ where P_i's are distinct and let $I = \mathcal{I}(Y)$. We write all points in $\mathbb{F}_q^m$ by $P_j = (a_{j1}, \ldots, a_{jm})$. Consider the following polynomial

$$\mathcal{X}_{P_j}(x_1, \ldots, x_m) = \prod_{l=1}^{m} (1 - (x_l - a_{jl})^{q-1}).$$

By Delsarte, Goethals and MacWilliams in [18], the polynomial $\mathcal{X}_{P_j}$ is zero at every point in $\mathbb{F}_q^m$ except at P_j where the value is 1.

Consider the following polynomials

$$\bar{f}_i = \sum_{j=1}^{n} c_{ij} \bar{\mathcal{X}}_{P_j}$$

for $i = 1, \ldots, k$ and $\bar{\mathcal{X}}_{P_j}$ is the image of $\mathcal{X}_{P_j}$ in the quotient ring $\mathbb{F}_q[x_1, \ldots, x_m]/I_q$. Let $L = (\bar{f}_1, \ldots, \bar{f}_k)$. Then $\mathrm{C} = \mathrm{C}(I, L)$. □

Example 4.3.4. Let C be the $[8, 4, 4]_3$ linear code with generator matrix:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

We order the points of $\mathbb{F}_3^2$ as follows: $P_1 = (0,0), P_2 = (0,1), P_3 = (0,2), P_4 = (1,0), P_5 = (1,1), P_6 = (1,2), P_7 = (2,0), P_8 = (2,1), P_9 = (2,2)$. Consider the first eight points of $\mathbb{F}_3^2$. Therefore, by Delsarte, Goethals and MacWilliams in [18], the ideal $I \subseteq \mathbb{F}_3[x, y]$ such that $V(I_3) = \{P_1, \ldots, P_8\}$ is generated by the polynomials $\mathcal{X}_{P_9} = (-x^2 + 4x - 3)(-y^2 + 4y - 3)$. Now we compute $f_i = \sum_{j=1}^{n} c_{ij} \mathcal{X}_{P_j}$ for $i = 1, 2, 3, 4$:

- $f_1 = (1 - x^2)(1 - y^2) + (-x^2 + 2x)(-y^2 + 4y - 3) + (-x^2 + 4x - 3)(1 - y^2) + (-x^2 + 4x - 3)(-y^2 + 2y)$;
- $f_2 = (1 - x^2)(-y^2 + 2y) + (-x^2 + 2x)(-y^2 + 2y) + (-x^2 + 4x - 3)(1 - y^2) + (-x^2 + 4x - 3)(-y^2 + 2y)$;

- $f_3 = (1-x^2)(-y^2+4y-3)+(-x^2+2x)(-y^2+2y)+(-x^2+4x-3)(1-y^2)+(-x^2+4x-3)(-y^2+2y)$;
- $f_4 = (-x^2+2x)(1-y^2)+(-x^2+2x)(-y^2+2y)+(-x^2+4x-3)(1-y^2)+(-x^2+4x-3)(1-y^2)$.

Thus by theorem 4.3.15, we have the code C is $\mathrm{C}(I,L)$ where I is the ideal generated by $(-x^2+4x-3)(-y^2+4y-3)$ and $L = \langle \bar{f}_1, \bar{f}_2, \bar{f}_3, \bar{f}_4 \rangle$ with $\bar{f}_i$ is the image of f_i in $\mathbb{F}_3[x,y]/I_3$.

To do decoding, it is more convenient to represent a linear code C as an affine variety code of the form $\mathrm{C}^\perp(I,L)$ for some suitable ideal I and subspace L of $F_q[x_1,\ldots,x_m]/I_q$ because we would like to work with syndromes. So instead we start with a generator matrix G in theorem 4.3.15, we use a parity check matrix. Let C be a linear code over $\mathbb{F}_q$ of length n and dimension k. Let $\mathrm{C}^\perp(I,L)$ be the corresponding affine variety code of C, where

$$\begin{cases} I & = (g_1,\ldots,g_l) \subseteq \mathbb{F}_q[x_1,\ldots,x_m]; \\ L & = (\bar{f}_1,\ldots,\bar{f}_{n-k}) \subseteq \mathbb{F}_q[x_1,\ldots,x_m]/I_q; \\ V(I_q) & = \{P_1,\ldots,P_n\}. \end{cases}$$

Then by the construction of C in theorem 4.3.15, we have a parity check matrix H for C where $H = [f_i(P_j)]$ with $i = 1,\ldots,n-k$ and $j = 1,\ldots n$.

Let y be a received word and let $s = (s_1,\ldots,s_{n-k})$ be the syndrome of y. Then we have $s_i = \sum_{j=1}^n y_j f_i(P_j)$. Moreover, if $y = c + e$ for some $c \in \mathrm{C}$ and e is the error vector, then $s_i = \sum_{j=1}^n e_j f_i(P_j)$. Hence the points $P_j \in V(I_q)$, on which $f_i(P_j)$ is nonzero, corresponds to the error locations and we call these points as error points.

Like cyclic codes case in previous subsection, we need to find the error positions and the error values for each position. Now we restrict the case when the number of errors t occurred is at most $\tau := \lfloor \frac{d-1}{2} \rfloor$, to make sure that the error vector e such that $y - e \in \mathrm{C}$ is unique.

Definition 4.3.16. Let $y \in \mathbb{F}_q^n$ which has nonzero syndrome $s = (s_1,\ldots,s_{n-k})$. Let $w \leq \tau$ be the variable for the number of errors occured in y. Let $z = (z_1,\ldots,z_w)$ and $x = (x_{11},\ldots,x_{1m},\ldots,x_{w1},\ldots,x_{wm})$. The error locator ideal $\mathcal{E}_w(y) \subseteq \mathbb{F}_q[x,z]$ of the received word y is defined as the ideal generated by

$$\begin{cases} \sum_{j=1}^w z_j f_i(x_{j1},\ldots,x_{jm}) - s_i) & 1 \leq i \leq n-k; \\ g_h(x_{j1},\ldots,x_{jm}) & 1 \leq h \leq l; \\ z_j^{q-1} - 1 & 1 \leq j \leq w. \end{cases}$$

Note that the variables $x_{j1},\ldots,x_{jm}$ for $j = 1,\ldots,w$ correspond to coordinates of each error points of $V(I_q)$ and the variables $z_1,\ldots,z_w$ correspond to the error values at those errors points. Moreover, let t be the number of errors occured in y. As we have in cyclic case, if $w < t$ the ideal $\mathcal{E}_w(y)$ has no solution. If $w = t$, then the ideal yields all information about the error vector of y. Therefore, the problem of decoding has been translated into the problem of computing a Gröbner basis of $\mathcal{E}_w(y)$.

Definition 4.3.17. Define the projection map $\pi : \mathbb{F}_q^{w+mw} \to \mathbb{F}_q^{1+m}$ by

$$\pi(u) = \pi(x_{11}, \ldots, x_{1m}, \ldots, x_{w1}, \ldots, x_{wm}, z_1, \ldots, z_w) = (x_{11}, \ldots, x_{1m}, z_1).$$

J.Fitzgerald showed in [16] the following result, which makes easier to find the error points of $V(I_q)$.

Proposition 4.3.18. $(x_{11}, \ldots, x_{1m}, \ldots, x_{w1}, \ldots, x_{wm}, z_1, \ldots, z_w) \in V(\mathcal{E}_w(y))$ if and only if $(x_{11}, \ldots, x_{1m}, z_1) \in \pi(V(\mathcal{E}_w(y))$.

Proof. See [16], proposition 2.2.13. □

Therefore, the proposition allows us to use elimination property of a Gröbner basis with respect to an elimination ordering on the variables $x_{11}, \ldots, x_{1m}, z_1$. Hence, to decode a received word v we perform the following algorithm:

Algorithm 4: Linear Code Decoding

Input: A parity check matrix H of a linear code $\mathrm{C} = \mathrm{C}^{\perp}(I, L)$, a received word $v \in \mathbb{F}_q^n$ of distance to C at most τ, an elimination ordering $\prec$.

Output: The unique codeword $\mathcal{D}(v)$.

```
Begin
Hv^T := s^T;
if s = 0 then
    v is a codeword and D(v) := v.
else
    w := 1;
    G : {1};
    while 1 ∈ G do
        G := Grobner(E_w(v));
        w := w + 1;
    Use the elimination property to compute V(G ∩ F_q[x_11, ..., x_1m, z_1]);
    Determine the error points which correspond to the error locations;
    Compute the error vector e;
    D(v) := v − e.
Return D(v);
End
```

In the example below we give step by step how to use the algorithm above. The example is by Fitzgerald:

Example 4.3.5. Let $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ with $\alpha^2 = \alpha + 1$. Let $I = (y^2 + y - x^3) \subset \mathbb{F}_4[x, y]$ and $R = \mathbb{F}_4[x, y]/I_4$. The points of $V(I_4)$ are the $\mathbb{F}_4$-rational points of $V(I)$ which are $P_1 = (0, 0)$, $P_2 = (0, 1)$, $P_3 = (1, \alpha)$, $P_4 = (1, \alpha^2)$, $P_5 = (\alpha, \alpha)$, $P_6 = (\alpha, \alpha^2)$, $P_7 = (\alpha^2, \alpha)$, $P_8 = (\alpha^2, \alpha^2)$. Let $L = \langle 1, \bar{x}, \bar{y}, \bar{x}^2, \bar{x}\bar{y} \rangle$. Then the code $\mathrm{C} = \mathrm{C}^{\perp}(I, L)$ has minimum distance 5 by [32]. Therefore we have a parity

check matrix of $\mathrm{C} = \mathrm{C}^{\perp}(I, L)$ is

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha^2 & \alpha & \alpha \\ 0 & 0 & \alpha & \alpha^2 & \alpha^2 & 1 & 1 & \alpha \end{pmatrix}.$$

Suppose that the error vector is $e = (0, 0, 1, 0, 0, \alpha, 0, 0)$. Then the syndrome of y is $s = (\alpha^2, \alpha, \alpha^2, 0, 0)$. Hence the error locator ideal $\mathcal{E}$ is the ideal in $\mathbb{F}_4[x_1, y_1, x_2, y_2, z_1, z_2]$ generated by the following polynomials:

$$\begin{aligned} &z_1^3 - 1, z_2^3 - 1, \\ &x_1^4 - x_1, x_2^4 - x_2, y_1^4 - y_1, y_2^4 - y_2, \\ &y_1^2 + y_1 - x_1^3, y_2^2 + y_2 - x_2^3, \\ &z_1 + z_2 - \alpha^2, z_1x_1 + z_2x_2 - \alpha, z_1x_1^2 + z_2x_2^2, z_1x_1y_1 + z_2x_2y_2. \end{aligned}$$

By using the lexicographic $\prec$ with $x_1 \prec y_1 \prec z_1 \prec x_2 \prec y_2 \prec z_2$ which is an elimination ordering we can obtain a Gröbner basis G with respect to $\prec$ via the computer program SINGULAR:

$$G = \{x_1^2 + \alpha^2 x_1 + \alpha, y_1 + \alpha x_1, z_1 + x_1, x_2 + x_1 + \alpha^2, y_2 + \alpha x_1 + 1, z_2 + x_1 + \alpha^2\}.$$

By proposition 4.3.18, we only need to consider $G \cap \mathbb{F}_4[x_1, y_1, z_1] = \{x_1^2 + \alpha^2 x_1 + \alpha, y_1 + \alpha x_1, z_1 + x_1\}$ where the first coordinates of the error points are the roots of $x_1^2 + \alpha^2 x_1 + \alpha$ which are α and 1. When we substitute the values of x_1 in $y_1 + \alpha x_1 = 0$, we obtain the two error points $P_3 = (1, \alpha)$ and $P_6 = (\alpha, \alpha^2)$ which correspond to the error positions 3 and 6 in e. Moreover, from the polynomial $z_1 + x_1 = 0$, we see that the error value at each point is the same as the first coordinate at that point.

One might wonder how if we treat a cyclic code using this method. The following example shows that using the algebraic properties of a cyclic code, namely its generator polynomial or equivalently its defining set, we will see that the ideal defined in definition 4.3.16 and the ideal $\mathrm{Cooper}_{q,r,w}(x, z)$ are really the same.

Example 4.3.6. Let $\mathbb{F}_{q^m}$ be the splitting field of $x^n - 1$ with $\gcd(n, q) = 1$ and let α is the root of unity of order n. Let C be a cyclic code with complete defining set S_{C}. By taking $V = \{1, \alpha, \ldots, \alpha^{n-1}\}$, we have

$$I := \mathcal{I}(V) = (X^n - 1)\,\mathbb{F}_{q^m}[x].$$

If we take the vector space $L = \langle x^j | j \in S_{\mathrm{C}} \rangle$ over $\mathbb{F}_{q^m}$, Then we have $\mathrm{C} = \mathrm{C}^{\perp}(I, L)$. Moreover, the ideal $\mathcal{E}_t$ defined in definition 4.3.16 and the ideal $\mathrm{Cooper}_{q,r,t}(x, z)$ are really the same.

Remark. The decoding process described above requires us to compute a Gröbner bases for $\mathcal{E}_w(y)$ every time we receive y. This would certainly take too much time to be practical. Instead of computing a Gröbner bases for every such word, it is nicer to compute a Gröbner basis one time which works for every y we receive. To do this we need to treat all syndromes s_i as variables and work on a bigger polynomial ring, namely the ring $T[s_1, \ldots, s_{n-k}]$ where T is the polynomial ring $\mathbb{F}_q[x_{11}, \ldots, x_{1m}, \ldots, x_{w1}, \ldots, x_{wm}, z_1, \ldots, z_w]$ where $1 \leq w \leq \tau$. The advantage is now one only needs to compute a single Gröbner basis for decoding words with exactly w errors. But the disadvantage is an increase in time and storage consuming for the computations of Gröbner bases as we work on a bigger polynomial ring. For more detail, see [17].

Bibliography

[1] B. Amrhein, O. Gloor, and W. Küchlin. *On The Walk*. Theoretical Computer Science, pages 179-202, 1997.

[2] M. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. University of Oxford, 1969.

[3] D. Augot, M. Bardet, and J.-C. Faugére. *On the Decoding of Cyclic Codes with Newton Identities*. J. Symb. Comp., Vol:44, pages:1606-1625, 2009.

[4] M. A. Boer and R. Pellikaan. *Gröbner Bases for Codes*. Chap.10 of: Some Tapas of Computer Algebra, Springer-Verlag, Berlin, 1999.

[5] M. Borges-Quintana, M. A. Borges-Trenard, P. Fitzpatrick, and E. Martinez-Moro. *Gröbner Bases and Combinatorics fro Binary Codes*. Appl. Algebra Eng. Comm. Comput., Vol:19, pages: 393-411, 2008.

[6] B. Buchberger. *A Criterion for Detecting Unnecessary Reduction in The Construction of Gröbner Basis*. Proceedings of EUROSAM, pages:3-21, Springer, 1979.

[7] B. Buchberger. *An Algorithm for Finding the Bases Elements of the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal (German)*. University of Innsbruck, Austria, 1965.

[8] S. Bulygin and R. Pellikaan. *Decoding and Finding the Minimum Distance with Gröbner Bases*. Series on Coding Theory and Cryptology, Vol:7, Pages:585-622, 2010.

[9] X.Chen, I.S. Reed, T. Helleseth, and T.K. Truong. *Algebraic Decoding of Cyclic Codes: A Polynomial point of view*. Contemporary Math. Vol. 168, pages:15-22, 1994.

[10] A. M. Cohen, H. Cuypers, H. Strerk. *Some Tapas of Computer Algebra*. Algorithms and computation in mathematics. Springer Verlag, New York, Berlin, Heidelberg, 1999.

[11] S. Collart, M. Kalkbrener, and D. Mall. *Converting Bases with the Gröbner Walk*. Camp. Linz. Bericht Nr.124, 1978.

[12] A. B. Cooper. *Toward a New Method of Decoding Algebraic Codes Using Gröbner Bases.* Transactions of the Tenth Army Conference on Applied Mathematics and Computing, pages: 1-11, 1993.

[13] D. A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer Publishing Company, Incorporated, 4th edition, 2015.

[14] P. Delsarte, J. M. Goethals, and F. J. MacWilliams. *On Generalized Reed-Muller Codes and their Relatives*. Information and Control, Vol. 16, pages:403-442, 1970.

[15] V. Ene, and J. Herzog. *Gröbner bases in Commutative Algebra*. American Mathematical Society, Rhode Island, 2010.

[16] J. Fitzgerald. *Applications of Gröbner Bases to Linear Codes*. Ph.D. Thesis, Louisiana State Un., 1996.

[17] J. Fitzgerald and R.F. Lax. *Decoding Affine Variety Codes Using Gröbner Bases*. Design. Code. Cryptogr., Vol:13, pages:147-158, 1998.

[18] R. Gebauer and H. Moller. *On an installation of Buchberger's algorithm*. Journal of Symbolic Computation, pages:275-286, 1988.

[19] P. Gritzmann and B. Sturmfels. *Minkowski Addition of Polytopes: Computational Complexity and Applications to Gröbner Bases*. SIAM J. Discrete Math, pages:246-269, 1993.

[20] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, New York, 1977.

[21] T. W. Hungerford. *Algebra*. Springer-Verlag, New York, 1997.

[22] N. Koblitz *Algebraic Aspects of Cryptography*. Algorithms and Computation in Mathematics, vol. 3, Springer, 1997.

[23] C. Kollreider. *Polynomial Reduction: The Influence of the Ordering of Terms on a Reduction Algorithm*. Journal of Symbolic Computation, pages 465-469, 1997.

[24] D. W. C. Kuijsters. *Coding theory a Gröbner basis approach*. Ph.D Thesis, Eindhoven University of Technology, 2017.

[25] R. Pellikaan, X. Wu, S. Bulygin, and R. Jurrius. *Codes, Cryptology and Curves with Computer Algebra*. Cambridge University Press, Cambridge, 2018.

[26] L. Robbiano. *Term Ordering on the Polynomial Ring*. EUROCAL 85, vol.2 (Linz,1985), Lecture Notes in Comput. Sci , Vol. 204, Springer, pages: 513-517, 1985.

[27] A. Seidenberg. *Constructions in Algebra.* Transactions of the American Mathematical Society, pages: 273-313, 1974.

[28] B. Sturmfels. *Gröbner Bases and Convex Polytopes.* University Lecture Series, Vol.8, AMS, Providence RI, 1996.

[29] Q.N. Tran. *A Fast Algorithm for Gröbner Basis Conversion and its Applications.* Journal of Symbolic Computation, pages: 451-467, 2000.

[30] Q.N. Tran. *Ideal Specified-term Orders for Elimination and Application in Implicitization.* Tenth International Conferenceon Application of Computer Algebra, pages: 15-25, 2005.

[31] Q.N. Tran. *A New Class of Term Orders for Elimination.* Journal of Symbolic Computation, pages: 533-548, 2007.

[32] K. Yang and P. V. Kumar. *On The True Minimum Distance of Hermitian Codes.* Coding Theory and Algebraic Geometry: Proceedings of AGCT-3, pages: 99-107, 1991.