Coding Theory via Groebner Bases

Vom Promotionsausschuss der
Technischen Universität Hamburg-Harburg

zur Erlangung des akademischen Grades

Doktorin der Naturwissenschaften

genehmigte Dissertation

von
Mehwish Saleemi

aus
Islamabad

2012

1. Gutachter: Prof. Dr. Karl-Heinz Zimmermann
   Institute für Rechnertechnologie, Technische Universität Hamburg-Harburg

2. Gutachter: Prof. Dr. Rudolf Scharlau
   Fakultät für Mathematik, Technische Universität Dortmund

Tag der mündlichen Prüfung: 14.02.2012

Vorsitzender des Prüfungsausschusses: Prof. Dr. Dieter Gollmann
Institut für Sicherheit in verteilten Anwendungen, Technische Universität Hamburg-Harburg

Abstract

Coding theory plays an important role in efficient transmission of data over noisy communication channels. It consists of two steps; the first step is to encode the data to reduce its sensitivity to noise during transmission, and the second step is to decode the received data by detecting and correcting the noise induced errors. In this thesis an algebraic approach is used to develop efficient encoding and decoding algorithms for a very commonly used class of linear codes, the Reed-Muller codes and the Golay codes.

To develop the approach first the algebraic structure of linear codes is explored. For this, the reduced Groebner basis for a class of ideals in commutative polynomial rings is constructed. The extension of these ideals to a residue class ring enabled us to find the parameters of the corresponding codes. It is found that the corresponding codes contains the primitive Reed-Muller codes. The added advantage of this approach is that, once these Groebner bases are constructed a standard procedure can be used to develop encoding and decoding processes. A binomial ideal, defined as a sum of toric ideal and a prime ideal over some arbitrary field, is explored. It is shown that this ideal is equal to a binomial ideal over a prime field. Purpose of proving this equivalence is to study binary codes associated to this ideal. Minimal generators and Groebner basis found for this ideal showed that the situation is quite closely related to the toric case. The investigation of universal Groebner basis, Graver basis and circuits for this ideal revealed that they have the same relationship among them which is true in general for toric ideals. Each linear code can be described as a binomial ideal defined above. Since the reduced Groebner basis for any ideal plays a vital role in describing encoding and decoding processes for the corresponding codes, a natural reduced Groebner basis for this ideal is proposed for any general term order. In fact, if a generator matrix is given for any code, by constructing the corresponding particular binomial ideal, one can immediately describe the reduced Groebner basis. Information positions and parity check positions are then given by standard and non-standard monomials for the ideal. A systematic encoding algorithm for such codes is explained in terms of remainders of the information word computed with respect to the reduced Groebner basis. Furthermore, the binary and ternary Golay codes are studied algebraically in terms of the binomial ideal. Finally, a presentation of the binomial ideal of a linear code in terms of its syzygy modules is provided and the corresponding finite free resolution has been described.

Acknowledgements

My deepest gratitude is to my supervisor Professor Karl-Heinz Zimmermann. His generous advice, inspiring guidence, encouragement and benevolence helped me tremendously through out my work. I am extremely grateful to him for his help and support, without which it would have been impossible for me to complete this thesis. I feel very priviledged indeed to have been one of his students.

My warm thanks are due to my colleague, Dr. Svetlana Torgasin, not only for generously giving her time to help me with latex but also for being there whenever I needed her.

I am gratefull to all my colleagues and staff for their support and providing friendly atmosphere. Special thanks go to Mr. Stefan Just for providing technical help.

Finally, I wish to express my love and gratitude to all my family, in-laws and friends for their encouragement and emotional support. I want to express my deep appreciation and love for my parents for their prayers, unconditional love and endless support in all my pursuits. I must express my gratitude to Saulat, my husband, for his continued support, encouragement and great sense of humor.

The forbearance shown by my children has been my greatest asset in concluding this study. To them, I am eternally grateful.

Contents

Notation

$d(x, y)$	Hamming distance between x and y
d	Minimum distance of a code
s	Syndrome of a received vector
$[n, k, d]$	A linear code with lenght n, dimension k and minimum distance d
$\mathbb{K}$	Field
$\mathbb{K}[x]$	Polynomial ring in n variables over $\mathbb{K}$
$\succ$	Term ordering
$\mathrm{lt}(f)$	Leading term of a polynomial f
$\mathrm{lt}(I)$	Leading ideal of an ideal I
$S(f, g)$	S-polynomial of f and g
G	Groebner basis of an ideal
$\mathcal{V}(I)$	Variety of an ideal
$\sqrt{I}$	Radical of an ideal I

Chapter 1

Introduction

1.1 The Problem

The problem of robust information transmission is one of the problems that is encountered in modern data transmission due to the presence of hostile enviroment during transmission, which thus results into the distorted information. In order to combat this situation error-correcting codes are introduced [42]. A fundamental problem is to send a message across a noisy channel with a maximum possible reliability. Error correcting codes are used to correct messages when they are transmitted through noisy channels(Figure 1.1).

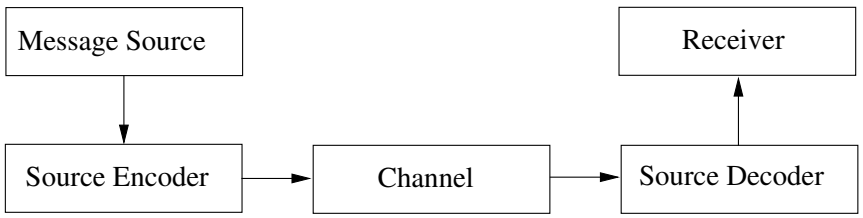

Figure 1.1: A basic communication model

The main features of coding theory are:

- efficient encoding of messages,
- easy transmission of encoded messages,

- fast and reliable decoding of recieved messages,
- transmission of large number of messages per unit of time.

1.2 Previous Work

The last several years have witnessed major theoretical advances in coding theory resulting in a new coding concepts such as algebraic codes, codes on graphs etc. With the publication of C. Shannon's [54] seminal paper the whole new subject of coding theory was inaugurated. Later, R.W. Hamming [30] proposed a first method of encoding data so that errors can not only be detected but can be corrected too. With this coding theory started to develop along two main directions: probabailistic coding theory and algebraic coding theory. The basic idea is to protect a message by adding some redundant information, thus in case even if the message is corrupted, enough redundancy can help in recovering the message completely. The main objects of study in algebraic coding are codes that are linear subspaces of finite-dimensional vector spaces over a finite field. In particular, research was mainly devoted to cyclic codes that form a class of linear codes allowing easier determination. The most important cyclic codes, BCH codes and Reed Solomon codes [8, 45, 32] were discovered between 1958 and 1960. The theory of algebraic codes indicates the fact that by adding more algebraic structure to the system, better descriptions can be obtained. A perfect illustration of this fact is the work of S. D. Berman [5], who discovered that the Reed-Muller codes over $\mathbb{F}_2$ may be described as ideals in group algebra over an elementary abelian 2-group. Later, P. Charpin [13], generalized this over $\mathbb{F}_p$.

In 1965 Buchberger introduced the theory of Greobner bases for polynomial ideals in commutative polynomial rings over fields [9, 10, 11]. Since then a rich stream of papers and many good books have been written on Groebner bases [1, 25, 46]. The "Cooper philosophy" was the first instance of applications to associate Groebner bases with linear codes [17]. Since then Groebner bases are considered as basic tool in understanding and improving linear codes [12, 3]. Following are a few examples [48]:

- Lally (2009) gives a description of quasi-cyclic codes in term of Groebner bases of polynomial modules.

- Borges-Quintana et al. (2009) provide a Groebner basis description for binary linear codes, allowing their decoding and the calculation of their distance.

- Martinez-Moro and Ruano (2009) present a new family of linear codes endowed with a natural Groebner basis description.

1.3 Contribution of the Thesis

The main contributions of this thesis are as follows:

- A reduced Groebner basis for a class of ideals in a commutative polynomial ring is constructed. A subclass of these ideals, when considered in a quotient ring corresponds to generalized Reed Muller codes. Their encoding and decoding procedures are also supplied. Furthermore, while studying primitive Reed Muller codes, another interesting family of codes, superior to primitive Reed Muller codes are discovered with designed Hamming distance [51].

- Recently linear codes have been associated to binomial ideals [48]. A linear code is associated with a binomial ideal which is a sum of a toric and a non-prime ideal. This correpondence allows to understand the in depth structure of the linear code using methods from commutative algebra and algebraic geometry. Graver bases, universal bases and the set of circuits are also considered for this binomial ideal. It turned out that in binary case, all three are equal [49].

- The main contribution of this work is a method by which a Groebner basis (with respect to the lexicographic order requiring that any monomial containing one of the information symbols is larger than any monomial containing only parity check symbols) can be read off directly from the generator matrix of the considered code. This in return provides a very compact encoding procedure [52].

- For better understanding of a linear code the structure of a corresponding binomial ideal is needed to be explored. For this, the syzygy module of this ideal is also studied along with its finite free resolution [50]. The syzygy

module of linear codes could be used to compare linear codes to decide whether they are isomorphic or not.

1.4 Organization

This thesis consists of six chapters; a brief overview of the contents of each chapter is as follows:

- Chapter 2 introduces some of the basic concepts of commutative polynomial algebra. After defining monomials, term orderings and monomial ideals in a commutative polynomial ring, the powerful theory of Groebner bases will be introduced. Definition of toric ideal as a special form of binomial ideal is given as toric ideals play an important role in this work. The chapter ends with a review of Groebner bases for modules.

- Chapter 3 begins with a short review of basic coding theory. Cyclic codes are defined as ideals in a quotient ring. This connection is established by using Groebner basis. Lastly, some well known families of codes are given along with their main features.

- Chapter 4 describes the relationship between coding theory and the Groebner bases theory by relating a linear code with a binomial ideal. Construction of the Groebner basis of that ideal results into better encoding procedure. Universal Groebner bases, Graver bases and the set of circuits are also studied for that ideal and found the situation quite close to that of toric ideal.

- Chapter 5 proposes a systematic method by which the reduced Groebner basis of a binomial ideal corresponding to the code can be constructed directly from its generator matrix. This approach will be applied to Golay codes.

- Chapter 6 presents the binomial ideal in terms of its syzygy module. The corrsponding finite free resolution and associated variety are also discussed.

Chapter 2

Polynomial Algebra

Certain sets of polynomials have special algebraic structure, they may be rings, fields or ideals. Algebraic properties associated to these structures play a very important role in solving computational tasks involving polynomials. In this chapter, we will discuss various aspects of polynomials which will play a fundamental role in our later discussion. We will define ideals over polynomial rings and will give brief summary on Groebner bases for ideals and modules. Most of the material given in this section is taken from [1, 18].

2.1 Monomials

A monomial, in n indeterminates $x_1, \ldots, x_n$, is a product of the form $x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n}$, where the u_i are non-negative integers, and $u = (u_1, \ldots, u_n)$. The total degree of this monomial is the sum $|u| = u_1 + \cdots + u_n$.

2.1.1 Definition [Polynomial] A polynomial f in $x_1, x_2, \ldots, x_n$ with the coefficients in $\mathbb{K}$ (where $\mathbb{K}$ is any field) is a finite linear combination of the monomials, written as

$$f = \sum_u c_u x^u, \quad c_u \in \mathbb{K}, \tag{2.1}$$

c_u is called the coefficient of the monomial $x^u = x_1^{u_1} \cdots x_n^{u_n}$. If $c_u \neq 0$ then we call $c_u x_u$ a term of f. The set of all polynomials in $x_1, x_2, \ldots, x_n$ with coefficients in

$\mathbb{K}$ is denoted by $\mathbb{K}[x] = \mathbb{K}[x_1, \ldots, x_n]$. These polynomials in n variables, over a field $\mathbb{K}$, together with operations of addition and multiplication, satisfy all axioms of ring, and so form commutative polynomial ring.

2.1.2 Example Let $f = 3x^2y + 6xy^3 - 9y^4$ be a polynomial with three terms and maximum degree 4. Here two terms are having the same degree, so in order to arrange the terms of this polynomial we need term ordering. ♦

In the case of one variable we only deal with the degree ordering on the one-variable monomials:

$$... > x^{n+1} > x^n > x^{n-1} ... \tag{2.2}$$

In the multivariate case, there are a lot more options. One basic requirement is that the ordering structure must be consistent with polynomial multiplication. Term orders are of critical importance when dealing with multivariate polynomial rings. Specially, in the case of division algorithm, one needs to distinguish a leading term in any polynomial.

2.1.3 Definition [Term Ordering] In order to arrange the terms of polynomial, one must be able to compare every pair of polynomials. Let M denote the set of all monomials in $\mathbb{K}[x]$. A relation $\succ$ on M is an admissible ordering if for any monomials m_1, m_2 and m_3

- for any pair of monomials m_1,m_2 either $m_1 \succ m_2$ or $m_2 \succ m_1$ or $m_1 = m_2$,
- if $m_1 \succ m_2$ and $m_2 \succ m_3$ then $m_1 \succ m_3$,
- $m_1 \succ 1$ for any monomial $m_1 \neq 1$,
- if $m_1 \succ m_2$ then $mm_1 \succ mm_2$ for any monomial m.

Most commonly used term orderings are the following.

2.1.4 Definition [Lexicographic Order] Let u and v be elements of $\mathbb{N}_0^n$, we say $u \succ_{lex} v$ if in $u - v$ (as integer vector), the left most non-zero entry is positive. We write $x^u \succ_{lex} x^v$ if $u \succ_{lex} v$.

2.1.5 Definition [Graded Lex Order] We say $u \succ_{grlex} v$ if $|u|>|v|$ or $|u| = |v|$ and $u \succ_{lex} v$.

2.1.6 Definition [Graded Reverse Lex Order] We say $u \succ_{grevlex} v$ if either $|u|>|v|$ or $|u| = |v|$ and the right most non-zero entry of $u-v$ (as integer vector) is negative.

Given a term order $\succ$, each non-zero polynomial $f \in \mathbb{K}[x]$ has a unique leading term, denoted by $\mathrm{lt}(f)$, given by the largest involved term with respect to the term order. If $\mathrm{lt}(f) = cx^u$, where $c \in \mathbb{K}$, then c is the leading coefficient of f and x^u is the leading monomial (lm).

2.1.7 Example Let $f = 4xy^2z4z^2 - 5x^3 + 7x^2z^2 \in \mathbb{K}[x, y, z]$.

- With respect to lex order $f = \underline{-5x^3} + 7x^2z^2 + 4xy^2z + 4z^2$,
- with respect to grlex order $f = \underline{7x^2z^2} + 4xy^2z - 5x^3 + 4z^2$,
- with respect to grevlex $f = \underline{4xy^2z} + 7x^2z^2 - 5x^3 + 4z^2$,

where underlined terms are the leading terms with respect to the corresponding term order. ♦

An ideal is a special kind of subset of $\mathbb{K}[x]$ which behaves well with respect to the ring operations.

2.1.8 Definition [Ideal] Specializing the general definition of an ideal to a polynomial ring, we have the following: A subset $I \subseteq \mathbb{K}[x]$ is an ideal (or a polynomial ideal) if it satisfies:

- $0 \in I$.
- If $f, g \in I$, then $f + g \in I$.
- If $f \in I$ and $h \in \mathbb{K}[x]$, then $fh \in I$.

An ideal I coincides with $\mathbb{K}[x]$ if and only if $1 \in I$. The first natural example of an ideal is the ideal generated by a finite number of polynomials.

2.1.9 Definition Let $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x]$. Then the set

$$\langle f_1, \ldots, f_s \rangle = \{h_1 f_1 + \ldots + h_s f_s : h_1, \ldots, h_s \in \mathbb{K}[x]\}$$

is an ideal in $\mathbb{K}[x]$, called ideal generated by $\langle f_1, \ldots, f_s \rangle$. This is the smallest ideal in $\mathbb{K}[x]$ containing $f_1, \ldots, f_s$.

2.1.10 Example Let $\mathbb{K}[x, y] = \mathbb{K}[x_1, \ldots x_n, y_1, \ldots y_m]$ and consider the ideal

$$I = \langle f_1, f_2 \rangle = \langle 1 + x, 1 + y \rangle$$

The following are elements in I:

$$0, x - y, x + xy, x^2y + x^2 - yx - y. \tag{2.3}$$

♦

The radical of an ideal I is defined as a set $\sqrt{I} = \{f \in \mathbb{K}[x] : f^m \in I, \text{for some } m > 0\}$.

An ideal I is a radical ideal if $\sqrt{I} = I$.

2.1.11 Example Let $I = \langle x^2y^3 \rangle \subset \mathbb{K}[x, y]$. Then $\sqrt{I} = \langle xy \rangle$. ♦

Another interesting class of ideals is the class of monomial ideals. Computations with these ideals are much easier when compared to polynomial ideals. Many invariants can be effectively computed for monomial ideals. As a result one can solve several problems by reducing them to monomials.

2.1.12 Definition [Monomial Ideal]

A monomial ideal I in $\mathbb{K}[x_1, x_2, \ldots x_n]$ is a polynomial ideal, generated by monomials.

2.1.13 Example $I = \langle y^3, xy, y^4 \rangle$ is a monomial ideal. ♦

The crucial fact about monomial ideals is that they are finitely generated (Dickson's lemma).

2.2 Groebner Bases

The concept of Groebner bases was introduced by Bruno Buchberger in 1965 in the context of his work on performing algorithmic computations in residue classes of polynomial rings. Buchberger's algorithm for computing Groebner bases is a powerful tool for solving many important problems in polynomial ideal theory. The main idea behind the Groebner bases technique is that if $I = \langle f_1, f_2, \ldots, f_n \rangle$ is an ideal then a Groebner basis algorithm will find the least complex list of polynomials that generates I, but it definitely depends on the choice of term order. Choosing a "wrong" term order will result into a more complex situation. In order to introduce the theory of Groebner bases we need to define the ideal of leading terms in $\mathbb{K}[x]$.

2.2.1 Definition Given a term order $\succ$, each non-zero polynomial $f \in \mathbb{K}[x]$ has a unique leading term, denoted by $\mathrm{lt}(f)$. If I is an ideal in $\mathbb{K}[x]$, then $\mathrm{lt}(I)$ is the monomial ideal generated by the leading terms of its elements,

$$\mathrm{lt}(I) = \langle \mathrm{lt}(f) \mid f \in I \rangle.$$

This is also called an initial ideal. The monomials that do not lie in the ideal $\mathrm{lt}(I)$ are called standard monomials. A finite subset G of I is a Groebner basis for I with respect to $\succ$ if the ideal $\mathrm{lt}(I)$ is generated by the set of leading terms in G,

$$\mathrm{lt}(I) = \langle \mathrm{lt}(g) \mid g \in G \rangle.$$

Informally, a subset $\{g_1, \ldots, g_n\} \subseteq I$ is a Groebner basis of I if and only if the leading term of any element of I is divisible by one of the leading term $\mathrm{lt}(g_i)$ where $1 \leq i \leq n$. Hilbert Basis Theorem implies that every ideal in a polynomial ring is finitely generated. In particular $\mathrm{lt}(I)$ is generated by finitely many terms.

Every ideal $I \subseteq \mathbb{K}[x_1, x_2, \ldots, x_n]$ has a Groebner Basis. We can use Maple and other computer algebra programs [29] to compute a Groebner basis of an ideal. Groebner bases are good generating sets in the sense that they allow us to solve many problems like the solution to systems of equations.

2.2.2 Example Let $I = \langle f_1, f_2 \rangle$ where $f_1 = x^3 - 2xy$ and $f_2 = x^2y - 2y^2 + x$. Then $\{f_1, f_2\}$ is not a Groebner basis for I w.r.t grevlex order since $x^2 \in \mathrm{lt}(I)$ but $x^2 \notin \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2) \rangle$. ♦

2.3 Classification of Groebner bases

There are many systematic ways by which we can determine that whether a basis is a Groebner basis or not. First very important observation about Groebner bases is that if we "divide" any polynomial f in $\mathbb{K}[x]$ by Groebner basis of an ideal I, we always get a unique remainder. This enables us to determine whether a polynomial f lies in I or not. Before we proceed further the concept of division in context of several variables needs to be explained.

2.3.1 The Reduction Process

The division algorithm for polynomials in one variable states that if f and g are polynomials such that $g \neq 0$ then there exist q and r such that $f = q \cdot g + r$ where either $r = 0$ or $\deg(r) < \deg(g)$. In order to generalize this concept of division algorithm to the polynomial ring in $\mathbb{K}[x]$, one needs to use term orderings, which have been defined earlier. To be more precise, let f be a polynomial in $\mathbb{K}[x]$ and let $G = (g_1, g_2 \dots g_n)$ be an ordered sequence of polynomials in several variables. Fix some admissible term ordering. The remainder in this case can recursively be described as follows: If $\mathrm{lt}(g_k)$ divides $\mathrm{lt}(f)$, then define $\mathrm{rem}(f, g_1, \dots, g_n) = \mathrm{rem}(f - l \cdot g_k, (g_1, g_2, \dots, g_n))$, where k is the smallest index such that $\mathrm{lt}(g_k)$ divides $\mathrm{lt}(f)$ and l is the term chosen so that $\mathrm{lt}(f) = \mathrm{lt}(l \cdot g_k)$. If no $\mathrm{lt}(g_i)$ divides $\mathrm{lt}(f)$, then define $\mathrm{rem}(f, (g_1, g_2, \dots, g_n) = \mathrm{lt}(f) + \mathrm{rem}(f - \mathrm{lt}(f), (g_1, g_2, \dots, g_n))$. The process is finite since in both cases the leading monomial drops. The following proposition gives a criterion to decide whether a polynomial $f \in \mathbb{K}[x]$ belongs to an ideal $I \subseteq \mathbb{K}[x]$ or not.

2.3.1 Proposition *Let $G = \{g_1, g_2, \dots g_n\}$ be a Groebner basis for an ideal $I \subseteq \mathbb{K}[x_1, x_2, \dots x_n]$ and let $f \in \mathbb{K}[x_1, x_2, \dots x_n]$. Then $f \in I$ if and only if the remainder on division of f by G is zero.*

2.4 Computing Groebner Bases

Once the concept of division is clear in the case of several variables, one can now compute Groebner bases of an ideal from its generating set, which crucially depends on the term ordering, different term orders may result into different Groeb-

ner bases. The Groebner basis from any set of generators of an ideal can be constructed by computing S-polynomial defined below.

2.4.1 Definition Let f and g be non-zero polynomials in $\mathbb{K}[x]$. Define the S-polynomial of f and g w.r.t some fixed term ordering, as

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

where lcm denotes the least common multiple.

The S-polynomial cancels the leading terms of f and g according to the term ordering.

2.4.2 Example If $(f,g) = (x^2, xy - y^2)$ and the ordering is lex then

$$S(f,g) = \frac{x^2y}{x^2}x^2 - \frac{x^2y}{xy}.(xy - y^2) = xy^2 \tag{2.4}$$

♦

The following criterion determines that whether a set is a Groebner basis for an ideal or not.

2.4.3 Theorem *Let $\{g_1, g_2, \ldots, g_n\}$ be a set of monic polynomials in $\mathbb{K}[x]$. Then $\{g_1, g_2, \ldots, g_n\}$ is a Groebner basis of the ideal it generates if and only if*

$$rem(S(g_i, g_j)) = 0 \text{ for all } i \neq j.$$

Groebner bases are not unique. However a reduced Groebner basis is always unique.

2.4.4 Definition A Groebner basis $G = \{g_1, g_2, \ldots, g_n\}$ for the ideal I in $\mathbb{K}[x]$ is said to be minimal if each g_i, $1 \leq i \leq n$, is monic and the leading term of the generator g_i is not divisible by the leading term of another generator g_j where $i \neq j$. A Groebner basis G is called reduced basis if it is minimal and no term in g_i is divisible by $\text{lt}(g_j)$ for any $i \neq j$.

There are many features which comtribute to the theory of Groebner basis such as Groebner basis can be constructed w.r.t arbitrary admissible orderings and lexical orderings having the elimination properties [57] or can be designed for desired orderings [15]. For extensive study of Groebner bases reader is referred to [1, 25, 4, 35].

2.5 Binomial Ideal

The following ideals are of great importance in this work. A binomial in a polynomial ring is a polynomial with two terms, say $ax^u + bx^v$.

2.5.1 Definition [Binomial Ideal]

A binomial ideal is an ideal of $\mathbb{K}[x]$ generated by binomials.

If I is a binomial ideal then the radical, associated primes, and isolated primary components of I are again binomial, and I admits primary decompositions in terms of binomial primary ideals [23]. Moreover these ideals have a finite number of binomials generators in a polynomial ring. Next we describe the notion of toric ideal which is a special type of binomial ideal. Let $y_1, \cdots, y_d$ and $x_1, \cdots, x_n$ be indeterminates over a field $\mathbb{K}$. Let $A = (a_{i,j})$ be a $d \times n$ matrix with nonnegative integer entries. The columns of A give rise to a collection of monomials in $\mathbb{K}[y_1, \ldots, y_d]$ given by

$$m_j = y_1^{a_{1,j}} \cdots y_d^{a_{d,j}}, \quad 1 \leq j \leq n.$$

The ideal associated to the matrix A is the kernel of the $\mathbb{K}$-algebra homomorphism

$$\phi : \mathbb{K}[x_1, \ldots, x_n] \to \mathbb{K}[y_1, \ldots, y_d] : x_j \mapsto m_j, \quad 1 \leq j \leq n. \tag{2.5}$$

This is a toric ideal and is denoted by I_A. A toric ideal is prime since it is the kernel ($\ker \phi$) of a homomorphism into an integral domain [21, 33, 56].

2.5.2 Proposition *The toric ideal I_A is generated by*

$$I_A = \langle x^u - x^v : Au = Av, u, v \in \mathbb{N}_0^n \rangle. \tag{2.6}$$

Proof: Choose $f \in I_A$ a polynomial, which cannot be written as a linear combination of the binomials given in the generating set. Let $\mathrm{lt}(f) = x^u$ be minimal w.r.t $\succ$. Now $f \in \ker \phi$, hence x^u gets cancelled with some x^v after applying ϕ. Also x^v is less than x^u since it is not the leading term. Let $g = x^u - x^v, \phi(g) = 0$ and so $\phi(f - g) = 0, f \neq g$. Moreover $\mathrm{lt}(f) \succ \mathrm{lt}(f - g)$, hence by assumption $f - g$ can be written as a linear combinition of binomials, which is a contradiction. ■

Hilbert Basis Theorem tells us that I_A is generated by finitely many binomials from the above set. A Groebner basis for the ideal $I = I_A$ can be computed from the ideal [6, 56]

$$J = \langle x_j - m_j : 1 \leq j \leq n \rangle. \tag{2.7}$$

For this, observe that $I = J \cap \mathbb{K}[x_1, \ldots x_n]$. Moreover, since J is generated by binomials, Groebner bases theory implies that all the elements in any reduced Groebner basis for J are binomials, too. Suppose G is a Groebner basis for J with respect to an elimination term order in which any monomial containing one of the y_i is greater than any monomial containing only the x_j. Then I has the Groebner basis $G \cap \mathbb{K}[x_1, \ldots x_n]$ and so is also generated by binomials. Another description of computation of Groebner basis for toric ideals is given in [44].

2.5.3 Example Consider the matrix $A = \begin{pmatrix} 3 & 2 & 1 & 0 \\ 0 & 1 & 2 & 3 \end{pmatrix}$. The toric ideal associated to this matrix has the following Groebner basis:

$$I_A = \langle x_1 x_3 - x_2^2, x_1 x_4 - x_2 x_3, x_2 x_4 - x_3^2 \rangle$$

♦

It is worth noticing here that not all binomial ideals are toric ideals, i.e the ideal $I = \langle x^2 - y^2 \rangle$ is a binomial ideal but not prime since $(x - y)(x + y) \in I$ but $(x - y), (x + y) \notin I$.

2.6 Groebner Bases for Modules

Modules are to rings what vector spaces are to fields [1, 38]. Let $\mathbb{K}$ be a field and $R = \mathbb{K}[x_1, \ldots, x_n]$ be a commutative ring with identity, a set M is called an

R-module provided that M is an abelian group under addition and multiplication by elements of R satisfying the following axioms:

- for every $r \in R$ and $m \in M$, $rm \in M$,
- for every $r \in R$ and $m, m \in M$, $r(m + m') = rm + rm'$,
- for every $r, r' \in R$ and $m \in M$, $(r + r')m = rm + r'm$,
- for every $r, r' \in R$ and $m \in M$, $r(r'm) = rr'm$,
- for every $m \in M$, $1m = m$.

The simplest example of modules are those which consist of all $m \times 1$ columns of R:

$$R^m = \left\{ \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} : r_i \in R, \text{for all } 1 \leq i \leq m \right\} \tag{2.8}$$

where addition and scalar multiplication are defined component-wise,

$$\begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} + \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} = \begin{pmatrix} r_1 + r_1 \\ \vdots \\ r_m + r_m \end{pmatrix} \tag{2.9}$$

and

$$r \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} = \begin{pmatrix} rr_1 \\ \vdots \\ rr_m \end{pmatrix} \tag{2.10}$$

A module satisfies almost the same axioms as a vector space, with elements taken from a ring rather than a field. Unlike vector spaces modules need not have a linearly independent generating set but if a module has one, then that is called a free module. For example the R-module R^m is a free module. A submodule of an R-module M is a subset of M, which itself is an R-module. Next, the generalisation of the theory of Groebner bases to submodules of R^m is described. Construction of these bases goes parallel to what we have for ideals in polynomial rings. Consider the standard basis of R^m,

$$\boldsymbol{e}_1 = (1, \ldots, 0)^T, \boldsymbol{e}_2 = (0, 1, \ldots, 0)^T, \cdots, \boldsymbol{e}_n = (0, \ldots, 1)^T.$$

Recall that a monomial in R is an element of the form $x^u = x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n}$, where $u = (u_1, \ldots, u_n) \in \mathbb{N}_0^n$ is a lattice point. More generally, a monomial $\boldsymbol{m}$ in R^m is an element of the form $x^u \boldsymbol{e}_i$ for some i. The product $c \cdot \boldsymbol{m}$ of a monomial $\boldsymbol{m} \in R^m$ with an element $c \in R$ is called a term and c is called its coefficient. Each element $\boldsymbol{f} \in R^m$ can be uniquely written as an R-linear combination of monomials $\boldsymbol{m}_i \in R^m$,

$$\boldsymbol{f} = \sum_i c_i \boldsymbol{m}_i, \quad 0 \neq c_i \in R. \tag{2.11}$$

If $\boldsymbol{m}$ and $\boldsymbol{n}$ are monomials in R^m, $\boldsymbol{m} = x^u \boldsymbol{e}_i$ and $\boldsymbol{n} = x^v \boldsymbol{e}_j$, then $\boldsymbol{m}$ is divisible by $\boldsymbol{n}$ if $i = j$ and x^u is divisible by x^v. If $\boldsymbol{m}$ is divisible by $\boldsymbol{n}$, then the quotient $\boldsymbol{m}/\boldsymbol{n}$ is defined to be $x^u/x^v = x^{u-v} \in R$. Thus if $\boldsymbol{n}$ divides $\boldsymbol{m}$, then $\boldsymbol{m} = (\boldsymbol{m}/\boldsymbol{n}) \cdot \boldsymbol{n}$. Moreover, if $i = j$ then the least common multiple of $\boldsymbol{m}$ and $\boldsymbol{n}$ is given as the least common multiple of x^u and x^v times $\boldsymbol{e}_i$; otherwise, the least common multiple is defined to be $\boldsymbol{0}$. In order to construct Groebner basis for R^m, we need to define the the concept of division in modules which depends heavily on term order [1, 18]. By a term order on monomials of R^m, we mean a total order, $\succ$, on these monomials satisfying the following conditions:

- $\boldsymbol{X} \succ Z\boldsymbol{Y}$, for every monomial $\boldsymbol{X}$ of R^m and monomial $Z \neq 1$ of R;
- if $\boldsymbol{X} \succ \boldsymbol{Y}$, then $Z\boldsymbol{X} \succ Z\boldsymbol{Y}$ for all monomials $\boldsymbol{X}, \boldsymbol{Y} \in R^m$ and every monomial $Z \in R$

For any term order $\succ$ on R, two term orders on R^m can be defined naturally :

- (the TOP extension of $\succ$) $x^u \boldsymbol{e}_i \succ_{TOP} x^v \boldsymbol{e}_j$ if and only if $x^u \succ x^v$, or if $x^u = x^v$ and $i < j$
- (the POT extension of $\succ$) i.e., $x^u \boldsymbol{e}_i \succ_{POT} x^v \boldsymbol{e}_j$ if and only if $i < j$, or if $i = j$ and $x^u \succ x^v$ [1, 18].

Given a term order $\succ$ on R^m, each non-zero element $\boldsymbol{f} \in R$ has a unique leading monomial, denoted by $\mathrm{lt}(\boldsymbol{f})$, which is given by the largest involved monomial with respect to the term order.

Once a term ordering on R^m is fixed, the division algorithm in R can be easily extended to the R-module R^m. The basic idea behind the division algorithm is the same as for polynomials, i.e to divide the polynomial of a module by an ordered sequence of elements of a module until the division process can not be done anymore. For this, let f be an element in R^m which is to be divided by an ordered sequence $\mathcal{G} = (g_1, \ldots, g_s)$ of elements in R^m. The key operation is the reduction of a partial dividend p ($p = f$ to start) by an g_k (k is assumed to be minimal) such that $\mathrm{lt}(g_k)$ divides $\mathrm{lt}(p)$. If $\mathrm{lt}(p) = t \cdot \mathrm{lt}(g_k)$ for some term $t \in R$, then p is replaced by $p - t \cdot g_k$. This reduction step can be stated by the recursion

$$\mathrm{rem}(p, (g_1, \ldots, g_s)) = \mathrm{rem}(p - t \cdot g_k, (g_1, \ldots, g_s)). \tag{2.12}$$

If at some point, no reduction is possible then $\mathrm{lt}(p)$ is not divisible by any of the $\mathrm{lt}(g_i)$. In this case, the leading term of p is subtracted and placed in the remainder. This step is given by the recursion

$$\mathrm{rem}(p, (g_1, \ldots, g_s)) = \mathrm{lt}(p) + \mathrm{rem}(p - \mathrm{lt}(p), (g_1, \ldots, g_s)). \tag{2.13}$$

The reduction stops when p is reduced to $\mathbf{0}$; it always terminates since in both cases the leading term of p drops.

Let M be a submodule of R^m and let $\succ$ be a term order on R^m. We denote by $\mathrm{lt}(M)$ the (monomial) submodule generated by the leading terms of all $f \in M$ with respect to $\succ$.

A finite subset $\mathcal{G} = \{g_1, \ldots, g_s\}$ of M is called a Groebner basis for M with respect to $\succ$ if the submodule of leading terms equals the submodule of leading terms generated by the elements of $\mathcal{G}$, i.e.,

$$\mathrm{lt}(M) = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle. \tag{2.14}$$

If $\mathcal{G}$ is a Groebner basis for M, then $f \in R^m$ lies in M if and only if the remainder on division by $\mathcal{G}$ is $\mathbf{0}$. The computation of Groebner bases depends on a generalization of Buchberger's S-criterion. For this, let f and g be elements of R^m. Define the S-vector of f and g as

$$S(f, g) = \frac{m}{\mathrm{lt}(f)} f - \frac{m}{\mathrm{lt}(g)} g, \tag{2.15}$$

where m is the least common multiple of the leading monomials of f and g. Thus the S-vector $S(f, g)$ cancels the initial terms of f and g according to the term

ordering. Buchberger's S-criterion says that a set $\mathcal{G} = \{g_1, \ldots, g_s\}$ in R^m is a Groebner basis for the module it generates if and only if the remainder on division by $\mathcal{G}$ of $S(g_i, g_j)$ is $\mathbf{0}$ for all i, j.

A reduced Groebner basis for a submodule M of R^m and a term order $\succ$ can be calculated by Buchberger's algorithm that starts with any set of generators for M. In the most rudimentary form, the algorithm appends in each step the remainders of the S-vectors between each pair of generators to the generating set until these remainders are all $\mathbf{0}$.

2.7 Syzygies and Finite Free Resolution

The existence of a Groebner basis for each submodule of R^m also shows that each submodule of R^m is finitely generated. However, submodules of R^m eventually have no bases (in the sense of linear algebra). Thus to handle computations in a module requires not only a generating set, but also the set of all relations satisfied by the generators. More specifically, let $F = (f_1, \ldots, f_t)$ be an ordered t-tuple of elements in R^m. A relation on F is an R-linear combination of the f_i which is equal to $\mathbf{0}$,

$$h_1 f_1 + \ldots + h_t f_t = \mathbf{0}. \tag{2.16}$$

We think of a relation on F as an element $\boldsymbol{h} = (h_1, \ldots, h_t)^T$ of R^t. Such relations are called syzygies. The set of all relations on F forms an R-submodule of R^t, called the (first) syzygy module of $(f_1, \ldots, f_t)$ and denoted by $\mathrm{Syz}(f_1, \ldots, f_t)$ [1, 18].

In particular, suppose that $\mathcal{G} = \{g_1, \ldots, g_t\}$ is a Groebner basis for a submodule M of R^m. Consider the corresponding S-vector

$$S(g_i, g_j) = \frac{\boldsymbol{m}_{ij}}{\mathrm{lt}(g_i)} g_i - \frac{\boldsymbol{m}_{ij}}{\mathrm{lt}(g_j)} g_j, \quad 1 \le i, j \le t, \tag{2.17}$$

where $\boldsymbol{m}_{ij}$ is the least common multiple of the leading monomials of g_i and g_j. Since $\mathcal{G}$ is a Groebner basis, by Buchberger's S-criterion, the remainder of $S(g_i, g_j)$ upon division by $\mathcal{G}$ is $\mathbf{0}$, and the division algorithm gives an expression

$$S(g_i, g_j) = \sum_{k=1}^{t} h_{ijk} g_k, \tag{2.18}$$

where $h_{ijk} \in R$ and $\mathrm{lt}(h_{ijk}\boldsymbol{g}_k) \succ \mathrm{lt}(S(\boldsymbol{g}_i, \boldsymbol{g}_j))$ for all i, j, and k. Let $\boldsymbol{h}_{ij} \in R^t$ denote the column vector

$$\boldsymbol{h}_{ij} = h_{ij1}\boldsymbol{e}_1 + \ldots + h_{ijt}\boldsymbol{e}_t \in R^t. \tag{2.19}$$

For each pair (i, j), $1 \leq i, j \leq t$, such that $\boldsymbol{m}_{ij} \neq \boldsymbol{0}$, define

$$\boldsymbol{s}_{ij} = \boldsymbol{h}_{ij} - \frac{\boldsymbol{m}_{ij}}{\mathrm{lt}(\boldsymbol{g}_i)}\boldsymbol{e}_i + \frac{\boldsymbol{m}_{ij}}{\mathrm{lt}(\boldsymbol{g}_j)}\boldsymbol{e}_j = \begin{pmatrix} h_{ij1} \\ \vdots \\ h_{iji} - a_i \\ \vdots \\ h_{ijj} + a_j \\ \vdots \\ h_{ijt} \end{pmatrix} \in R^t, \tag{2.20}$$

where $a_i = \boldsymbol{m}_{ij}/\ \mathrm{lt}(\boldsymbol{g}_i)$ and $a_j = \boldsymbol{m}_{ij}/\ \mathrm{lt}(\boldsymbol{g}_j)$. Otherwise, put $\boldsymbol{s}_{ij} = \boldsymbol{0}$. Note that $S(\boldsymbol{g}_i, \boldsymbol{g}_j)$ and $S(\boldsymbol{g}_j, \boldsymbol{g}_i)$ only differ by the sign and so it suffices to consider the $\boldsymbol{s}_{ij}$ only for $i < j$.

By Schreyer's theorem [1, 18, 53], the set $\{\boldsymbol{s}_{ij} \mid 1 \leq i, j \leq t\}$ forms a Groebner basis for the syzygy module $M = \mathrm{Syz}(\boldsymbol{g}_1, \ldots, \boldsymbol{g}_t)$ with respect to the term order $\succ$ on R^t defined as follows:

$$x^u\boldsymbol{e}_i \succ x^v\boldsymbol{e}_j \text{ if } \mathrm{lt}(x^u\boldsymbol{g}_i) \succ \mathrm{lt}(x^v\boldsymbol{g}_j), \text{ or if } \mathrm{lt}(x^u\boldsymbol{g}_i) = \mathrm{lt}(x^v\boldsymbol{g}_j) \text{ and } i < j.$$

2.7.1 Example Let $R = \mathbb{Q}[x, y, z, w]$ and $I = \langle x^2 - yw, xy - wz, y^2 - xz\rangle$. The reduced Groebner basis of I with respect to degrevlex order is $\{g_1, g_2, g_3\}$ where $g_1 = x^2 - wy, g_2 = xy - wz, g_3 = y^2 - xz$, with $x > y > z > w$. Also $\mathrm{lt}(g_1) = x^2, \mathrm{lt}(g_2) = xy, \mathrm{lt}(g_3) = y^2$. Least common multiples are

$m_{11} = x^2y, m_{12} = x^2y^2, m_{13} = xy^2$.

Now $S(g_1, g_2) = -wg_3$ so $s_{12} = (-y, x, -w)^T$. Similarly $s_{13} = (-y^2 + xz, 0, x^2 - yw)^T$ and $s_{23} = (z, -y, x)^T$. Hence $\mathrm{Syz}(g_1, g_2, g_3) = \langle(-y, x, -w)^T, (-y^2+xz, 0, x^2-yw)^T, (z, -y, x)^T\rangle$. Since $s_{13} = ys_{12} + xs_{23}$, we are left with only two generators: $\mathrm{Syz}(g_1, g_2, g_3) = \langle(-y, x, -w)^T, (z, -y, x)^T\rangle$. ♦

Let M be a submodule of R^m with generating set $F = \{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_t\}$. The generators give rise to a surjective homomorphism $\phi_0 : R^t \to M$ sending $(h_1, \ldots, h_t)^T \in R^t$

to $\sum_i h_i \boldsymbol{f}_i \in M$. It follows that the syzygies on $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_t$ form the kernel of ϕ_0. Choosing a set of generators $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_s$ for the syzygy module $\mathrm{Syz}(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_t)$ corresponds to choosing a homomorphism ϕ_1 of R^s onto the kernel of ϕ_0, which amounts to the fact that $\mathrm{im}\,(\phi_1) = \ker(\phi_0)$. Equivalently, the sequence

$$R^s \to R^t \to M \to 0$$

is exact at R^t. Moreover, in order to understand the syzygy module $\mathrm{Syz}(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_t)$, we not only need its generators $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_s$, but also the set of relations on these generators, the so-called second syzygies, and so on. The connection between a module M and its syzygies can be summarized in an exact sequence of the form

$$\cdots \to F_2 \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0 \xrightarrow{\phi_0} M \to 0, \tag{2.21}$$

where all modules F_i are free R-modules. Such a sequence is called a free resolution of M. If there is an index ℓ such that $F_\ell \neq 0$ and $F_{\ell+1} = F_{\ell+2} = \ldots = 0$, then the resolution is said to be finite of length ℓ. The famous Hilbert Syzygy Theorem says that each finitely generated R-module has a finite free resolution whose length is not exceeding the number of variables.

Chapter 3

Algebraic Coding Theory

Communicating accurate information is extremely important and arises in a variety of situations. In 1948 C.E. Shannon gave a formal description of a communication system and introduced a theory about coding. Later R.W. Hamming in 1950 showed how to construct and decode algebraic codes. This incorporation of algebraic structure to codes enabled researchers to provide better codes and to introduce more efficient decoding algorithms. In this chapter first some definitions and some known results regarding coding theory are presented. In the second section the notion of algebraic codes will be introduced. The last section is related to the introduction of one of the oldest codes namely Reed Muller codes. Most of the material in this chapter is taken from [47, 40].

3.1 Basic Coding Theory

The main aim of coding theory is the transmission of messages over noisy channels and develop techniques to recover the original message which may be distorted due to the noise present. All information is sent as a sequence of 'words' or blocks of zeros and ones. Each block is then translated into a longer block called a 'coded-word'. This encoding is formulated so that any two codewords look very different. Formally:

3.1.1 Definition [Word] Let $F = \{a_1, \ldots, a_q\}$ be a set of size q, which we refer to as a code alphabet and whose elements are called code symbols. A q-ary word of length n over F is a sequence $x = x_1 x_2 \ldots x_n$ with each $x_i \in F$ for all i. Equivalently, x may also be regarded as the vector $(x_1, \ldots, x_n)$.

3.1.2 Remark In practice, and specially in this work, the code alphabet is often taken to be a finite field $\mathbb{F}_q$ of order q. The following is the set of all words of lenght n with entries in $\mathbb{F}_q$:

$$\mathbb{F}_q^n = \{(x_1, \ldots, x_n) : x_i \in \mathbb{F}_q\} \tag{3.1}$$

No errors can generally be detected or corrected if all elements of F^n are used as messages. The obvious idea is to only use a subset. A code C of length n is a non-empty subset of a set F^n. Its elements are called codewords. If $|F| = q$, we say that C is a q-ary code. When $q = 2$, we say that C is a binary code. In order to measure how much the codewords in a code differ from one another we need the following definition.

3.1.3 Definition [Hamming Distance] Let x, y be the words of length n over F. The Hamming distance $d(x, y)$ is the number of coordinates where x and y differ,

$$d(x, y) = |\{i : 1 \leq i \leq n, x_i \neq y_i\}|. \tag{3.2}$$

The Hamming distance can be thought of as the number of positions required to change a codeword x into another codeword y.

The Hamming weight of the vector x is the number of non-zero coordinates and it is denoted by $\mathrm{wt}(x)$. The set of words of length n over F, equipped with Hamming distance d, is a metric space. An important invariant of a code C is the minimum distance among the codewords.

3.1.4 Definition [Minimum Distance] The minimum distance $d = d(C)$ of a code C is the minimum Hammming distance between two distinct codewords in C, i.e.,

$$d = \min\{d(x, y) : x, y \in C, x \neq y\} \tag{3.3}$$

whereas minimum weight is

$$wt_C = \min\{wt(x) : x \in C, x \neq 0\}. \tag{3.4}$$

3.1.5 Example The binary repetition code of length 5 has minimum distance 5 since the two codewords differ in all five positions. ♦

The notion of minimum distance enables us to measure the error detection and correction capabilities of the code. The following result explains that fact.

3.1.6 Theorem *A code C can detect up to t errors if its minimum distance is* $t+1$ *or greater and can correct up to t errors if its minimum distance is* $2t+1$ *or greater.*

We will describe the error correcting capabilities of codes through the geometric point of view. Given $x \in F^n$, we will denote $B_r(x)$, the closed ball of radius r centered at x:

$$B_r(x) = \{y \in F^n : d(y,x) \leq r\}.$$

From above we know that if $d(C) \geq 2t+1$ then for $x, y \in C, x \neq y, B_t(x) \cap B_t(y) = \emptyset$. For if $z \in B_t(x) \cap B_t(y)$, then $0 \neq d(x,y) \leq d(x,z) + d(z,y) \leq 2t < d(C)$. So, geometrically, t-spheres centered at distinct codewords do not overlap. This means that if t or fewer errors have occured during the transmission, they can be corrected by the nearest neighbour decoding, i.e., any codewords lying in any sphere will be decoded as its center.

For $x = (x_1, \cdots, x_n), y = (y_1, \cdots, y_n) \in F^n$ the scalar product between x and y is $x \cdot y = x_1y_1 + \cdots + x_ny_n$. If $x \cdot y = 0$ then x and y are called orthogonal. Let C be a code we define the orthogonal code of C, as the set of vectors which are orthogonal to all codewords of C:

$$C^{\perp} = \{x \in F^n : x \cdot c = 0 \text{ for every } c \in C\}$$

If $C \subseteq C^{\perp}$ then C is called a self orthogonal code and if $C = C^{\perp}$ then C is called a self dual code.

3.1.7 Definition A code C over F is said to be an $[n, M, d]$ code if

- $d = d(C)$ is the minimum distance of C,
- $|C| = M$ is the number of codewords in C, and

- each codeword has length n.

A "good $[n, M, d]$ code" is one which has minimum n, for the purpose of speedy transmission, maximum M, so that large number of messages can be encoded and maximum d, in order to detect and correct as many errors as possible. As a mathematical optimization problem, M needs to be maximized with the condition that $[n, M, d]$ code exists. The following definition gives some bounds on codes. If C is t error correcting, spheres around each codeword are disjoint, we begin by counting the words in a sphere. Let $F = \mathbb{F}_q$ and let $y \in B_r(x)$, where $r \leq n$ and $x \in \mathbb{F}_q^n$. Clearly, $d(x, y) = i$ means that y differs from x in exactly i positions. These i positions can be chosen in $\binom{n}{i}$ ways. For each position we can choose any symbol other than the symbol appearing in x in that position, it gives us $q - 1$ choices, for i symbols there will be $(q-1)^i$ choices. By varying i and adding the resulting numbers, we get all words in a sphere. Hence, the total number of words in all spheres is:

$$M \cdot \left(\binom{n}{0} + (q-1)\binom{n}{1} + \ldots + (q-1)^t \binom{n}{t} \right) \tag{3.5}$$

which cannot be larger than q^n. The following is known as sphere packing bound (or Hamming bound):

$$M \leq \left(\frac{q^n}{\binom{n}{0} + (q-1)\binom{n}{1} + \ldots + (q-1)\binom{n}{t}} \right). \tag{3.6}$$

Codes which satisfy this condition are called perfect codes. For example, there is a perfect code $[7, 16, 3]$ code, known as Hamming code.

3.2 Finite Fields

For deeper analysis and construction of linear codes, the alphabet is endowed with some meaningful structure, that is usually of a finite field [39, 47]. Finite fields play a major role in coding theory. A field is a set $\mathbb{F}$ together with two operations namely, $+$, called addition and $\cdot$, called multiplication. The set $\mathbb{F}$ is an abelian group under addition with additive identity called *zero*, denoted as 0, the set of all non-zero elements is also an abelian group under multiplication with multiplicative identity 1; and multiplication distributes over addition. The field $\mathbb{F}$ is finite if it has finite number of elements, the number of elements in $\mathbb{F}$ is

called the order of $\mathbb{F}$. In general a field with p elements is denoted by $\mathbb{F}_p$. Most commonly used finite fields are the fields of integers modulo p, when p is prime. Let F be a field, the characteristic of F is the least positive interger r such that $r \cdot 1 = 1 + 1 + ... + 1$ is 0, where 1 is the multiplicative identity of F. If no such r exists then the characteristic is defined as 0. The set of p distinct elements of $\mathbb{F}_p$ is isomorphic to the field $\mathbb{F}_p$ of integers modulo p. Following are a few basic results on finite fields: Let $\mathbb{F}_q$ be a finite field with q elements. Then:

- If $\mathbb{F}$ is a finite field then $\mathbb{F}$ has prime characteristic.
- If characteristic of $\mathbb{F}$ is p then $\mathbb{F}$ has p^m elements for some positive integer m.
- $\mathbb{F}_q$ is a vector space over $\mathbb{F}_p$ of dimension m, where $q = p^m$.
- $\mathbb{F}_q$ is unique up to isomorphism.

Familiar examples of fields are the fields of real numbers and complex numbers. Both of these fields contain infinitely many elements. The smallest field of order two consists of two elements i.e. $\{0, 1\}$, multiplication is "same" as for real numbers while addition is mod 2. If $\mathbb{F}_q$ is a field of order q, then the set $\mathbb{F}_q^n$ is an n-dimensional vector space with addition of vectors and multiplication of vectors by a scalar from $\mathbb{F}_q$:

$$(x_1, \ldots, x_n)^T + (y_1, \ldots, y_n)^T = (x_1 + y_1, \ldots, x_n + y_n)^T$$
$$\alpha(x_1, \ldots, x_n)^T = (\alpha x_1, \ldots, \alpha x_n)^T, \alpha \in \mathbb{F}_q.$$

There are several ways by which one can represent the elements of finite fields. Here they are described via factor rings $\mathbb{F}_q[x]/\langle g \rangle$, where g is an irreducible polynomial of degree n in $\mathbb{F}_q[x]$. It is well known that the elements of a quotient ring are in one to one correspondence with the possible remainders on division by g. Hence the elements of the field $\mathbb{F}_q$ may be represented by the cosets modulo $\langle g \rangle$ of the polynomials of degree $n - 1$ or less:

$$a_0 + a_1(x).... + a_{n-1}x^{n-1}, a_i \in \mathbb{F}_q.$$

3.3 Linear Codes

So far only the basic definitions are provided. In order to make implementation of codes easier, concept from algebra are introduced, and with this coding theory becomes more elegent. One of the great advantages of using a field as a code alphabet is that one can perform vector space operations on the codewords. Since we have assumed $\mathbb{F}_q$ to be a field so $\mathbb{F}_q^n$ is an n-dimensional vector space over $\mathbb{F}_q$ as described earlier.

3.3.1 Definition [Linear Code] A linear code C of length n is a linear subspace of the vector space $\mathbb{F}_q^n$ where $\mathbb{F}_q$ is the finite field with q elements.

As explained earlier that the minimum weight of a code is the smallest non-zero weight of any code. Since C is a linear code, $C + c = C$ for all $c \in C$, hence minimum weight and distance coincide. So here we observe the first advantage of a linear code, that is instead of comparing all the codewords for minimum distance, we just calculate the minimum weight. Since, C is a subspace of $\mathbb{F}_q^n$, we can choose a basis for this subspace. Suppose a set of k-words of length n is a basis of C, i.e., $C = \langle c_1, \ldots, c_k \rangle$, then C has q^k codewords. We can arrange these vectors as rows of $k \times n$-matrix G, known as its generator matrix.

$$\begin{pmatrix} c_{11} & \ldots & c_{kl} \\ \vdots & \ldots & \vdots \\ c_{k1} & \ldots & c_{kn} \end{pmatrix} \tag{3.7}$$

By using this matrix, we can encode any message, i.e., if $x \in \mathbb{F}_q^k$ is a message of length k then it may be encoded as the codeword xG. The encoding procedure is particularly simple when the generator matrix is in the standard form: $G = (I_k, A)$ where I_k is the identity matrix of size k. In this case the original message x is regained from xG by deleting the last $n - k$ terms. These last terms are called parity check digits. If a code C has generator matrix G in the standard form then the corresponding parity check matrix is $H = (-A^t, I_{n-k})$. Note the $GH^t = 0$ which implies that c is a codeword if and only if $cH^t = 0$.

3.3.2 Remark A linear code C with length n, dimension k and minimum distance d is called an $[n, k, d]$ code over $\mathbb{F}_q$. Since there are q^k distinct codewords, hence an $[n, k, d]$ code can be referred as $[n, q^k, d]$ code.

3.3.3 Example The matrix $G = (I_4, A)$ where

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

is a generater matrix for an $[7, 4, 3]$ code known as binary Hamming code. The codewords generated by the rows of G are:

0000000	1111111	1000011
0111100	0100101	1011010
0010110	1101001	1101001
1110000	0011001	1100110
0101010	1010101	1001100
0110011	0001111	

♦

So far we have explained a method for efficient generation of linear codes using generator matrix. Codewords are obtained simply by multiplying a message with a generator matrix. When it comes to recovering the original message, which has been transmitted over a noisy channel, the main objective is to make the best possible guess regarding the originally transmitted codeword on the basis of the received word. One obvious decoding algorithm is to examine all codewords unless one is found with a minimum distance d or less from the received word. This strategy is known as nearest neighbour decoding. But this is possible for codes with a small number of codewords. In order to counter this problem a more efficient decoding method known as syndrome decoding is introduced. This method is based on the standard array which is a table in which the elements of $\mathbb{F}_q^n$ are arranged into cosets of C.

3.4 Syndrome Decoding

Assume that $c \in C$ is transmitted and $y = c + e$ is received. If $C = \{c_1, \ldots c_k\}$ is a code with dimension k, the set E of possible error patterns is [36]:

$$E = \{y - c_1, \ldots y - c_k\} = \{y - c : c \in C\} = y - C. \tag{3.8}$$

Given a received vector y there is a one to one correspondence between the possible error patterns and the codewords. When C is a linear code, then

$$E = y - C = y + C = \{y + c : c \in C\} \tag{3.9}$$

thus the set of all possible error patterns corresponding to the recieved word y is precisely $y + C$, known as the coset of C. Formally, let C be an $[n, k, d]$ code over $\mathbb{F}_q$. For any $x \in \mathbb{F}_q^n$, the set

$$x + C = \{x + c : c \in C\}$$

is called a coset of C. Since C is a linear space, the distinct cosets partition $\mathbb{F}_q^n$ into q^{n-k} sets of size q^k. Thus, in order to decode, we must examine the coset corresponding to the recieved vector, to find the appropriate error pattern.

3.4.1 Definition Let H be a parity check matrix for C. The syndrome s associated with the received word y is $s = yH^T$. Observe that

$$s = yH^T = (c + e)H^T = cH^t + eH^T = eH^T. \tag{3.10}$$

the sydrome depends only on error pattern e and not on the transmitted codeword. The following assertion shows the close relationship between the syndromes and cosets of C.

3.4.2 Theorem *Two vectors $x, y \in \mathbb{F}^n$ yield the same syndrome if and only if they are elements of the same coset of C.*

3.4.3 Definition Let C be $[n, k, d]$ code. For any coset $x + C$ and any vector $y \in C$, we say that y is a coset leader if it is an element of minimum weight in the coset.

Since the syndrome determines the coset, and the error pattern must be an element of the coset, hence the syndrome is the sufficient statistic for determining the error pattern.

3.4.1 Decoding Linear Codes

Let y be a received word. We want to find a vector e of smallest weight in the coset containing y [48].

- after recieving a vector y, compute the syndrome $s = yH^T$;
- find z, a coset leader of the corresponding coset;
- the decoded word is $c = y - z$;
- recover the message m from c.

The above procedure requires to construct a standard array (list of elements of each coset of C) that contains the 2^n vectors ordered by coset. Then the complexity of the decoding procedure is exponential in terms of memory occupancy.

3.5 Cyclic Code

Cyclic codes form a subclass of linear codes [47]. Most of the important linear codes used in practice are cyclic. They are based on polynomials over finite fields so ring theory is used to perform coding theory operations. This additional structure allows very efficient encoding and decoding procedures.

3.5.1 Definition Let C be linear code of length n over $\mathbb{F}_q$. The code C is cyclic if for every word $(c_1, c_2, \ldots, c_n) \in C$ the cyclic shift $(c_n, c_1, \ldots, c_{n-1})$ is also in C.

For instance, the code $\{000, 011, 101, 110\}$ is cyclic. Transition of this concept to algebra is as follows: take $(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$, associate a polynomial

$$a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x]/\langle x^n - 1\rangle, \tag{3.11}$$

where $\mathbb{F}_q[x]$ is a polynomial ring in one variable and I is the ideal of $\mathbb{F}_q[x]$ generated by $x^n - 1$. Any element of factor ring $R = \mathbb{F}_q[x]/I$ has a unique representation which is a polynomial of degree at most $n - 1$. Clearly this residue class ring is isomorphic to $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$.

Proposition 3.1 *Let $R = \mathbb{F}_q[x]/\langle x^n - 1\rangle$. A vector subspace C of R is a cyclic code if and only if C is an ideal in R.*

A cyclic code C can be obtained by multiplying each polynomial of degree less than k by a fixed polynomial $g(x)$ of degree $n - k$ with $g(x)$ a divisor of $x^n - 1$.

Also since every ideal in $R = \mathbb{F}_q[x]\langle x^n - 1\rangle$ is principal, hence every cyclic code can be generated by a monic polynomial of lowest degree in the ideal. It can be stated as follows:

Let $C = \langle g(x)\rangle$ be a cyclic code. Then $g(x)$ is called the generator polynomial of C and $h(x) = (x^n - 1)/g(x)$ is called the parity check polynomial of C.

3.6 Ideals as Linear Codes

Cyclic codes can be defined in several ways but the most elementary way is to define them in terms of ideals in a quotient ring. The above concept of one-dimensional cyclic codes can be naturally extended to n-dimensional cyclic codes. In what follows, $\mathbb{K}[x] = \mathbb{K}[x_1, \ldots, x_n]$. The quotient ring

$$R = \mathbb{K}[x]/I, \tag{3.12}$$

where I is an ideal in $\mathbb{K}[x]$ is defined as:

3.6.1 Definition The quotient of $\mathbb{K}[x]$ mod I is the set of all equivalence classes:

$$\mathbb{K}[x]/I = \{[f] : f \in K[x]\} \tag{3.13}$$

where

$$[f] = \{g \in \mathbb{K}[x] : f - g \in I\}.$$

Since $\mathbb{K}[x]$ is a ring we define sum and product as:

$$[f] + [g] = [f + g] \text{ and } [f] \cdot [g] = [f \cdot g]$$

The set $\mathbb{K}[x]/I$ is a ring under the operations defined above. This forces one to think of ideals in this ring. The definition is the same as the definition of ideals in $\mathbb{K}[x]$. For the purpose of computation in this quotient ring, we need to define the form of elements first. The description of simple representatives of these equivalence classes stems out of the fact that the remainder on division of a polynomial f by a Groebner basis G for an ideal I is uniquely determined by the polynomial f. Let G be a Groebner basis of an ideal I. Also consider the ideal defined by the leading terms of I, $\mathrm{lt}(I)$, as given in the previous chapter. The following map:

$$\phi : \mathbb{K}[x]/I \to S \tag{3.14}$$

defined by

$$\phi[f] = f^G, \text{ where } S = Span(x^\alpha : x^\alpha \notin \text{lt}(I))$$

establishes a one to one correspondence between the classes $\mathbb{K}[x]/I$ and the elements of S. Formally, this can be descibed as follows [18, 25]:

Proposition 3.2 *Let $I \subset \mathbb{K}[x]$ be an ideal. Then*

$$R = \mathbb{K}[x]/I \tag{3.15}$$

is isomorphic as a k-vector space to $S = Span(x^\alpha : x^\alpha \notin \text{lt}(I))$

Hence standard representatives for elements in R can be computed by finding remainders with respect to G. For the better understanding of this ring structure we try to explore the form of ideals in R. There is a close relation between ideals in the quotient $\mathbb{K}[x]/I$ and ideals in $\mathbb{K}[x]$ as stated by the following proposition.

Proposition 3.3 *Let I be an ideal in $\mathbb{K}[x]$. The ideals in the quotient ring $\mathbb{K}[x]/I$ are in one to one correspondence with the ideals of $\mathbb{K}[x]$ containing I.*

If J is an ideal in $\mathbb{K}[x]$ containing I, the corresponding ideal in $\mathbb{K}[x]/I$ will be

$$J/I = \{[j] : j \in J\}. \tag{3.16}$$

On the other hand if J' is an ideal in the quotient ring then the form of the corresponding ideal in $K[x]$ is

$$J = \{j : [j] \in J'\}. \tag{3.17}$$

3.6.2 Remark Replace $\mathbb{K}$ by $\mathbb{F}_p$ in R, and consider the quotient ring

$$R = \mathbb{F}_p[x_1, \ldots, x_n]/\langle x_1^p, \ldots, x_n^p \rangle. \tag{3.18}$$

Any ideal I in R will be a linear code closed under products by elements in R. Any code obtained in this way is called an n-dimensional cyclic code. One main advantage of an n-dimensional cyclic code over linear code is that their extra structure helps in describing a compact encoding algorithm, which will be discussed in the next chapter.

3.7 Families of Codes

Now we will discuss some of the most famous families of codes.

3.7.1 Hamming Codes

The family of Hamming codes is probably the most famous of all error correcting codes. These codes were discovered independently by M. Golay in 1949 and R.W. Hamming in 1950. These are perfect linear codes. All binary Hamming codes are equivalent to cyclic codes. For each $r > 0$, $H_q(r)$ is an $[n, k, d]$ code where

$$n = (q^r - 1)/(q - 1), k = n - r, d = 3.$$

These codes are single error correcting. Since these are linear codes their encoding process can be described in terms of the generating matrix, for example, as given earlier, the following matrix generates the $[7, 4, 3]$ Hamming code:

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

The corresponding parity check matrix is:

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Note that the columns of H are exactly the non-zero vectors of $\mathbb{F}_2^3$. The matrix H can be used to decode binary Hamming code. Let y be a received binary vector, compute its syndrome s w.r.t H, if $s = 0$ then the received word is a codeword, otherwise compare the computed syndrome with the columns of H. If H_i is a column equal to s then there is an error in the i^{th} position of y. Hence the decoded codewords is $y + e_i$. This method fails if more than one error occurs.

3.7.2 Reed Muller Codes

The very first definition of the Reed Muller codes was given in terms of Boolean functions, by D.E. Muller in 1954 [43], while presenting a mathematical model for circuit. Later, I.S. Reed proposed a decoding algorithm for these codes. These binary linear codes have a good practical value and nice decoding properties. Reed Muller codes can be defined in many ways [16, 24], here they are described through Boolean polynomials and Boolean functions [47].

A Boolean function of m variables is a function $f(x_1, \ldots, x_m)$ from $\mathbb{F}_2^m$ to $\mathbb{F}_2$. A Boolean monomial p in variables $\{x_1, \ldots, x_m\}$ is an expression of the form

$$x_1^{r_1} x_2^{r_2} \cdots x_m^{r_m} \text{ where } r_i \in \{0, 1, 2, \ldots\} \text{ and } 1 \leq i \leq m.$$

The reduced form of p is obtained by applying the rules $x_i x_j = x_j x_i$ and $x_i^2 = x_i$ until the factors are distinct. A Boolean polynomial is a linear combination of Boolean monomials with coefficient from $\mathbb{F}_2$. The degree of a Boolean polynomial is the largest of the degrees of monomials that form p, in its reduced form. The set B_m of all Boolean polynomials form a vector space over $\mathbb{F}_2$. The total number of distinct Boolean monomials is

$$1 + \binom{m}{1} + \ldots + \binom{m}{m} = 2^m,$$

hence there are 2^{2^m} distinct Boolean polynomials in m variables. For every Boolean function $f(x_1, \ldots, x_m)$, there exists a Boolean polynomial $P(x_1, \ldots, x_m)$.

3.7.1 Definition Let $0 \leq r \leq m$, the r^{th} order Reed-Muller code $R(r, m)$ is the set of all binary strings of lenght 2^m associated with the Boolean polynomial p of degree at most r.

The 0^{th} order Reed muller code is just the repetition code of length 2^m of 0's or 1's, while the $m^{th}order$ code consists of all binary strings of length 2^m. The Reed Muller codes have minimum distance $2^m - r$. The following theorem gives a recursive definition of Reed-Muller codes.

3.7.2 Theorem *Let r, m be intergers such that $0 \leq r \leq m$. The $r + 1^{th}$ order Reed Muller code of length 2^{m+1} is*

$$RM(r+1,m+1) = \{(u, u+v) : u \in RM(r+1,m), v \in RM(r,m)\}.$$

If $G(r,m)$ is the generator matrix of the Reed Muller code $RM(r,m)$ then

$$G(r+1,m+1) = \begin{pmatrix} G(r+1,m) & G(r+1,m) \\ 0 & G(r,m) \end{pmatrix} \tag{3.19}$$

is the generator matrix of $RM(r+1,m+1)$.

3.7.3 Example

$$GM(1,5) = \left(\begin{array}{cccc|cccc} 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 \\ 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 \\ 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 \\ 0000 & 1111 & 0000 & 1111 & 0000 & 1111 & 0000 & 1111 \\ 0000 & 0000 & 1111 & 1111 & 0000 & 0000 & 1111 & 1111 \\ \hline 0000 & 0000 & 0000 & 0000 & 1111 & 1111 & 1111 & 1111 \end{array}\right) = \begin{pmatrix} 1 \\ v_5 \\ v_4 \\ v_3 \\ v_2 \\ v_1 \end{pmatrix}$$

♦

3.7.4 Lemma *Let r, m be integers such that $0 \le r \le m$. Let $RM(r,m)$ be the r^{th} order Reed-Muller code of lenght 2^m.*

- *The dimension of the code is $k = 1 + \begin{pmatrix} m \\ 1 \end{pmatrix} + \begin{pmatrix} m \\ 2 \end{pmatrix} + \ldots + \begin{pmatrix} m \\ r \end{pmatrix}$.*
- *The minimum distance is $d = 2^{m-r}$.*
- *$RM(r,m) \subset RM(r+1,m)$, for all $r < m$.*
- *$RM(r,m)^{\perp} = RM(m-r-1,m)$, for all $r < m$.*

In particular,

- $RM(0,m)$ is the repetition code.
- $RM(1,m)$ is the dual of the extended Hamming code.
- $RM(m-2,m)$ is the extended Hamming code.
- $RM(m-1,m)$ is the even weight code (all vectors in $\mathbb{F}_2^{2^m}$ of even weight).
- $RM(m,m) = \mathbb{F}_2^{2^m}$.

3.7.3 Golay Codes

The binary Golay code is one of the most important type of linear binary codes [28, 14]. Perfect codes are considered the best codes and are of much interest to mathematicians. They play an important role in coding theory for theoretical and practical reasons. In 1949, M. Golay [28] noticed that:

$$\binom{23}{0}+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}=2^{11}. \tag{3.20}$$

It indicated to him that the possibility of a $[23,12]$ perfect binary code existed that could correct three or fewer errors. It is one of the few examples of a nontrivial perfect code. This is the only known code capable of correcting any combination of three or fewer random errors in a block of 23 elements. The binary Golay code C_{23} is a $[23,12,7]$ code with parity check matrix $H=(M,I_{11})$, where I_{11} is the 11×11 identity matrix and M is the 11×12 matrix given by

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

The ternary Golay code C_{11} is an $[11,6,5]$ perfect code with parity check matrix $H_{11}=(N,I_5)$, where

$$N=\begin{pmatrix}
1&0&1&2&2&1\\
1&1&0&1&2&2\\
1&2&1&0&1&2\\
1&2&2&1&0&1\\
1&1&2&2&1&0
\end{pmatrix}.$$

Chapter 4

Variants of Reed Muller Codes

4.1 Introduction

It has been established by several authers that many classical codes are ideals in quotient rings [37]. Berman [5], showed that binary Reed Muller codes coincide with powers of the radical of the quotient ring

$$R = \mathbb{F}_2[x_1, \ldots, x_n]/\langle x_1^2 - 1, \ldots, x_n^2 - 1\rangle. \tag{4.1}$$

Later Charpin [13], proved it for generalised Reed Muller codes. Here we have presented an approach, similar to Landrock and Manz [37], to define variants of Reed Muller codes and their parameters. Moreover, a strong link between the theory of Groebner bases and cyclic codes, defined in terms of ideals in quotient ring, is explored. This chapter is organised as follows: In Section 4.1, Groebner bases are presented for an ideal which plays a major role in this work. Outline of a general encoding process for a cyclic code via Groebner bases is described in Section 4.2. Variants of Reed Muller codes and their decoding process are given in Section 4.3. Lastly, parameters for the variants of primitive Reed Muller codes are given.

4.2 Groebner Basis Construction

This section describes the construction of a reduced Groebner basis of an ideal, which is later used to define a class of codes which contains primitive Reed Muller

codes. Let $\mathbb{K}$ be a field and let $\mathbb{K}[x] = \mathbb{K}[x_1, \ldots, x_n]$ be a commutative polynomial ring over $\mathbb{K}$. Take a nonempty subset S of $\mathbb{N}_0^n$ and consider the ideal $I = I(S)$ generated by the set

$$\{\eta(\boldsymbol{a}) : \boldsymbol{a} \in S\}, \tag{4.2}$$

where

$$\eta(\boldsymbol{a}) = (x_1 - 1)^{a_1} \cdots (x_n - 1)^{a_n}, \quad a_1 \geq 0, \ldots, a_n \geq 0. \tag{4.3}$$

Let $M = M(S)$ be the set of n-tuples $\boldsymbol{a} \in S$ that are minimal with respect to the component-wise natural $\leq$-ordering. In particular, if we choose $S = \mathbb{N}_0^n$ then the set of minimal elements will be $M(S) = \{\mathbf{0}\}$ and $I(S) = \mathbb{K}[x]$, since $1 \in I(S)$. Secondly, if $S = \mathbb{N}_0^n \setminus \{\mathbf{0}\}$ then $M(S)$ consists of the unit vectors and the ideal $I = I(S)$ is generated by the terms $x_j - 1$, $1 \leq j \leq n$. The following theorem constructs a Groebner basis for an ideal, which will be considered later to understand the structure of the corresponding codes.

4.2.1 Theorem *For any monomial order on* $\mathbb{K}[x]$*, the ideal* $I = I(S)$ *in* $\mathbb{K}[x]$ *has the reduced Groebner basis*

$$G = \{\eta(\boldsymbol{a}) : \boldsymbol{a} \in M\}. \tag{4.4}$$

The ideal of leading terms of I *equals* $\langle\{x^{\boldsymbol{a}} : \boldsymbol{a} \in M\}\rangle$.

Observe that for each term ordering $\succ$ on $\mathbb{N}_0^n$, the leading term of $\eta(\boldsymbol{a})$, $\boldsymbol{a} \in \mathbb{N}_0^n$, is $x^{\boldsymbol{a}}$. Indeed, each monomial in $\eta(\boldsymbol{a})$ is of the form $x^{\boldsymbol{b}}$ for some $\boldsymbol{b} \in \mathbb{N}_0^n$ with $\boldsymbol{b} \leq \boldsymbol{a}$. Thus $\boldsymbol{a} = \boldsymbol{b} + \boldsymbol{c}$ for some $\boldsymbol{c} \in \mathbb{N}_0^n$. But $\mathbf{0} \leq \boldsymbol{c}$ and so $\boldsymbol{b} \leq \boldsymbol{b} + \boldsymbol{c} = \boldsymbol{a}$. The quest for a proof of this theorem led us to two propositions which are of great interest and importance in themselves. Proofs of these propositions are given according to the following setting: To each nonempty subset S of $\mathbb{N}_0^n \setminus \{\mathbf{0}\}$ define

$$S' = \{(a_1, \ldots, a_j - 1, \ldots, a_n) : (a_1, \ldots, a_j, \ldots, a_n) \in S, a_j > 0, 1 \leq j \leq n\}.$$

Then

$$M' = \{(a_1, \ldots, a_j - 1, \ldots, a_n) : (a_1, \ldots, a_j, \ldots, a_n) \in M, a_j > 0, 1 \leq j \leq n\}$$

is the corresponding set of minimal elements of S'. Finally, put $G' = \{\eta(\boldsymbol{a}) \mid \boldsymbol{a} \in M'\}$.

4.2.2 Lemma *For each polynomial $f \in \mathbb{K}[x]$ and each variable x_j, $1 \leq j \leq n$, we have*

$$(x_j - 1)\text{rem}(f, G') = \text{rem}((x_j - 1)f, G).$$

Proof: Fix a term ordering $\prec$ on $\mathbb{K}[x]$. First, suppose there is a generator $g \in G'$ such that $\text{lm}(f)$ is divisible by $\text{lm}(g)$. Then $\text{rem}(f, G') = \text{rem}(f - g' \cdot g, G')$ for some monomial $g' \in \mathbb{K}[x]$ and so $\text{lm}((x_j - 1)f)$ is divisible by $\text{lm}((x_j - 1)g)$. But $(x_j - 1)g \in G$ and thus $\text{rem}((x_j - 1) \cdot f, G) = \text{rem}((x_j - 1)[f - g'g], G)$. We may assume that the assertion holds for all polynomials f' with $f' \prec f$. But $f - g'g \prec f$ and thus $(x_j - 1)[f - g'g] \prec (x_j - 1)f$. Therefore, $\text{rem}((x_j - 1)[f - g'g], G) = (x_j - 1)\text{rem}(f - g'g, G') = (x_j - 1)\text{rem}(f, G')$, as required.

Second, suppose there is no generator $g \in G'$ such that $\text{lm}(f)$ is divisible by $\text{lm}(g)$. Then there is no generator $g \in G'$ such that $\text{lm}((x_j - 1)f)$ is divisible by $\text{lm}((x_j - 1)g)$. Write $f = m + h$, where $m = \text{lt}(f)$. Then $\text{rem}(f, G') = \text{lt}(f) + \text{rem}(f - \text{lt}(f), G') = m + \text{rem}(h, G')$. Moreover, $\text{rem}((x_j - 1)f, G) = \text{lt}((x_j - 1)f) + \text{rem}((x_j - 1)f - \text{lt}((x_j - 1)f), G) = x_j m + \text{rem}((x_j - 1)h - m, G)$.

First, suppose that the leading term of $(x_j - 1)h - m$ is $-m$. Thus $\text{rem}((x_j - 1)h - m, G) = -m + \text{rem}((x_j - 1)h - m - (-m), G) = -m + \text{rem}((x_j - 1)h, G)$. We may assume that the assertion holds for all polynomials f' with $f' \prec f$. But $h \prec f$ and thus $\text{rem}((x_j - 1)h, G) = (x_j - 1)\text{rem}(h, G')$. It follows that $\text{rem}((x_j - 1)f, G) = (x_j - 1)m + (x_j - 1)\text{rem}(h, G') = (x_j - 1)[m + \text{rem}(h, G')] = (x_j - 1)\text{rem}(f, G')$, as required.

Second, assume that the leading term of $(x_j - 1)h - m$ is $x_j m'$, where $h = m' + h'$ and m' is the leading term of h. There are two cases.

First, suppose that there exists no generator $g \in G'$ such that $\text{lm}(h) = m'$ is divisible by $\text{lm}(g)$. Thus $\text{rem}(h, G') = m' + \text{rem}(h', G')$ and there is no generator $g \in G'$ such that $\text{lm}((x_j - 1)h) = x_j m'$ is divisible by $\text{lm}((x_j - 1)g)$. But $(x_j - 1)g \in G$ and thus $\text{rem}((x_j - 1)h - m, G) = x_j m' + \text{rem}((x_j - 1)h' - (m + m'), G)$. It follows that $\text{rem}((x_j - 1)f, G) = x_j(m + m') + \text{rem}((x_j - 1)h' - (m + m'), G)$. But there is no generator $g \in G'$ such that $\text{lm}(g)$ divides m or m' and so there is no generator $g \in G$ with this property. It follows that $\text{rem}((x_j - 1)f, G) = (x_j - 1)(m + m') + \text{rem}((x_j - 1)h', G)$. On the other hand, $(x_j - 1)\text{rem}(f, G') = (x_j - 1)(m + m') + (x_j - 1)\text{rem}(h', G')$. Since $h' \prec f$, we obtain by induction, $(x_j - 1)\text{rem}(h', G') = \text{rem}((x_j - 1)h', G)$ and thus $\text{rem}((x_j - 1)f, G) = (x_j - 1)(m + m') + \text{rem}((x_j - 1)h', G)$, as required.

Second, assume that there is a generator $g \in G'$ such that $\mathrm{lm}(h) = m'$ is divisible by $\mathrm{lm}(g)$. Then $\mathrm{rem}(f, G') = m + \mathrm{rem}(h, G') = m + \mathrm{rem}(h - g'g, G')$ for some $g' \in A$ and $\mathrm{lm}((x_j - 1)h) = x_j m'$ is divisible by $\mathrm{lm}((x_j - 1)g)$. But $(x_j - 1)g \in G$ and thus $\mathrm{rem}((x_j - 1)h, G) = \mathrm{rem}((x_j - 1)(h - g'g)), G) = (x_j - 1)\mathrm{rem}(h - g'g, G')$, where the last equation follows by induction, since $h - g'g \prec h$. Now $\mathrm{rem}((x_j - 1)f, G) = mx_j + \mathrm{rem}((x_j - 1)h - m, G) = mx_j + \mathrm{rem}((x_j - 1)(h - g'g) - m, G)$. But by hypothesis, there is no generator $g \in G'$ such that $\mathrm{lm}(g)$ divides m and so there is no generator $g \in G$ with this property. Thus the last term becomes $(x_j - 1)m + \mathrm{rem}((x_j - 1)(h - g'g), G)$. Since $h - g'g \prec h$, we obtain by induction the term $(x_j - 1)m + (x_j - 1)\mathrm{rem}((h - g'g), G')$, which equals $(x_j - 1)\mathrm{rem}(f, G')$, as claimed. ■

4.2.3 Lemma *Let S be a nonempty subset of $\mathbb{N}_0^n \setminus \{\mathbf{0}\}$. For each polynomial $f \in I(S)$, $\mathrm{rem}(f, G') = 0$ implies $\mathrm{rem}(f, G) = 0$.*

Proof: Let $f \in I(S)$ such that $\mathrm{rem}(f, G') = 0$. First, suppose there is a generator $g' \in G'$ such that $\mathrm{lm}(f)$ is divisible by $\mathrm{lm}(g')$. Since $f \in I(S)$, we have that $\mathrm{lm}(f)$ is divisible by $\mathrm{lm}((x_j - 1)g')$ for some $1 \leq j \leq n$. But $g = (x_j - 1)g'$ lies in G and thus $\mathrm{rem}(f, G) = \mathrm{rem}(f - h'g, G) = \mathrm{rem}(f - [h'(x_j - 1)]g', G') = \mathrm{rem}(f, G')$ for some polynomial $h' \in \mathbb{K}[x]$.

Second, assume that there is no generator $g' \in G'$ such that $\mathrm{lm}(g')$ divides $\mathrm{lm}(f)$. Then there is no generator $g \in G$ such that $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$. Thus we obtain $\mathrm{rem}(f, G') = \mathrm{lt}(f) + \mathrm{rem}(f - \mathrm{lt}(f), G') = \mathrm{rem}(f, G)$.

Therefore, we can mimic the division of f with respect to G by the division of f with respect to G'. ■

Now we are able to prove our main theorem, based on these lemmas, using induction.

Proof: Let S be a subset of $\mathbb{N}_0^n$. First we prove that G provides a generating set of the ideal $I = I(S)$. Indeed, let $\boldsymbol{a} \in S$. Assume that $\boldsymbol{b} \in M$ is a minimal element such that $\boldsymbol{b} \leq \boldsymbol{a}$. Then $\boldsymbol{a} = \boldsymbol{b} + \boldsymbol{c}$ for some $\boldsymbol{c} \in \mathbb{N}_0^n$ and thus $\eta(\boldsymbol{a}) = \eta(\boldsymbol{b}) \cdot \eta(\boldsymbol{c})$. Thus the claim follows.

In order to show that the ideal I is finitely generated, we refer to Dickson's Lemma [18], which implies that there is a finite set of vectors $\boldsymbol{s}^{(1)}, \ldots, \boldsymbol{s}^{(r)} \in S$ such that

$$S \subseteq (\boldsymbol{s}^{(1)} + \mathbb{N}_0^n) \cup \ldots \cup (\boldsymbol{s}^{(r)} + \mathbb{N}_0^n).$$

For each element $\boldsymbol{s} \in \boldsymbol{s}^{(i)} + \mathbb{N}_0^n$, $1 \leq i \leq r$, there is some $\boldsymbol{t} \in \mathbb{N}_0^n$ such that $\boldsymbol{s} = \boldsymbol{s}^{(i)} + \boldsymbol{t}$. Thus $\boldsymbol{s}^{(i)} \leq \boldsymbol{s}$ and hence the set of minimal elements of S is contained in the set $\{\boldsymbol{s}^{(1)}, \ldots, \boldsymbol{s}^{(r)}\}$. The claim follows.

For proving that G is a Groebner basis for $I = I(S)$. We need to show that $\mathrm{rem}(S(g,h), G) = 0$ for all polynomials $g, h \in G$. First, take a nonempty subset $S \subseteq \mathbb{N}_0^n$ such that $\mathbf{0} \in S$. Then $I(S) = \mathbb{K}[x]$, $M(S) = \{\mathbf{0}\}$ and $G = \{1\}$ is a Groebner basis for $\mathbb{K}[x]$.

Second, let S be a nonempty subset of $\mathbb{N}_0^n \setminus \{\mathbf{0}\}$. Let $\boldsymbol{a}, \boldsymbol{b} \in M(S)$ such that the generators $\eta(\boldsymbol{a})$ and $\eta(\boldsymbol{b})$ have a common factor $x_j - 1$, $1 \leq j \leq n$. By considering the set S', there exist $\boldsymbol{a}', \boldsymbol{b}' \in M(S')$ such that $\eta(\boldsymbol{a}) = (x_j - 1)\eta(\boldsymbol{a}')$ and $\eta(\boldsymbol{b}) = (x_j - 1)\eta(\boldsymbol{b}')$. By induction, we may assume that G' is a Groebner basis for $I(S')$. We have $S(\eta(\boldsymbol{a}), \eta(\boldsymbol{b})) = (x_j - 1)S(\eta(\boldsymbol{a}'), \eta(\boldsymbol{b}'))$. Thus by Lemma 4.2.2, $\mathrm{rem}(S(\eta(\boldsymbol{a}), \eta(\boldsymbol{b})), G) = (x_j - 1)\mathrm{rem}(S(\eta(\boldsymbol{a}'), \eta(\boldsymbol{b}')), G')$. By induction, we have $\mathrm{rem}(S(\eta(\boldsymbol{a}'), \eta(\boldsymbol{b}')), G') = 0$ and hence the assertion follows.

Let $\boldsymbol{a}, \boldsymbol{b} \in M(S)$ such that the generators $\eta(\boldsymbol{a})$ and $\eta(\boldsymbol{b})$ have no common factor. Assume that $a_u > 0$, $a_{u+1} = \ldots = a_n = 0$, $b_1 = \ldots = b_{v-1} = 0$, and $b_v > 0$, where $1 \leq u < v \leq n$. By considering the set S', the elements $\boldsymbol{a}' = (a_1, \ldots, a_u - 1, 0, \ldots, 0)$ and $\boldsymbol{b}' = (0, \ldots, 0, b_v - 1, \ldots, b_n)$ belong to the set $M' = M(S')$ of minimal elements of S'. We have

$$S(\eta(\boldsymbol{a}), \eta(\boldsymbol{b})) = g_u g_v S(\eta(\boldsymbol{a}'), \eta(\boldsymbol{b}')) + \prod_{i=1}^{u} g_i^{a_i} \cdot \eta(\boldsymbol{b}') - \prod_{i=v}^{n} g_i^{b_i} \cdot \eta(\boldsymbol{a}').$$

This polynomial lies in $I(S)$. Moreover, by induction, the polynomial on the right hand side reduces to zero modulo G'. Thus, by Lemma 4.2.3, the polynomial reduces to zero modulo G. The claim follows.

We proceed by proving that the Groebner basis G for I is minimal. Indeed, the elements of G are monic. Moreover, let $\eta(\boldsymbol{a})$ and $\eta(\boldsymbol{b})$ be distinct elements of G. If the leading term $bx^{\boldsymbol{a}}$ of $\eta(\boldsymbol{a})$ would be a divisor of the leading term $x^{\boldsymbol{b}}$ of $\eta(\boldsymbol{b})$, then $\boldsymbol{a} \leq \boldsymbol{b}$ contradicting that $\boldsymbol{a}$ and $\boldsymbol{b}$ lie in M and thus are $\leq$-incompatible. Hence G is minimal.

By construction the minimal Groebner basis G for I is reduced. To see this, let $\eta(\boldsymbol{a})$ and $\eta(\boldsymbol{b})$ be distinct elements of G. Each monomial in the support of $\eta(\boldsymbol{a})$ is of the form $\boldsymbol{x}^{\boldsymbol{c}}$ such that $\boldsymbol{c} \leq \boldsymbol{a}$. If the leading term $\boldsymbol{x}^{\boldsymbol{b}}$ of $\eta(b)$ would divide $\boldsymbol{x}^{\boldsymbol{c}}$ then $\boldsymbol{b} \leq \boldsymbol{c}$. But then $\boldsymbol{b} \leq \boldsymbol{a}$ contradicting that $\boldsymbol{a}$ and $\boldsymbol{b}$ are $\leq$-incompatible. The claim follows. ■

We end this section by giving an application of the above theorem. The reduced Greobner basis in this example is constructed by considering only the minimal elements belonging to the set S.

4.2.4 Example Let $p = 7$ and $n = 2$. Define $S = \{(a_1, a_2) \mid (a_1 + 1)(a_2 + 1) \geq 14\}$. The ideal I has the reduced Groebner basis

$$\{\eta(13,0), \eta(6,1), \eta(4,2), \eta(3,3), \eta(2,4), \eta(1,6), \eta(0,13)\}.$$

♦

4.3 Encoding Linear Codes using Groebner Bases

In the previous chapter natural generalization of 1-dimensional cyclic codes to n-dimensional cyclic codes was discussed. Groebner bases play a pivotel role in describing this connection. This section elaborates the encoding procedure for cyclic codes described in [19].

Consider the quotient ring R of the commutative polynomial ring $\mathbb{F}_p[x_1, \ldots, x_n]$ of the form

$$R = \mathbb{F}_p[x_1, \ldots, x_n]/\langle x_1^p - 1, \ldots, x_n^p - 1\rangle. \tag{4.5}$$

As an $\mathbb{F}_p$-algebra, R is isomorphic to the group algebra $\mathbb{F}_pG$ of an elementary abelian p-group G of order p^n. As an $\mathbb{F}_p$-vector space, R is isomorphic to the space $\mathbb{F}_p^{p^n}$.

It is clear that $H = \{x_1^p - 1, \ldots, x_n^p - 1\}$ is a Groebner basis for the ideal it generates, with respect to all monomial orders, since all leading monomials of the generators are relatively prime, hence the S-polynomial goes to zero for any two generators, which proves that H is indeed a Groebner basis. Therefore standard representatives for the elements of R can be computed by applying the division algorithm in $\mathbb{F}_p[x_1, \ldots, x_n]$ and computing remainders with respect to H. In this way, representatives of all elements of R are given by the polynomials whose degree in x_i is at most $p-1$, $1 \leq i \leq n$. These polynomials are called standard forms of the elements in R. Next, a linear code is described in terms of an ideal in the quotient ring. Let $I = \langle f_1, \ldots, f_m\rangle$ be an ideal in the polynomial ring $\mathbb{F}_p[x_1, \ldots, x_n]$. Consider the associated ideal C in the quotient ring R that is generated by the residue classes of

the elements of I. A generating set for this ideal is given by $\{[f_1], \ldots, [f_m]\}$, where $[f]$ denotes the coset $f + I$ in R.

The ideal J corresponding to C in the polynomial ring $\mathbb{F}_p[x_1, \ldots, x_n]$ is given as

$$J = \langle f_1, \ldots, f_m \rangle + \langle x_1^p - 1, \ldots, x_n^p - 1 \rangle. \tag{4.6}$$

The code C equals $J/\langle x_1^p - 1, \ldots, x_n^p - 1 \rangle$ and thus by the Standard Isomorphism Theorems there is an $\mathbb{F}_p$-algebra isomorphism

$$R/C \cong \mathbb{F}_p[x_1, \ldots, x_n]/J. \tag{4.7}$$

The ideal C can be viewed as a linear code in the ambient space R. For this, the space R is represented by the set of polynomials in standard form. An $\mathbb{F}_p$-basis of R is given by all monomials in standard form; that is, all monomials in which each x_i appears to a power of at most $p - 1$, $1 \leq i \leq p - 1$. The ambient space R has the dimension p^n and so, by definition, the code C has the length p^n. The codewords in C are represented in standard form and thus each codeword is a linear combination of monomials in standard form. The Hamming weight of each codeword is measured according to the number of involved monomials in standard form.

Fix a term ordering on $\mathbb{F}_p[x_1, \ldots, x_n]$. Let G be a Groebner basis for the ideal J. A Groebner basis for J enables us to determine whether an element of R is a codeword or not (using ideal-membership concept).

4.3.1 Proposition *An element of the ambient space R represented in standard form is a codeword if and only if its remainder on division by G is zero.*

Proof: The division of an element f in standard form by the Groebner basis for J yields a unique remainder (in standard form). By Eq. (4.7), this remainder is zero if and only if f lies in the code C. ■

The following proposition gives the parameters of the considered code.

4.3.2 Proposition *The linear code C is a $[p^n, k]$-code over $\mathbb{F}_p$ where the dimension k is given by the number of non-standard monomials for J.*

Proof: Each element of $\mathbb{F}_p[x_1, \ldots, x_n]$ can be divided by the Groebner basis G of J such that the remainder is a linear combination of standard monomials. These monomials are linearly independent in $\mathbb{F}_p[x_1, \ldots, x_n]/J$ and form an $\mathbb{F}_p$-basis of $F_p[x_1, \ldots, x_n]/J$. Thus by Eq. (4.7), the dimension of the $\mathbb{F}_p$-vector space R/C is the number of standard monomials for J. But the dimension of the linear code C equals the difference $\dim R - \dim R/C$ and is thus given by the number of non-standard monomials for J. ■

It follows that the information positions of the linear code C are the coefficients of the non-standard monomials for J, while the parity check positions are the coefficients of the standard monomials for J.

The extra structure of the linear code C given by a reduced Groebner basis for the ideal J provides a compact encoding function. The following encoding procedure was stated in [18].

4.3.3 Proposition *If w is an information word given as an $\mathbb{F}_p$-linear combination of non-standard monomials for J, then $w - \mathrm{rem}(w, G)$ is a codeword in C.*

Proof: The polynomials w and $\mathrm{rem}(w, G)$ are in standard form. The difference $w - \mathrm{rem}(w, G)$ lies in J. As this defference is in standard form it belongs to the code C. ■

4.4 Variants of Primitive Reed-Muller Codes

This section is a straightforward application of the results given in the last two sections. Consider the ideal $J(S)$ in the polynomial ring $\mathbb{F}_p[x_1, \ldots, x_n]$ given as

$$J(S) = I(S) + \langle x_1^p - 1, \ldots, x_n^p - 1 \rangle$$

and the corresponding code $C(S)$ defined as $J(S)/\langle x_1^p - 1, \ldots, x_n^p - 1 \rangle$.

Let $P = \{0, 1, \ldots, p-1\}$. If we put $S' = S \cap P^n$, then we have $J(S') = J(S)$ and thus $C(S') = C(S)$. Let $M' = M(S')$ be the set of all n-tuples $\boldsymbol{a} \in S'$ that are minimal with respect to the component-wise natural $\leq$-ordering. In the following, we assume that S' is nonempty. By Theorem 4.2.1, we obtain the following result.

4.4.1 Corollary *The set* $G = \{\eta(\boldsymbol{a}) : \boldsymbol{a} \in M'\}$ *forms a reduced Groebner basis for the ideal* $J(S')$ *and the corresponding ideal of leading terms equals* $\langle\{x^{\boldsymbol{a}} : \boldsymbol{a} \in M'\}\rangle$.

The main properties of the linear code $C(S')$ are summarized as follows.

4.4.2 Theorem *The linear code* $C(S')$ *is a* $[p^n, k, d]$ *code over* $\mathbb{F}_p$*, where the dimension* k *is the number of generators* $\eta(\boldsymbol{a})$ *for which there is an element* $\boldsymbol{m} \in M'$ *such that* $\boldsymbol{m} \leq \boldsymbol{a}$*, and minimum distance* d *is given by the minimum Hamming weight of the generators* $\eta(\boldsymbol{m})$*, where* $\boldsymbol{m} \in M'$*. The information positions of the code* $C(S')$ *are the coefficients of the monomials in the set* $\{x^{\boldsymbol{a}} : \exists \boldsymbol{m} \in M' : \boldsymbol{m} \leq \boldsymbol{a}\}$.

Proof: First, the set $B = \{\eta(\boldsymbol{a}) : \boldsymbol{a} \in P^n\}$ is linearly independent [5, 13]. By definition, each codeword c in $C(S')$ can be written according to the Groebner basis as follows,

$$c = \sum_{\boldsymbol{a} \in M'} f_{\boldsymbol{a}} \eta(\boldsymbol{a}),$$

where $f_{\boldsymbol{a}}$ is a polynomial in R given in standard form. But each variable x_i can be written as $x_i = (x_i - 1) + 1$, $1 \leq i \leq n$. Thus each monomial $x^{\boldsymbol{a}}$ is given as a linear combination of elements of the form $\eta(\boldsymbol{b})$, where $\boldsymbol{b} \in P^n$. But $\eta(\boldsymbol{a})\eta(\boldsymbol{b}) = \eta(\boldsymbol{a} + \boldsymbol{b})$ and thus the codeword c can be written as a linear combination of elements $\eta(\boldsymbol{a})$, where $\boldsymbol{a} \in S'$. The result on the dimension follows.

Second, the code C is visible in the sense that the minimum distance equals the minimum Hamming weight of its generators $\eta(\boldsymbol{a})$, where $\boldsymbol{a} \in S'$ [5, 13, 59]. But for each generator $\eta(\boldsymbol{a})$ with $\boldsymbol{a} \in S'$ there is a generator $\eta(\boldsymbol{m})$ with $\boldsymbol{m} \in M'$ such that $\boldsymbol{m} \leq \boldsymbol{a}$; that is, $\eta(\boldsymbol{a})$ is divisible by $\eta(\boldsymbol{m})$. Thus the minimum Hamming weight is attained by some generator $\eta(\boldsymbol{m})$ with the property that $\boldsymbol{m} \in M'$.

Finally, the information positions of the code $C(S')$ are given by the non-standard monomials, which by definition correspond to the monomials in the ideal of leading terms. But by Corollary 4.4.1, this ideal is generated by the monomials $x^{\boldsymbol{a}}$, $\boldsymbol{a} \in M'$, and thus the result follows. ■

This considered class of codes contains the primitive Reed Muller codes. To see this, put $N = n(p-1)$ and consider the set $S_l = \{\boldsymbol{a} \in P^n \mid \sum_{i=1}^{n} a_i \geq l\}$, $0 \leq l \leq N$. The associated code $C(S_l)$ is called primitive Reed-Muller code of order $N - l$. For instance, the code $C(S_0)$ is the full code R, the code $C(S_1)$ equals the radical

of R, and the code $C(S_N)$ is the constant-weight code [5, 13]. The corresponding set of minimal elements is $M(S_l) = \{\boldsymbol{a} \in P^n : \sum_{i=1}^n a_i = l\}$, $0 \le l \le N$. By Corollary 4.4.1, the set $G_l = \{\eta(\boldsymbol{a}) \mid \sum_{i=1}^n a_i = l\}$ is a reduced Groebner basis for the ideal $J(S_l)$, $0 \le l \le N$.

Let $P = \{0, 1, \ldots, p-1\}$. The set P^n forms a lattice with the component-wise natural $\le$-order. Denote by $\mathbf{1} = (p-1, \ldots, p-1)$ the largest element in P^n. Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be elements in P^n. We have

$$\eta(\boldsymbol{a}) \cdot \eta(\boldsymbol{b}) = \begin{cases} \eta(\boldsymbol{a}+\boldsymbol{b}), & \boldsymbol{a}+\boldsymbol{b} \le \mathbf{1}, \\ 0, & \text{otherwise.} \end{cases} \tag{4.8}$$

Putting $\bar{\boldsymbol{a}} = (p - a_1^{-1}, \ldots, p - a_n^{-1})$, we obtain

$$\eta(\boldsymbol{a}) \cdot \eta(\bar{\boldsymbol{a}}) = \eta(\mathbf{1}).$$

4.4.3 Proposition *The dual code of C generated as an ideal by $\{\eta(\boldsymbol{a}) : \boldsymbol{a} \in M'\}$ is generated as an ideal by the set*

$$\{\eta(\boldsymbol{b}) : \boldsymbol{b} \not\le \bar{\boldsymbol{a}} \text{ for all } \boldsymbol{a} \in M'\}.$$

Proof: It is known that each linear code C given as an ideal in the group algebra $\mathbb{K}G$ has the dual code $C^\perp = \overline{\mathcal{L}(C)}$, where $\mathcal{L}(C) = \{a \in \mathbb{K}G : ac = 0\}$ is the left annihilator of C in $\mathbb{K}G$, and the mapping $g \mapsto \overline{g'}$, where $g' \in G$ and $\overline{g'} = g'^{-1}$, linearly extends to an anti-algebra automorphism of $\mathbb{K}G$.

By Eq. (4.8), the left annihilator of C is generated by all elements $\eta(\boldsymbol{b})$ for which $\boldsymbol{a} + \boldsymbol{b} \not\le \mathbf{1}$ for all $\boldsymbol{a} \in M'$; equivalently, $\boldsymbol{b} \not\le \mathbf{1} - \boldsymbol{a} = \bar{\boldsymbol{a}}$ for all $\boldsymbol{a} \in M'$.

■

4.5 Variants of Primitive Reed-Muller Codes with Designated Distance

The studied class of codes contains another interesting family of codes. The codes in this class have a designated minimum distance like the well-known BCH codes [42]. To see this, put $N = p^n$ and take the set $T_\delta = \{\boldsymbol{a} \in P^n : \prod_{i=1}^n (a_i + 1) \ge \delta\}$, $0 \le \delta \le N$.

4.5.1 Theorem *The linear code $C(T_\delta)$ over $\mathbb{F}_p$ has the length p^n and the minimum distance $\geq \delta$, with equality if there is an element $\boldsymbol{a} \in T_\delta$ such that $\prod_{i=1}^{n}(a_i+1) = \delta$.*

For each primitive Reed-Muller code $C(S_l)$ over $\mathbb{F}_p$ of length p^n there exists a linear code $C(T_\delta)$ of the same length and minimum distance such that

$$\dim C(S_l) \leq \dim C(T_\delta).$$

In particular, the family of binary codes $C(T_\delta)$, $0 \leq \delta \leq N$, coincides with the family of binary Reed-Muller codes.

Proof: The first assertion is clear from the proof of Theorem 4.4.2.

In view of the second assertion, take a $[p^n, k, d]$ code $C(S_l)$ over $\mathbb{F}_p$. This code has the $\mathbb{F}_p$-basis $\{\eta(\boldsymbol{a}) : \sum_{i=1}^{n} a_i \geq l\}$. Each basis element $\eta(\boldsymbol{a})$ has the Hamming weight $\prod_{i=1}^{n}(a_i + 1) \geq d$ and thus each basis element $\eta(\boldsymbol{a})$ lies in the linear code $C(T_d)$. Hence, we have $\dim C(S_l) \leq \dim C(T_d)$. Moreover, since the code is visible, at least one of the basis elements $\eta(\boldsymbol{a})$ attains the minimum distance d. It follows that the code $C(T_d)$ has minimum distance d, too.

Finally, in the binary case, the term $\prod_{i=1}^{n}(a_i + 1)$ is a power of 2, where $0 \leq a_1, \ldots, a_n \leq 1$. But we have $\prod_{i=1}^{n}(a_i + 1) = 2^l$ if and only if $\sum_{i=1}^{n} a_i = l$. It follows that the linear code $C(T_{2^l})$ coincides with the binary Reed-Muller code $C(S_l)$. More generally, the linear code $C(T_\delta)$, $2^{l-1} < \delta \leq 2^l$, equals the binary Reed-Muller code $C(S_l)$. ■

The linear code $C(T_\delta)$ is called a primitive Reed-Muller code with designed distance δ. Examples show that the designed distance may be smaller than the minimum distance of the code; e.g., the primitive ternary Reed-Muller code $C(T_7)$ of length 27 has minimum distance 8 (Table 7.2). The primitive Reed-Muller codes with designed distances are compared with the original primitive Reed-Muller codes for short lenghts over small fields in the Tables 7.1, 7.2 and 7.3. The last Theorem shows that the family of primitive Reed-Muller codes with designed distances is superior to the family of primitive Reed-Muller codes.

The primitive Reed-Muller code $C(T_{13})$ over $\mathbb{F}_7$ with designed distance $\delta = 13$ is a $[49, 24, 14]$ code. On the other hand, the subset $S_7 = \{(a_1, a_2) : a_1 + a_2 \geq 7\}$ of $\mathbb{N}_0^2$ provides the primitive Reed-Muller code $C(S_7)$ over $\mathbb{F}_7$, which is a $[49, 21, 14]$ code (Table 7.1).

Chapter 5

Linear Codes as Binomial Ideals

5.1 Introduction

Binomial ideals are ideals generated by polynomials with at most two terms. Eisenbud and Strumfels [23] in their monumental paper on binomial ideals showed that the radical, associated primes and isolated primary components of a binomial ideal are again binomial. The main advantage of studying these ideals is that their structure can be interpreted directly from their generators. Another special class of polynomial ideals are toric ideals. Toric ideals are prime ideals with a generating set of binomials. This chapter basically relates a linear code over a prime field with a binomial ideal given as a sum of a toric ideal and a non-prime ideal. Encoding procedure for a linear code has been described by constructing the Groebner basis for the corresponding ideal. Moreover, minimal generators and affine variety are also described for the binomial ideal.

5.2 Groebner Basis of the Ideal $I_{A,P}$

Recall that a binomial in a polynomial ring $\mathbb{K}[x]$ is a difference of two monomials, say $x^u - x^v$, where $u, v \in \mathbb{N}_0^n$. The special form of their generators makes it possible to tackle problems like computations of Groebner bases and primary decompositions in much easier way and helps in generating effective algorithms for better understanding of the structure. Some elementary facts about binomial

ideals are given in the following proposition.

5.2.1 Proposition *Let $\succ$ be a term order on $\mathbb{K}[x]$ and let $I \subseteq \mathbb{K}[x]$ be a binomial ideal*

- *The reduced Groebner basis G of I with respect to $\succ$ consists of binomials.*
- *The elimination ideal $I \cap \mathbb{K}[x_1, \ldots, x_r]$ is a binomial ideal for every $r \leq n$.*

Let A be a $d \times n$ matrix with non-negative entries, the toric ideal associated to A is

$$I_A = \langle x^u - x^v : Au = Av, u, v \in \mathbb{N}_0^n \rangle. \tag{5.1}$$

The zero set of I_A in affine n-space is called the affine toric variety defined by I_A [26]. If all columns of A have the same coordinate sum, then the ideal I_A is homogeneous and defines a projective toric variety. The following proposition describes the form of generators for the ℓth power of a toric ideal.

5.2.2 Proposition *Let $\mathbb{K}$ be a field and let A be a matrix in $\mathbb{Z}_{\geq 0}^{m \times n}$. The toric ideal I_A in $\mathbb{K}[x_1, \ldots, x_n]$ is generated by pure binomials,*

$$I_A = \langle x^{\alpha^+} - x^{\alpha^-} \mid A\alpha^+ = A\alpha^-, \gcd(x^{\alpha^+}, x^{\alpha^-}) = 1 \rangle. \tag{5.2}$$

Let $\ell \geq 1$ be an integer. The ℓth power of I_A is generated by elements of the form

$$\sum_{i=0}^{2^{\ell-1}-1} (-1)^i (x^{\alpha_i^+} - x^{\alpha_i^-}), \tag{5.3}$$

where $\alpha_i \in \mathbb{N}_0^n$, $0 \leq i \leq 2^{\ell-1} - 1$, $A\alpha_i^+ = A\alpha_i^-$, $0 \leq i \leq 2^{\ell-1} - 1$, and the gcd of all $x^{\alpha_i^+}$, $x^{\alpha_i^+}$ is 1.

Proof: By Proposition 1.5.2, the assertion holds for the ideal I_A. Suppose the ℓth power of I_A has a generating set given by (5.3), and let $x^\beta - x^\gamma$ be a generator of I_A, i.e., $A\beta = A\gamma$ and $\gcd(x^\beta, x^\gamma) = 1$. Then we have

$$\left(\sum_{i=0}^{2^\ell - 1} (-1)^i x^{\alpha_i} \right) \left(x^\beta - x^\gamma \right) \;=\; \sum_{i=0}^{2^\ell - 1} (-1)^i \left(x^{\alpha_i + \beta} - x^{\alpha_i + \gamma} \right),$$

where the last sum can be written as

$$\left(\sum_{i \text{ even}} \left(x^{\alpha_i+\beta} - x^{\alpha_i+\gamma}\right)\right) + \left(\sum_{i \text{ odd}} (-1)^i \left(x^{\alpha_i+\beta} - x^{\alpha_i+\gamma}\right)\right)$$
$$= \left(\sum_{i=0}^{2^{\ell-1}-1} \left(x^{\alpha_{2i}+\beta} - x^{\alpha_{2i}+\gamma}\right)\right) + \left(\sum_{i=0}^{2^{\ell-1}-1} \left(x^{\alpha_{2i+1}+\gamma} - x^{\alpha_{2i+1}+\beta}\right)\right).$$

If we put $\alpha'_{4i} = \alpha_{2i} + \beta$, $\alpha'_{4i+1} = \alpha_{2i} + \gamma$, $\alpha'_{4i+2} = \alpha_{2i+1} + \gamma$, and $\alpha'_{4i+3} = \alpha_{2i+1} + \beta$, $0 \leq i \leq 2^{\ell-1} - 1$, then we obtain the expression $\sum_{i=0}^{2^{\ell+1}-1} (-1)^i x^{\alpha'_i}$. By induction, we have $A\alpha'_{2i} = A\alpha'_{2i+1}$, $0 \leq i \leq 2^{\ell+1} - 1$. Moreover, $\gcd(x^{\alpha'_{2i}} - x^{\alpha'_{2i+1}}) = x^{\alpha_i}$, $0 \leq i \leq 2^{\ell} - 1$, and thus by induction, the gcd of all $x^{\alpha'_i}$ equals 1. ■

We associate with the toric ideal I_A in $\mathbb{K}[x]$ the binomial ideal

$$I_{A,p} = I_A + \langle x_i^p - 1 \mid 1 \leq i \leq n \rangle.$$

Note that this ideal is not toric, since it is not prime as the polynomials $x_i^p - 1$, $1 \leq i \leq n$, are reducible. In order to utilize the structure of toric ideals for the purpose of constructing linear codes we need to study them in context of finite fields. For that, we consider the saturation of an ideal I in $\mathbb{K}[x]$, given as

$$\bar{I} = \{f \in \mathbb{K}[x] \mid x_i^m \cdot f \in I \text{ for some } m \text{ and all } i\}.$$

Clearly, $\bar{I}$ is an ideal and we have $I \subseteq \bar{I}$ and $\bar{\bar{I}} = \bar{I}$. Moreover, for any ideals I and J in $\mathbb{K}[x]$, $\bar{I} + \bar{J} = \overline{I + J}$. For instance, if $I = \langle f \cdot x_1, \ldots, f \cdot x_n \rangle$, then $\bar{I} = \langle f \rangle$. The following proposition establishes an equality between a general toric ideal and the toric ideal defined over a field.

5.2.3 Proposition *Let $\mathbb{K}$ be a field, let p be a prime, and let A be a $d \times n$ matrix with non-negative integral entries. The ideal $I_{A,p}$ in $\mathbb{K}[x]$ equals the ideal*

$$J_{A,p} = \langle x^{u'} - x^{v'} \mid Au' \equiv Av' \mod p, u', v' \in \underline{p-1}^n, \gcd(x^{u'}, x^{v'}) = 1 \rangle$$
$$+ \langle x_i^p - 1 \mid 1 \leq i \leq n \rangle.$$

Proof: First, let $x^u - x^v$ be a pure binomial in $I_{A,p}$, where $u, v \in \mathbb{N}_0^n$ such that $Au = Av$. Write $u = u_1 p + u_2$ and $v = v_1 p + v_2$, where $u_1, v_1 \in \mathbb{N}_0^n$ and $u_2, v_2 \in \underline{p-1}^n$. We have

$$x^u - x^v = x^{(u_1+v_1)p}(x^{u_2} - x^{v_2}) - x^u(x^{v_1 p} - 1) + x^v(x^{u_1 p} - 1).$$

Claim that the right-hand side lies in $J_{A,p}$. Indeed, we have

$$x_i^p x_j^p - 1 = (x_i^p - 1)(x_j^p - 1) + (x_i^p - 1) + (x_j^p - 1), \quad 1 \le i, j \le n.$$

Thus for each $w \in \mathbb{N}_0^n$, $x^{wp} - 1$ lies in $\langle x_i^p - 1 \mid 1 \le i \le n \rangle$ and hence in $J_{A,p}$. Moreover, $Au = Av$ and $\gcd(x^u, x^v) = 1$ imply that $Au_2 \equiv Av_2 \mod p$ and $\gcd(x^{u_2}, x^{v_2}) = 1$. This shows that $x^u - x^v \in J_{A,p}$. The claim is proved.

Second, let $x^{u_2} - x^{v_2}$ be a pure binomial in $J_{A,p}$, where $Au_2 \equiv Av_2 \mod p$ and $u_2, v_2 \in \overline{p-1}^n$. By definition, there are $u_1, v_1 \in \mathbb{N}_0^n$ such that $u = u_1 p + u_2$, $v = v_1 p + v_2$, and $Au = Av$. Moreover, we have $\gcd(x^u, x^v) = 1$. It follows that

$$x^{(u_1+v_1)p}(x^{u_2} - x^{v_2}) = (x^u - x^v) + x^u(x^{v_1 p} - 1) - x^v(x^{u_1 p} - 1)$$

lies in $I_{A,p}$ and hence $x^{u_2} - x^{v_2}$ belongs to the saturation of $I_{A,p}$.

Thus we have proved that $I_{A,p} \subseteq J_{A,p} \subseteq \overline{I_{A,p}}$. But the binomials $x_i^p - 1$, $1 \le i \le n$, show that all variables x_i are invertible modulo $I_{A,p}$; i.e., if $x_i \cdot f \in I_{A,p}$ then $f = x_i^p \cdot f - (x_i^p - 1) \cdot f \in I_{A,p}$, $1 \le i \le n$. This is equivalent to $I_{A,p} = \overline{I_{A,p}}$. Hence the result follows. ■

5.2.4 Example Take the matrix

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

The toric ideal I_A in $\mathbb{F}_2[x]$ has the reduced Groebner basis $\{x_1x_2 + x_4, x_1x_3 + x_5, x_1x_6 + x_2x_5, x_1x_7 + x_4x_5, x_2x_3 + x_6, x_2x_5 + x_4x_5, x_2x_7 + x_4x_6, x_3x_4 + x_7, x_3x_7 + x_5x_6, x_4x_5x_6 + x_7^2\}$. On the other hand, the ideal $I_{A,2}$ in $\mathbb{F}_2[x]$ has the reduced Groebner basis $\{x_1 + x_2x_4, x_2 + x_3x_6, x_3 + x_4x_7, x_4 + x_5x_6, x_5^2 + 1, x_6^2 + 1, x_7^2 + 1\}$. ♦

Thus we get a different set of generators when we extend a toric ideal to a non-prime ideal.

An alternative way to compute a Groebner basis for the ideal $I_{A,p}$ is to consider a basis $\mathcal{B}$ of the integral lattice $\ker(A)$ in $\mathbb{Z}^n$. Consider the subideal of I_A given as

$$I_{\mathcal{B}} = \langle x^{u^+} - x^{u^-} \mid u \in \mathcal{B} \rangle.$$

As $\mathcal{B}$ is a lattice basis of $\ker(A)$,

$$I_A = I_{\mathcal{B}} : (x_1 \cdots x_n)^\infty.$$

We augment the basis $\mathcal{B}$ by vectors $p \cdot e_i$ in $\mathbb{Z}^n$, $1 \leq i \leq n$. Then we obtain

$$I_{A,p} = [I_{\mathcal{B}} + \langle x_i^p - 1 \mid 1 \leq i \leq n \rangle] : (x_1 \cdots x_n)^\infty.$$

But the binomials $x_i^p - 1$, $1 \leq i \leq n$, show that all variables x_i are invertible modulo $I_{\mathcal{B}} + \langle x_i^p - 1 \mid 1 \leq i \leq n \rangle$. Thus the ideal $I_{\mathcal{B}} + \langle x_i^p - 1 \mid 1 \leq i \leq n \rangle$ is $(x_1 \cdots x_n)^\infty$-saturated and hence

$$I_{A,p} = I_{\mathcal{B}} + \langle x_i^p - 1 \mid 1 \leq i \leq n \rangle.$$

Let B be a subset of $\mathbb{Z}^n$. Consider the ideal $I(B) = \langle x^{\beta^+} - x^{\beta^-} \mid \beta \in B \rangle$ in $\mathbb{K}[x_1, \ldots, x_n]$. If B generates the kernel of A as a $\mathbb{Z}$-module, the ideal $I(B)$ is a lattice ideal associated to the kernel of A.

Here are some familiar examples of toric varieties.

5.2.5 Example [27] Let r and s be positive integers. Define the $(r+s) \times rs$ matrix

$$\begin{aligned} A_{r,s} &= \begin{pmatrix} 1_r \otimes I_s \\ I_r \otimes 1_s \end{pmatrix} \\ &= \begin{pmatrix} 1 & \ldots & 1 & 0 & \ldots & 0 & \ldots & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 1 & \ldots & 1 & \ldots & 0 & \ldots & 0 \\ & & & & & & & & & \\ 0 & \ldots & 0 & 0 & \ldots & 0 & \ldots & 1 & \ldots & 1 \\ 1 & & 0 & 1 & & 0 & & 1 & & 0 \\ & \ddots & & & \ddots & & \ldots & & \ddots & \\ 0 & & 1 & 0 & & 1 & & 0 & & 1 \end{pmatrix}, \end{aligned}$$

where 1_r is the all-one vector of lenght r, I_r is the $r \times r$ identity matrix, and $\otimes$ denotes the Kronecker product. Let $\mathbb{K}[x]$ be the polynomial ring in the indeterminates x_{ij}, $1 \leq i \leq r$, $1 \leq j \leq s$, and let $\mathbb{K}[y,z]$ be the polynomial ring in the indeterminates $y_1, \ldots, y_r, z_1, \ldots, z_s$. The matrix $A_{r,s}$ gives rise to the $\mathbb{K}$-algebra homomorphism

$$\phi : \mathbb{K}[x] \to \mathbb{K}[y,z] : x_{ij} \mapsto y_i z_j.$$

The reduced Groebner basis for the toric ideal $I_{A_{r,c}}$ is given by the 2×2 minors of the $r \times s$ matrix of indeterminates (x_{ij}); that is,

$$G_{r,s} = \{x_{il}x_{jk} - x_{ik}x_{jl} \mid 1 \leq i < j \leq r,\ 1 \leq k < l \leq s\}.$$

Consider the projective spaces $\mathbb{P}^{r-1}$ with homogeneous coordinates $y_1, \ldots, y_r$, $\mathbb{P}^{s-1}$ with homogeneous coordinates $z_1, \ldots, z_s$, and $\mathbb{P}^{rs-1}$ with homogeneous coordinates x_{ij}, $1 \leq i \leq r$, $1 \leq j \leq s$. The morphism corresponding to the $\mathbb{K}$-algebra homomorphism is the Segre embedding given by $\phi^* : \mathbb{P}^{r-1} \times \mathbb{P}^{s-1} \to \mathbb{P}^{rs-1}$ given by $x_{ij} = y_i z_j$. ♦

5.2.6 Example [56] Let r and s be positive integers with $r \leq s$. Consider the polynomial ring $\mathbb{K}[y]$ whose indeterminates are given by an $r \times s$ matrix (y_{ij}). We associate a new variable $[i_1 i_2 \ldots i_r]$ to the $r \times r$ minor of the matrix (y_{ij}) that is given by the column indices $1 \leq i_1 < i_2 < \cdots < i_r \leq s$ and consider these $\binom{s}{r}$ brackets as the indeterminates of the polynomial ring $\mathbb{K}[x]$. The toric ideal $I_{A_{r,s}}$ is the kernel of the map

$$\phi : K[x] \to \mathbb{K}[y] : [i_1 \ldots i_r] \mapsto y_{1i_1} \cdots y_{ri_r}.$$

The associated matrix $A_{r,s}$ is an $s \times \binom{s}{r}$ matrix whose columns are all vectors of length s with r 1's and $s - r$ 0's.

The associated projective toric variety can be obtained from the (r, s) Grassmann variety by a toric deformation, where the (r, s) Grassmann variety is the projective subscheme given by the subalgebra of $\mathbb{K}[y]$ generated by the $r \times r$ minors. ♦

5.2.7 Example [27] Let r and s be positive integers with $r \leq s$. Consider the matrix $A_{r,s}$ whose columns are indexed by all non-negative integral vectors $(a_1, \ldots, a_r)$ whose entries sum up to s; this matrix has r rows and $n = \binom{r+s-1}{r-1}$ columns. For instance, we have

$$A_{2,3} = \begin{pmatrix} 3 & 2 & 1 & 0 \\ 0 & 1 & 2 & 3 \end{pmatrix}.$$

Let $\mathbb{K}[x]$ be the polynomial ring in the indeterminates $x_{a_1,\ldots,a_r}$ indexed by the columns of $A_{r,s}$. The matrix $A_{r,s}$ provides the $\mathbb{K}$-algebra homomorphism

$$\phi : \mathbb{K}[x] \to \mathbb{K}[y_1, \ldots, y_r] : x_{a_1,\ldots,a_r} \mapsto y_1^{a_1} \cdots y_r^{a_r}.$$

The morphism associated to this $\mathbb{K}$-algebra homomorphism is the rth Veronese embedding $\phi^* : \mathbb{P}^{r-1} \to \mathbb{P}^{n-1}$ given by $(x_1 : \cdots : x_r) \mapsto (f_1, \ldots, f_n)$, where $f_1, \ldots, f_n$ are the monomials in $\mathbb{K}[y_1, \ldots, y_r]$ of degree s. ♦

5.3 Ideal Bases

Let C be a linear code of length n and dimension k over $\mathbb{F}_p$. Define the ideal associated with C as

$$I_C = \langle x^u - x^v : u - v \in C \rangle + \langle x_i^p - 1 : 1 \leq i \leq n \rangle,$$

where each vector $u \in \mathbb{F}_p^n$ is considered as integral vector in the monomial x^u. For the binary case, the ideal I_C was defined in [7]. If H denotes a parity check matrix of C, then the condition $u - v \in C$ is equivalent to $Hu = Hv$. Thus by Proposition 5.2.3, we obtain

$$I_C = I_A + \langle x_i^p - 1 : 1 \leq i \leq n \rangle,$$

where A is an integral $(n-k)\times n$ matrix such that $H = A \otimes_{\mathbb{Z}} \mathbb{F}_p$. Our approach here is to construct a Groebner basis corresponding to this ideal, which is associated to the structure of a linear code. The computation of a Groebner basis for the ideal I_C has some advantages in this case. First, there is no coefficient growth since the coefficient field is $\mathbb{F}_p$. Second, the maximal degree of monomials appearing in the computation is restricted by the binomials $x_i^p - 1$, $1 \leq i \leq n$.

Each codeword $u \in C$ can be written as $u = u^+ - u^-$, where u^+ and u^- are elements of $\mathbb{F}_p^n$ that have disjoint support. Since $Hu = 0$, it follows that $Hu^+ = Hu^-$ and so the binomial $x^{u^+} - x^{u^-}$ lies in I_C. An important fact here is that the decomposition $u = u^+ - u^-$ is not unique. In fact, if $x_i^j y - Z \in I_{A,p}$ is a binomial, where $1 \leq i \leq n$ and $1 \leq j \leq p-1$, then

$$y - x_i^{p-j} Z = x_i^{p-j}(x_i^j y - Z) - y(x_i^p - 1) \in I_{A,p}.$$

We frequently switch back and forth between codewords u in C and associated binomials $x^{u^+} - x^{u^-}$ in I_C.

Each toric ideal has two special generating sets, the Graver basis and the universal Groebner basis [56, 41, 60]. Apart from some special toric ideals, these two bases rarely coincide.

5.3.1 Definition The universal Groebner basis U_C is the union of all reduced Groebner bases G for the toric ideal I_C as $\succ$ runs over all term orders. Since any ideal has only finitely many distinct initial ideals, the set U_C is a finite set of binomials.

A binomial $x^{u^+} - x^{u^-}$ in I_C is called primitive if there is no other binomial $x^{v^+} - x^{v^-}$ in I_C such that x^{v^+} divides x^{u^+} and x^{v^-} divides x^{u^-}. Primitive binomials help in identifying the minimal generators of the binomial ideal.

5.3.2 Definition The set of all primitive binomials in I_A is called the Graver basis for I_A and denoted by Gr_A.

The converse is not true. There may be primitive binomials that do not belong to U_C. Now to understand the structure of this ideal I_C, we construct its Groebner basis, Graver basis and universal basis. We will see that the results are quite similar to the case of toric ideals [56]. In general, the Graver basis provides a pretty good approximation to the universal Groebner basis.

5.3.3 Proposition *The Graver basis of the ideal I_C is given by the binomials $x_i^p - 1$, $1 \leq i \leq n$, and all pure and primitive binomials in I_A of the form $x^{u^+} - x^{u^-}$, where $u \in C$.*

Proof: Each primitive binomial in I_C is pure since all variables x_i, $1 \leq i \leq n$, are invertible modulo I_C.

Let $x^{v^+} - x^{v^-}$ be a pure binomial in I_C. Write $v^+ = v_1 p + u^+$ and $v^- = v_2 p + u^-$, where $v_1, v_2 \in \mathbb{N}_0^n$ and $u^+, u^- \in \underline{p-1}^n$. If $u^+ = zero = u^-$ then $x^{v^+} - x^{v^-}$ is divisible by some $x_i^p - 1$, $1 \leq i \leq n$. Otherwise, x^{u^+} divides x^{v^+} and x^{u^-} divides x^{v^-}. But by Proposition 5.2.3, $x^{u^+} - x^{u^-}$ lies in I_C and so $u \in C$. The result follows. ■

5.3.4 Proposition *Each binomial in the universal Groebner basis of I_C is primitive.*

5.3.5 Proposition *For every term order $\succ$, the reduced Groebner basis G of I_C consists of pure and primitive binomials of the form $x_i^p - 1$, $1 \leq i \leq n$, and $x^{u^+} - x^{u^-}$, where $u \in C$.*

Proof: Claim that G consists of pure binomials. Indeed, by Proposition 5.2.3, the ideal I_C is generated by a finite set of binomials. Apply the Buchberger algorithm to this set. In each step, the new polynomials produced are binomials, too. Thus the resulting Groebner basis consists of binomials. These binomials are pure,

since the variables x_i are invertible modulo I_C, $1 \leq i \leq n$. Claim that each binomial $x^{u^+} - x^{u^-}$ in G is primitive. Indeed, let $u^+ \succ u^-$. Then x^{u^+} is a minimal generator in the initial ideal of I_C and x^{u^-} is a standard monomial. Suppose $x^{u^+} - x^{u^-}$ is not primitive. Take a vector v in C different from u such that x^{v^+} divides x^{u^+} and x^{v^-} divides x^{u^-}. If $v^+ \succ v^-$, then x^{u^+} is not a minimal generator, a contradiction. If $v^+ \succ v^-$, then x^{v^-} is an initial monomial and so x^{u^-} is not standard, a contradiction. The result now follows from Proposition 5.3.3. ■

A non-zero vector u in C is called a circuit if it has minimum Hamming weight and the coordinates of u are relatively prime. Equivalently, a binomial $x^{u^+} - x^{u^-}$ in I_C is a circuit if it is irreducible and has minimal support with respect to inclusion. Each circuit in C has Hamming weight $\leq n - k + 1$ by the Singleton bound.

5.3.6 Proposition *All circuits in C lie in the universal Groebner basis of I_C.*

Proof: Let u be a circuit in C. Fix an elimination term order $\succ$ such that all variables x_i, where $u_i = 0$, are larger than the variables x_j, where $u_j \neq 0$, and write $u = u^+ - u^-$ such that $u^+ \succ u^-$. Claim that $x^{u^+} - x^{u^-}$ appears in the reduced Groebner basis G of I_C. Indeed, let v be a non-zero vector in C such that $v^+ \succ v^-$ and x^{v^+} divides x^{u^+}. Then $\mathrm{supp}(v^+) \subset \mathrm{supp}(u)$ and by the choice of the term order, $\mathrm{supp}(v^-) \subset \mathrm{supp}(u)$. Hence $\mathrm{supp}(v) \subset \mathrm{supp}(u)$. Since u is a circuit, it follows that v must be a multiple of u. But x^{v^+} divides x^{u^+} and so $u = v$. ■

Let $x^{u^+} - x^{u^-}$ and $x^{v^+} - x^{v^-}$ be binomials in I_C. We say that u is conformal to v if $\mathrm{supp}(u^+) \subset \mathrm{supp}(v^+)$ and $\mathrm{supp}(u^-) \subset \mathrm{supp}(v^-)$.

5.3.7 Proposition *Each codeword v in C can be written as a linear combination of circuits each of which conformal to v.*

Proof: Let v be a codeword in C. If v is a circuit, then we are done. If not, we can assume that the coordinates of v are relatively prime and that there is a circuit u in C such that $\mathrm{supp}(u) \subset \mathrm{supp}(v)$. We may write u and v as binomials $x^{u^+} - x^{u^-}$ and $x^{v^+} - x^{v^-}$ such that u is conformal to v. Among all non-zero coordinate ratios v_i/u_i let λ denote the minimum. Then $v - \lambda u$ is conformal to v and has zero ith coordinate for some $1 \leq i \leq n$. By induction, the vector $v - \lambda u$ can be written as a linear combination of circuits each of which conformal to v. Now the identity $v = \lambda u + (v - \lambda u)$ provides the assertion. ■

5.3.8 Theorem *In the binary case, the set of circuits in C equals the Graver basis for C.*

Proof: Let $x^{v^+} - x^{v^-}$ be an element in the Graver basis of I_C. By Proposition 5.3.7, there is a circuit $x^{u^+} - x^{u^-}$ in I_C such that $\mathrm{supp}(u^+) \subseteq \mathrm{supp}(v^+)$ and $\mathrm{supp}(u^-) \subseteq \mathrm{supp}(v^-)$. Since the monomials are square-free it follows that x^{u^+} divides x^{v^+} and x^{u^-} divides x^{v^-}. But v is primitive and so $v = u$. The reverse inclusion follows from Propositions 5.3.4 and 5.3.6. ∎

Next we demonstrate how the Graver basis and the Groebner basis can be computed for the ideal associated to a given matrix. Let A be a $d \times n$ matrix with non-negative entries, The Graver basis for the toric ideal I_A can be computed by Groebner basis techniques. For this, consider the enlarged matrix

$$\Gamma(A) = \begin{pmatrix} A & I \\ I & 0 \end{pmatrix},$$

where I is the $n \times n$ identity matrix and 0 is the $d \times n$ zero matrix. The $(d+n) \times 2n$ matrix $\Gamma(A)$ is called the Lawrence lifting of A. The matrices A and $\Gamma(A)$ have isomorpic kernels, $\ker(\Gamma(A)) = \{(u, -u) : u \in \ker A\}$. The toric ideal $I_{\Gamma(A)}$ is the homogeneous prime ideal

$$I_{\Gamma(A)} = \langle x^{u^+} y^{u^-} - x^{u^-} y^{u^+} : uA = 0 \rangle$$

in the polynomial ring $\mathbb{K}[x, y] = \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_n]$. The Graver basis for A can be computed in two steps. First, choose any term order on $\mathbb{K}[x, y]$ and compute the reduced Groebner basis G for $I_{\Gamma(A)}$. Second, substitute $y_1 \to 1, \ldots, y_n \to 1$ in G. The resulting subset of $\mathbb{K}[x]$ is the Graver basis for I_A.

5.3.9 Example Let $k \geq 2$ be an integer. Take the projective space $\mathbb{P}^{k-1}$ of dimension $k-1$ over the finite field $\mathbb{F}_q$. This space consists of $n = \frac{q^n-1}{q-1}$ points. Let H_k be the $k \times n$ matrix, whose columns are given by the points of

$\mathbb{P}^{k-1}$. The q-nary linear code given by the parity check matrix H_k is an $[n, n-k, 3]$ code and is called Hamming code over $\mathbb{F}_q$.

In particular, the $[7, 4]$ Hamming code has the parity check matrix

$$H_{3,7} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

A reduced Groebner basis of the binary code $I_{H_{3,7}}$ is given by

$$G = \{x_1 + x_2x_4, x_2 + x_3x_6, x_3 + x_4x_7, x_4 + x_5x_6, x_5^2 + 1, x_6^2 + 1, x_7^2 + 1\}.$$

♦

5.3.10 Example Let H_d be the vertex-edge incidence matrix of the complete graph K_d. This is a binary $d \times \binom{d}{2}$ matrix with column sums 2 and row sums $d-1$. The corresponding toric ideal is the kernel of the map

$$\phi : \mathbb{K}[\{x_{ij} \mid 1 \leq i < j \leq d\}] \to \mathbb{K}[y_1, \ldots, y_d] : x_{ij} \mapsto y_i y_j.$$

The variables x_{ij} are indexed by the edges in the complete graph K_d.

The circuits form a universal Groebner basis of I_{H_d} for $d \leq 7$; the statement is not true for $d \geq 8$ [56].

The binary code given by the parity check matrix H_d has length $n = \binom{d}{2}$ and dimension $k = \binom{d}{2} - d = d(d-3)/2$. The minimum distance is $d = 3$, since any two columns of the matrix H_d are linearly independent and there exist three linearly dependent columns. ♦

5.3.11 Example [56] Let $A_{r,s}$ be the $s \times \binom{s}{r}$ matrix arising in the toric deformation of the (r,s) Grassmann variety. The binary code with $A_{r,s}$ as parity check matrix has length $n = \binom{s}{r}$ and dimension $k = \binom{s}{r} - s$. The minimum distance is $d \leq 4$, since any three columns of the matrix H_d are linearly independent and there exist four linearly dependent columns.

In particular, the toric ideal $I_{A_{2,s}}$ has the property that the set of circuits equals the universal Groebner basis [56]

$$G = \{[i_1j_1[i_2j_2]\cdots[i_vj_v] - [i_2j_1[i_3j_2]\cdots[i_1j_v] \mid i_1, i_2 < j_1, i_2, i_3 < j_2, \ldots, i_vi_1 < j_v\}.$$

♦

There are plenty of toric varieties [26, 34] arising naturally in combinatorics and geometry. Each of the underlying configurations A gives rise to a project to examine its toric ideal I_A, especially its Groebner bases and the associated code.

5.4 Reduced Groebner Basis of I_C

Next, we provide a reduced Groebner basis to each binomial ideal associated with a linear code. The corresponding term order is rather general and only requires that any monomial containing one of the information symbols is larger than any monomial containing only parity check symbols. Moreover, it will be shown that Groebner bases for linear codes provide a very compact representation of the encoding function. The following result shows that for any term ordering the reduced Groebner basis for an ideal corresponding to a code can be constructed directly from its generator matrix.

Reconsider the ideal associated with C as

$$I_C = \langle x^c - x^{c'} : c - c' \in C \rangle + \langle x_i^p - 1 \mid 1 \leq i \leq n \rangle, \tag{5.4}$$

where each element $c \in \mathbb{F}_p^n$ is considered as an integral vector in the monomial x^c [7, 49].

In the following, let C be an $[n, k]$ code over $\mathbb{F}_p$ given in standard form with generator matrix $G = (I_k, A)$. Let a_i denote the ith row of the matrix $-A$ over F_p, $1 \leq i \leq k$.

5.4.1 Theorem *Given a term order such that $x_1 \succ \ldots \succ x_n$ in $\mathbb{K}[x]$. The binomial ideal I_C has the reduced Groebner basis*

$$G = \{x_i - x^{a_i} \mid 1 \leq i \leq k\} \cup \{x_i^p - 1 \mid k+1 \leq i \leq n\}. \tag{5.5}$$

Proof: By definition, the elements of G lie in the ideal I_C. Conversely, let $x^c - x^d$ be an element of I_C with $c - d \in C$. The reduction of $x^c - x^d$ w.r.t G results into another binomial $x^l - x^m$, where $l = c_1 a_1 + \ldots + c_k a_k + c'$, $m = d_1 a_1 + \ldots + d_k a_k + d'$, $c' = (0, \ldots, 0, c_{k+1}, \ldots, c_n)$ and $d' = (0, \ldots, 0, d_{k+1}, \ldots, d_n)$. In each step of the reduction, the resulting binomial $x^{c'} - x^{d'}$ satisfies $c' - d' \in C$. Note that the vectors l and m both have zeros at the positions 1 to k and so $lH^T = mH^T$ implies that $l = m$. Thus the binomial $x^c - x^d$ is reduced by G to 0.

Furthermore, the binomial $x_i^p - 1$, $1 \leq i \leq k$, is reduced by G to $x^{pa_i} - 1$ and this binomial in turn is reduced by G to 0. It follows that G is a generating set of the ideal I_C. Consider the S-polynomials of the elements in G. First, let $1 \leq i < j \leq k$.

We have $S(x_i - x^{a_i}, x_j - x^{a_j}) = x_i x^{a_j} - x_j x^{a_i}$. Division into G yields

$$\begin{aligned}
&\mathrm{rem}(x_i x^{a_j} - x_j x^{a_i}, G) = \\
&= \mathrm{rem}(x_i x^{a_j} - x_j x^{a_i} - x^{a_j}(x_i - x^{a_i}), G) \\
&= \mathrm{rem}(-x_j x^{a_i} + x^{a_j} x^{a_i}), G) \\
&= \mathrm{rem}(-x_j x^{a_i} + x^{a_j} x^{a_i} - (-x^{a_i})(x_j - x^{a_j}), G) \\
&= \mathrm{rem}(x^{a_j} x^{a_i} - x^{a_i} x^{a_j}, G) = 0.
\end{aligned}$$

Second, let $k+1 \leq i < j \leq n$. We have $S(x_i^p - 1, x_j^p - 1) = x_i^p - x_j^p = (x_i^p - 1) - (x_j^p - 1)$ and thus the S-polynomial reduces to zero. Third, let $1 \leq i \leq k$ and $k+1 \leq j \leq n$. We have $S(x_i - x^{a_i}, x_j^p - 1) = x_i - x_j^p x^{a_i}$. Division into G provides

$$\begin{aligned}
\mathrm{rem}(x_i - x_j^p x^{a_i}, G) &= \mathrm{rem}(x_i - x_j^p x^{a_i} - (x_i - x^{a_i}), G) \\
&= \mathrm{rem}(-x_j^p x^{a_i} + x^{a_i}, G) \\
&= \mathrm{rem}(-x_j^p x^{a_i} + x^{a_i} - (-x^{a_i})(x_j^p - 1), G) = 0.
\end{aligned}$$

It follows that the set G is a Groebner basis for I_C. Finally, it is clear that the Groebner basis G is reduced. ■

The above theorem illustrates the fact that the reduced Groebner basis for the ideal I_C can be read directly from its generating matrix.

5.4.1 Application to Golay Codes

The Golay codes belong to the most prominent linear error-correcting codes [58]. The Golay codes are perfect and unique and have several other properties [42, 58]. Amazingly, Golay's original paper was barely a half-page long [28].

There are two versions, binary Golay code G_{23} and the ternary Golay .

5.4.2 Example The binary Golay code is a $[23, 12, 7]$ code C_{23} with generator

matrix $G_{23} = (I_{12}, M)$, where

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

By Theorem 5.4.1, a reduced Groebner basis for the ideal $I_{C_{23}}$ in $\mathbb{Q}[x_1, \ldots, x_{23}]$ w.r.t. the lexicographic order $\succ$ with $x_1 \succ \cdots \succ x_{23}$ is given by the elements

$$\begin{aligned} &x_1 - x_{13}x_{14}x_{15}x_{16}x_{17}x_{18}x_{19}x_{20}x_{21}x_{22}, && x_7 - x_{15}x_{16}x_{17}x_{18}x_{21}x_{23}, \\ &x_2 - x_{17}x_{18}x_{19}x_{20}x_{21}x_{22}x_{23}, && x_8 - x_{14}x_{16}x_{18}x_{19}x_{20}x_{23}, \\ &x_3 - x_{14}x_{15}x_{16}x_{20}x_{21}x_{22}x_{23}, && x_9 - x_{14}x_{15}x_{17}x_{19}x_{22}x_{23}, \\ &x_4 - x_{13}x_{15}x_{16}x_{18}x_{19}x_{22}x_{23}, && x_{10} - x_{13}x_{16}x_{17}x_{20}x_{22}x_{23}, \\ &x_5 - x_{13}x_{14}x_{16}x_{17}x_{19}x_{21}x_{23}, && x_{11} - x_{13}x_{15}x_{19}x_{20}x_{21}x_{23}, \\ &x_6 - x_{13}x_{14}x_{15}x_{17}x_{18}x_{20}x_{23}, && x_{12} - x_{13}x_{14}x_{18}x_{21}x_{22}x_{23}, \end{aligned}$$

and $x_{13}^2 - 1, \ldots, x_{23}^2 - 1$. ♦

5.4.3 Example The ternary Golay code is an $[11, 6, 5]$ code C_{11} with generator matrix $G_{11} = (I_6, M)$, where

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 & 1 \\ 1 & 0 & 1 & 2 & 2 \\ 2 & 1 & 0 & 1 & 2 \\ 2 & 2 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \end{pmatrix}.$$

Using the above theorem, the reduced Groebner basis corresponding to these generator matrices are: The Golay code C_{11} has the Groebner basis G_{11} over the

polynomial ring $\mathbb{Q}[x_1, \ldots, x_{11}]$,

$$\begin{array}{ll} x_7^3 - 1, & x_1 - x_7^2 x_8^2 x_9^2 x_{10}^2 x_{11}^2, \\ x_8^3 - 1, & x_2 - x_8^2 x_9 x_{10} x_{11}^2, \\ x_9^3 - 1, & x_3 - x_7^2 x_9^2 x_{10} x_{11}, \\ x_{10}^3 - 1, & x_4 - x_7 x_8^2 x_{10}^2 x_{11}, \\ x_{11}^3 - 1, & x_5 - x_7 x_8 x_9^2 x_{11}^2, \\ & x_6 - x_7^2 x_8 x_9 x_{10}^2. \end{array}$$

♦

5.5 Decomposition of the Ideal I_C

Decomposition of any ideal into smaller ideals has several benefits, for example, given generators of pair of ideals one can compute the generators of their sum. We describe the reduced Groebner bases of the ideals which decompose I_C. Let C be an $[n, k]$ code over $\mathbb{F}_p$ given in standard form with generator matrix $G = (I_k, M)$. Take the lexicographic order $\succ$ on $\mathbb{K}[X]$ such that $x_1 \succ \ldots \succ x_n$. In view of [52], the binomial ideal I_C has the reduced Groebner basis $G = \{g_1, \ldots, g_n\}$ with respect to $\succ$ given by

$$g_i = \begin{cases} x^{r_i} - 1, & 1 \le i \le k, \\ x_i^p - 1, & k+1 \le i \le n, \end{cases} \tag{5.6}$$

where r_i denotes ith row vector of G, $1 \le i \le k$.

Write e_i for the ith unit vector of length n (that is, e_i is the vector with a 1 in the ith component and 0's elsewhere), $1 \le i \le n$. Then we have $r_i = e_i + (0, s_i)$, where s_i is the vector of the last $n - k$ components of r_i, $1 \le i \le k$. Put $m_i = -s_i$ over $\mathbb{F}_p$, $1 \le i \le n$. Then, we have

$$x^{r_i} - 1 = x_i - x^{(0,m_i)}, \quad 1 \le i \le k. \tag{5.7}$$

It follows from (5.5) and (5.7) that the corresponding ideal of leading terms is

$$\mathrm{lt}(I_C) = \langle x_1, \ldots, x_k, x_{k+1}^p, \ldots, x_n^p \rangle. \tag{5.8}$$

5.5.1 Proposition *Let $\succ$ be the lexicographic order on $\mathbb{K}[x]$ with $x_1 \succ \ldots \succ x_n$. The ideal I_C decomposes into the sum*

$$I_C = I_T + I_p, \tag{5.9}$$

where the ideal $I_T = \langle x_i - x^{(0,m_i)} \mid 1 \leq i \leq k \rangle$ *is toric and has the reduced Groebner basis* $G_T = \{x_i - x^{(0,m_i)} \mid 1 \leq i \leq k\}$*, and the ideal* $I_p = \langle x_i^p - 1 \mid k+1 \leq i \leq n \rangle$ *has the reduced Groebner basis* $G_p = \{x_i^p - 1 \mid k+1 \leq i \leq n\}$.

Proof: We prove the assertion in several steps. First, by the Groebner basis (5.5) for I_C, the ideal I_C can written as the sum $I_T + I_p$.

Second, the parity check matrix $H = (-M^T, I_{n-k})$ for I_C contains $m_1, \ldots, m_k$ (as column vectors) in its the first k columns. Consider the matrix H as a non-negative integral $(n-k) \times n$ matrix and denote this matrix by A. The latter matrix defines a toric ideal I_A in $\mathbb{K}[x]$.

We try to show that $I_T = I_A$. Infact, we have $x_i - x^{(0,m_i)} = x^{e_i} - x^{(0,m_i)}$ in I_T, $1 \leq i \leq k$. But we have

$$Ae_i = m_i = A \begin{pmatrix} 0 \\ m_i \end{pmatrix}, \quad 1 \leq i \leq k,$$

and so by definition, the ideal I_T is contained in I_A.

Conversely, let $x^u - x^v$ be a binomial in I_A. Successive reduction via G_T leads to the binomial $x^{u_1 \cdot \boldsymbol{m}_1 + \ldots + u_k \cdot \boldsymbol{m}_1 + \boldsymbol{u}_{n-k}} - x^{v_1 \cdot \boldsymbol{m}_1 + \ldots + v_k \cdot \boldsymbol{m}_k + \boldsymbol{v}_{n-k}}$, where u_{n-k} and v_{n-k} are the vectors containing the last $n-k$ coordinates of u and v, respectively. The variables $x_1, \ldots, x_k$ are not involved in this binomial. But if $x^a - x^b$ is a binomial in I_A such that the variables $x_1, \ldots, x_k$ are not involved, then $Aa = Ab$ implies $a = b$. Thus the reduction leads to 0 and hence the binomial ideal I_A lies I_T. This proves the claim.

Let $x^u - x^v$ be a binomial in I_T. If one of the variables $x_1, \ldots, x_k$ is involved, then the binomial is divisible by G_T. Otherwise, the above argument shows that the binomial is 0. It follows that G_T is a Groebner basis for the ideal I_T.

Third, by the Elimination theorem [18], the set $G_p = G \cap \mathbb{K}[x_{k+1}, \ldots, x_n]$ is a Groebner basis for the kth elimination ideal of I_C given by $I_k = I_C \cap \mathbb{K}[x_{k+1}, \ldots, x_n]$. By definition, we have $I_p = I_k$.

Finally, both Groebner bases are reduced. This completes the proof. ∎

5.6 Affine Varieties

We fix an algebraically closed field $\mathbb{K}$. The affine n-space over $\mathbb{K}$ is denoted by $\mathbb{K}^n$ which is simply the set of n-tuples of elements of $\mathbb{K}$. Let $f_1, \ldots, f_n$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. The set

$$\mathcal{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) : f_i(a_1, \ldots, , a_n) = 0, \text{for every } 1 \leq i \leq s\} \quad (5.10)$$

is called the affine variety defined by $f_1, \ldots, f_s$. For example, the variety of $f = x^2 + y^2 - 1 = 0$ is the circle centered at origin with radius 1. For ideals I and J, the affine varieties have the following properties :

- $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cap J)$, finite union
- $\bigcap_\alpha \mathcal{V}(J_\alpha) = \mathcal{V}(\sum_\alpha J_\alpha)$, arbitrary intersection.
- If $1 \in I$, then $\mathcal{V}(I) = \phi$.
- $\mathcal{V}(0) = \mathbb{K}^n$.

These properties show that affine varieties form the closed set topology on $\mathbb{K}^n$, called the Zariski topology. For any subset $V \subseteq \mathbb{K}^n$, by defining the inverse operation of taking common zeros of locus of polynomials, we define the ideal

$$\mathcal{I}(V) = \{f : f(a_1, \ldots, a_n) = 0, \text{for every } (a_1, \ldots, a_n) \in V\}. \quad (5.11)$$

It is easy to see from the definition that for any ideal I, we have $I \subset \mathcal{I}(\mathcal{V}(I))$. There is a one-to-one correspondence between the radical ideals and varieties. The following theorem makes this fact clear.

5.6.1 Theorem *[The Strong Nullstellensatz] Let* $\mathbb{K}$ *be an algebraically closed field. If* I *is an ideal in* $\mathbb{K}[x_1, \ldots, x_n]$*, then*

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}. \quad (5.12)$$

We study the affine variety $\mathcal{V}(I_C)$ of the ideal associated to an $[n, k]$ code C over $\mathbb{F}_p$. For this, we consider the $\mathbb{K}$-algebra $A = \mathbb{K}[x]/I_C$. It has a $\mathbb{K}$-basis given by the cosets of the standard monomials of I_C [19].

5.6.2 Proposition *Let* $\mathbb{K}$ *be an algebraically closed field of characteristic 0 and let* C *be an* $[n,k]$ *code over* $\mathbb{F}_p$.

- *The algebra* A *has the dimension* p^{n-k} *over* $\mathbb{K}$.
- *The affine variety* $V = \mathcal{V}(I_C)$ *has* p^{n-k} *points in* $\mathbb{K}^n$ *and is smooth at each point.*
- *The ideal* I_C *is radical.*

Proof:

- In terms of the ideal of leading terms of I_C given in (5.8), the standard monomials of I_C are $x_{k+1}^{\alpha_1} \cdots x_n^{\alpha_{n-k}}$, $\alpha_1, \ldots, \alpha_{n-k} \in \{0, \ldots, p-1\}$. Their cosets form a $\mathbb{K}$-basis of A [19].
- By the Groebner basis of I_C given in (5.5), each point $(a_1, \ldots, a_n)$ in V has to satisfy the equations

  $$a_i^p = 1, \quad k+1 \leq i \leq n,$$

  and

  $$a_i = a_{k+1}^{m_{i,1}} \cdots a_n^{m_{i,n-k}}, \quad 1 \leq i \leq k,$$

  where $\boldsymbol{m}_i = (m_{i,1}, \ldots, m_{i,n-k})^T$, $1 \leq i \leq k$. Thus the variety V has p^{n-k} points in $\mathbb{K}^n$.

  The "Jacobi matrix" $J = \left(\frac{\partial g_i}{\partial x_j}(P)\right)$ at each point P of V has rank n and thus by the affine Jacobi criterion [18], the variety V is smooth at P.
- It is well-known that the dimension of A equals the number of points in V if and only if the underlying ideal I_C is radical [19]. Thus by the first two assertions, I_C is a radical ideal.

■

The last assertion and Hilbert's Strong Nullstellensatz imply that

$$\mathcal{I}(\mathcal{V}(I_C)) = \sqrt{I_C} = I_C.$$

It follows that the coordinate ring $\mathbb{K}[V] = \mathbb{K}[x]/\mathcal{I}(V)$ of the affine variety $V = \mathcal{V}(I_C)$ equals the $\mathbb{K}$-algebra A.

5.7 Encoding

The extra structure of the linear code C given by a reduced Groebner basis for the ideal I_C provides a compact encoding function. An immediate consequence of Theorem 5.4.1 is a systematic encoding algorithm for linear codes using division with respect to a Groebner basis. Note that this procedure is a variant of the encoding method for multi-dimensional cyclic codes in which the codewords are represented as polynomials in a residue class ring [19]. By Theorem 5.4.1, the binomial ideal I_C has the associated initial ideal

$$\mathrm{in}(I_C) = \langle x_1, \ldots, x_k, x_{k+1}^p, \ldots, x_n^p \rangle. \tag{5.13}$$

5.7.1 Proposition *Let C be an $[n,k]$ code over $\mathbb{F}_p$, and let G be the reduced Groebner basis for C given in (5.5).*

- *The information positions are given by the nonstandard monomials for I_C in which each x_i appears to a power of at most $p-1$, $1 \leq i \leq k$.*
- *The parity check positions are provided by the standard monomials for I_C in which each x_i appears to a power of at most $p-1$, $k+1 \leq i \leq n$.*
- *The following algorithm gives a systematic encoder E for the code C: Take an information word $w \in \mathbb{F}_p^k$ and put $x^w = x_1^{w_1} \cdots x_k^{w_k}$. Divide x^w into G and form $E(w) = (x^w - 1) - \mathrm{rem}(x^w - 1, G)$. This gives the corresponding codeword in C.*

Proof: The first two assertions are clear from the initial ideal of I_C. Finally, let $w \in \mathbb{F}_p^k$ be an information word. The division of $x^w - 1$ into the Groebner basis G gives

$$\begin{aligned} \mathrm{rem}(x^w - 1, G) &= \mathrm{rem}(x^{w_1 a_1 + \ldots + w_k a_k} - 1, G) \\ &= x^{w_1 a_1 + \ldots + w_k a_k} - 1, \end{aligned}$$

where the exponent in the last binomial $x^{w_1 a_1 + \ldots + w_k a_k} - 1$ is computed over $\mathbb{F}_p$. It follows that the remainder only involves parity check positions so that the information position are not changed in the process of computing the remainder. The encoded binomial

$$E(w) = (x^w - 1) - \mathrm{rem}(x^w - 1, G) = x^w - x^{w_1 a_1 + \ldots + w_k a_k}$$

is an element of the ideal I_C and represents the codeword wG. Thus the reduction of w by the basis G mimicks the representation of w by a codeword in C. As a result, E is a systematic encoding function for C. ■

We conclude this chapter by remarking that the study of a linear code C by using the corresponding binomial ideal I_C provides an extra structure that allows a very compact representation of the encoding function. We only need to know a reduced Groebner basis for the ideal I_C.

Chapter 6

Syzygies

6.1 Introduction

This chapter presents the binomial ideal of the linear code in terms of its syzygy module. Groebner basis for the first syzygy module of the binomial ideal is constructed, which is then used to compute the corresponding finite free resolution.

6.2 Syzygies and Free Resolutions of Linear Codes

It is a well known fact that most modules over a ring do not have bases, infact their generators usually satisfy some nontrivial relations called syzygies [61]. Recall that the set $\{\boldsymbol{s}_{ij} \mid 1 \leq i, j \leq t\}$ forms a Groebner basis for the syzygy module $M = \mathrm{Syz}(g_1, \ldots, g_t)$ with respect to the monomial order $\succ$ on R^t, where

$$\boldsymbol{s}_{ij} = \boldsymbol{h}_{ij} - \frac{\boldsymbol{m}_{ij}}{\mathrm{lt}(\boldsymbol{g}_i)}\boldsymbol{e}_i + \frac{\boldsymbol{m}_{ij}}{\mathrm{lt}(\boldsymbol{g}_j)}\boldsymbol{e}_j = \begin{pmatrix} h_{ij1} \\ \vdots \\ h_{iji} - a_i \\ \vdots \\ h_{ijj} + a_j \\ \vdots \\ h_{ijt} \end{pmatrix} \in R^t, \tag{6.1}$$

for each pair (i, j), $1 \leq i, j \leq t$, such that $\boldsymbol{m}_{ij} \neq \boldsymbol{0}$.

This section provides a presentation of the binomial ideal of a linear code in terms of its syzygy modules and gives a corresponding finite free resolution.

As before, let C be an $[n,k]$ code over $\mathbb{F}_p$ given in standard form with generator matrix $G = (I_k, M)$. Let m_i denote the ith row of the matrix $-M$, $1 \le i \le k$. By Theorem 5.4.1, given any monomial order $\succ$ on $\mathbb{K}[x]$ such that $x_1 \succ \ldots \succ x_n$, the binomial ideal I_C has the reduced Groebner basis $G = \{g_1, \ldots, g_n\}$. The following theorem gives the formulation of the Groebner basis for the first syzygy module.

6.2.1 Theorem *Let $G = \{g_1, \ldots, g_n\}$ be the Groebner basis for the ideal I_C given in (5.5). Put*

$$\boldsymbol{s}_{ij} = g_j \boldsymbol{e}_i - g_i \boldsymbol{e}_j \in R^n, \quad 1 \le i < j \le n.$$

The collection $\{\boldsymbol{s}_{ij} \mid 1 \le i < j \le n\}$ forms a Groebner basis for the first syzygy module $\mathrm{Syz}(g_1, \ldots, g_n)$ *of I_C.*

Proof: First, let $1 \le i < j \le k$. We have

$$\begin{aligned} S(x_i - x^{\boldsymbol{m}_i}, x_j - x^{\boldsymbol{m}_j}) &= x_j(x_i - x^{\boldsymbol{m}_i}) - x_i(x_j - x^{\boldsymbol{m}_j}) \\ &= x_i x^{\boldsymbol{m}_j} - x_j x^{\boldsymbol{m}_i} \\ &= x^{\boldsymbol{m}_j}(x_i - x^{\boldsymbol{m}_i}) + (-x^{\boldsymbol{m}_i}) \cdot (x_j - x^{\boldsymbol{m}_j}) \end{aligned}$$

and therefore by (6.1),

$$\boldsymbol{s}_{ij} = (x_j - x^{\boldsymbol{m}_j})\boldsymbol{e}_i - (x_i - x^{\boldsymbol{m}_i})\boldsymbol{e}_j.$$

Second, let $1 \le i \le k$ and $k+1 \le j \le n$. We have

$$\begin{aligned} S(x_i - x^{\boldsymbol{m}_i}, x_j^p - 1) &= x_j^p(x_i - x^{\boldsymbol{m}_i}) - x_i(x_j^p - 1) \\ &= x_i - x^{\boldsymbol{m}_i} x_j^p \\ &= (x_i - x^{\boldsymbol{m}_i}) + (-x^{\boldsymbol{m}_i}) \cdot (x_j^p - 1) \end{aligned}$$

and so by (6.1),

$$\boldsymbol{s}_{ij} = (1 - x_j^p)\boldsymbol{e}_i + (-x^{\boldsymbol{m}_i} + x_i)\boldsymbol{e}_j.$$

Third, let $k+1 \le i < j \le n$. We have

$$\begin{aligned} S(x_i^p - 1, x_j^p - 1) &= x_j^p(x_i^p - 1) - x_i^p(x_j^p - 1) \\ &= (x_i^p - 1) + (-1) \cdot (x_j^p - 1) \end{aligned}$$

and thus by (6.1),

$$\boldsymbol{s}_{ij} = (1 - x_j^p)\boldsymbol{e}_i + (-1 + x_i^p)\boldsymbol{e}_j.$$

The result now follows from Schreyer's theorem [1, 53]. ■

In the following, the standard basis of the free R-module $R^{\binom{n}{m}}$ is indexed by the set of m-element subsets of $\{1, \ldots, n\}$,

$$B_m = \{\boldsymbol{e}_{i_1 \ldots i_m} \mid 1 \leq i_1 < i_2 < \ldots < i_m \leq n\}, \quad 0 \leq m \leq n. \tag{6.2}$$

6.2.2 Theorem *Let $G = \{g_1, \ldots, g_n\}$ be the Groebner basis for the ideal I_C given in (5.5). The ideal I_C has a finite free resolution of length n,*

$$0 \xrightarrow{\phi_n} R^{t_{n-1}} \xrightarrow{\phi_{n-1}} \cdots \xrightarrow{\phi_2} R^{t_1} \xrightarrow{\phi_1} R^{t_0} \xrightarrow{\phi_0} R \to 0, \tag{6.3}$$

where $I_C = \mathrm{im}\,(\phi_0)$ and $t_m = \binom{n}{m+1}$, $0 \leq m \leq n-1$.

The mapping $\phi_m : R^{\binom{n}{m+1}} \to R^{\binom{n}{m}}$ in the resolution is defined as

$$\phi_m(\boldsymbol{e}_{i_1 \ldots i_{m+1}}) = \sum_{j=1}^{m+1} (-1)^{j-1} g_{i_j} \boldsymbol{e}_{i_1 \ldots i_{j-1} i_{j+1} \ldots i_{m+1}}. \tag{6.4}$$

The m-th syzygy module of I_C is an R-submodule of $R^{\binom{n}{m+1}}$, $0 \leq m \leq n-1$, and has the Groebner basis

$$\{\boldsymbol{s}_{i_1 \ldots i_{m+1}} \mid 1 \leq i_1 < i_2 < \ldots < i_{m+1} \leq n\}, \tag{6.5}$$

where

$$\boldsymbol{s}_{i_1 \ldots i_{m+1}} = \sum_{j=1}^{m+1} (-1)^{j-1} g_{i_j} \boldsymbol{e}_{i_1 \ldots i_{j-1} i_{j+1} \ldots i_{m+1}}. \tag{6.6}$$

Note that in last two formulae, in the term with index j, i_j is omitted to yield an m-element subset.

Proof: We use induction on m. The base case is already given by Theorem 6.2.1. Let m be an integer with $2 \leq m \leq n$ and suppose the result already holds for the $m-1$-th syzygy module.

Claim that the composition $\phi_{m-1} \circ \phi_m$ is the zero map. Indeed, this is essentially due to the sign in the definition of the homomorphisms. More concretely, for each

basis vector $\boldsymbol{e}_{i_1\dots i_{m+1}}$ we have

$$\begin{aligned}(\phi_{m-1}\circ\phi_m)(\boldsymbol{e}_{i_1\dots i_{m+1}}) &= \sum_{j=1}^{m+1}(-1)^{j-1}g_{i_j}\phi_{m-1}(\boldsymbol{e}_{i_1\dots i_{j-1}i_{j+1}\dots i_{m+1}}) \\ &= \sum_{j=1}^{m+1}\sum_{k=1}^{j-1}(-1)^{j+k}g_{i_j}g_{i_k}\boldsymbol{e}_{i_1\dots i_{k-1}i_{k+1}\dots i_{j-1}i_{j+1}\dots i_{m+1}} \\ &\quad+\sum_{j=1}^{m+1}\sum_{k=j+1}^{m+1}(-1)^{j+k-1}g_{i_j}g_{i_k}\boldsymbol{e}_{i_1\dots i_{j-1}i_{j+1}\dots i_{k-1}i_{k+1}\dots i_{m+1}}.\end{aligned} \tag{6.7}$$

In the expansion of this sum according to the standard basis, each standard basis vector $\boldsymbol{e}_{i_1\dots i_{k-1}i_{k+1}\dots i_{j-1}i_{j+1}\dots i_{m+1}}$ has the coefficient $g_{i_j}g_{j_k}-g_{i_j}g_{j_k}=0$ and thus the whole sum becomes $\mathbf{0}$. Hence, $\operatorname{im}(\phi_m)\subseteq\ker(\phi_{m-1})$.

In the following, we need a statement about syzygy relations that is essentially due to the sign in the definition of the syzygies. By induction hypothesis, we have

$$\begin{aligned}&\sum_{j=1}^{m+1}(-1)^{j-1}g_{i_j}\boldsymbol{s}_{i_1\dots i_{j-1}i_{j+1}\dots i_{m+1}} = \\ &= \sum_{j=1}^{m+1}\sum_{k=1}^{j-1}(-1)^{j+k}g_{i_j}g_{i_k}\boldsymbol{e}_{i_1\dots i_{k-1}i_{k+1}\dots i_{j-1}i_{j+1}\dots i_{m+1}} \\ &\quad+\sum_{j=1}^{m+1}\sum_{k=j+1}^{m+1}(-1)^{j+k-1}g_{i_j}g_{i_k}\boldsymbol{e}_{i_1\dots i_{j-1}i_{j+1}\dots i_{k-1}i_{k+1}\dots i_{m+1}} \\ &= \mathbf{0},\end{aligned} \tag{6.8}$$

where the last equation follows from (6.7).

Observe that by the definition of least common multiple, the S-vector $S(\boldsymbol{s}_{i_1\dots i_m},\boldsymbol{s}_{j_1\dots j_m})$ is $\mathbf{0}$ unless $\{i_2,\dots,i_m\}=\{j_2,\dots,j_m\}$ and $i_1\neq j_1$. Assume that $i_1<j_1$ and consider three cases.

First, let $1\le i_1<j_1\le k$. We have by (6.8),

$$\begin{aligned}S(\boldsymbol{s}_{i_1i_2\dots i_m},\boldsymbol{s}_{j_1i_2\dots i_m}) &= x_{j_1}\boldsymbol{s}_{i_1i_2\dots i_m}-x_{i_1}\boldsymbol{s}_{j_1i_2\dots i_m} \\ &= x^{\boldsymbol{m}_{j_1}}\boldsymbol{s}_{i_1i_2\dots i_m}-x^{\boldsymbol{m}_{i_1}}\boldsymbol{s}_{j_1i_2\dots i_m} \\ &\quad+\sum_{s=2}^{m}(-1)^{s-1}g_{i_s}\boldsymbol{s}_{i_1j_1i_2\dots i_{s-1}i_{s+1}\dots i_m},\end{aligned}$$

Second, let $1 \leq i_1 \leq k$ and $k+1 \leq j_1 \leq n$. In view of (6.8), we have

$$\begin{aligned} S(\boldsymbol{s}_{i_1 i_2 \ldots i_m}, \boldsymbol{s}_{j_1 i_2 \ldots i_m}) &= x_{j_1}^p \boldsymbol{s}_{i_1 i_2 \ldots i_m} - x_{i_1} \boldsymbol{s}_{j_1 i_2 \ldots i_m} \\ &= \boldsymbol{s}_{i_1 i_2 \ldots i_m} - x^{\boldsymbol{m}_{i_1}} \boldsymbol{s}_{j_1 i_2 \ldots i_m} + \sum_{s=2}^{m} (-1)^{s-1} g_{i_s} \boldsymbol{s}_{i_1 j_1 i_2 \ldots i_{s-1} i_{s+1} \ldots i_m}. \end{aligned}$$

Third, let $k+1 \leq i_1 < j_1 \leq n$. By (6.8), we have

$$\begin{aligned} S(\boldsymbol{s}_{i_1 i_2 \ldots i_m}, \boldsymbol{s}_{j_1 i_2 \ldots i_m}) &= x_{j_1}^p \boldsymbol{s}_{i_1 i_2 \ldots i_m} - x_{i_1}^p \boldsymbol{s}_{j_1 i_2 \ldots i_m} \\ &= \boldsymbol{s}_{i_1 i_2 \ldots i_m} - \boldsymbol{s}_{j_1 i_2 \ldots i_m} + \sum_{s=2}^{m} (-1)^{s-1} g_{i_s} \boldsymbol{s}_{i_1 j_1 i_2 \ldots i_{s-1} i_{s+1} \ldots i_m}. \end{aligned}$$

It follows that the syzygies provided by the S-vectors according to (6.1) are given by the $\boldsymbol{s}_{i_1 \ldots i_{m+1}}$. By Schreyer's theorem, the $\boldsymbol{s}_{i_1 \ldots i_{m+1}}$ form a Groebner basis of the m-th syzygy module. ■

This resolution is an example of a Koszul complex [22].

Given a generator matrix for any code, Groebner basis, generators of the syzygy modules and free resolution of the ideal corresponding to the code can be contructed as follows.

6.2.3 Example The third binary Hamming code C is a $[7,4]$ code with minimum Hamming distance 3 and generator matrix $G_3 = (I_4, M)$ [58, 42], where

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

Given any monomial order with $x_1 \succ \ldots \succ x_7$, the corresponding ideal I_C in $\mathbb{Q}[x]$ has the reduced Groebner basis

$$\begin{aligned} g_1 &= x_1 - x_5 x_6 x_7, \\ g_2 &= x_2 - x_5 x_6, \\ g_3 &= x_3 - x_5 x_7, \\ g_4 &= x_4 - x_6 x_7, \\ g_5 &= x_5^2 - 1, \\ g_6 &= x_6^2 - 1, \\ g_7 &= x_7^2 - 1. \end{aligned}$$

A free resolution of I_C is given by

$$0 \xrightarrow{\phi_7} R \xrightarrow{\phi_6} R^7 \xrightarrow{\phi_5} R^{21} \xrightarrow{\phi_4} R^{35} \xrightarrow{\phi_3} R^{35} \xrightarrow{\phi_2} R^{21} \xrightarrow{\phi_1} R^7 \xrightarrow{\phi_0} R \to 0,$$

where $I_C = \text{im}\,(\phi_0)$. For instance, generators of the syzygy modules of I_C (one for each module) are as follows,

$$\begin{aligned}
\boldsymbol{s}_{12} &= g_1\boldsymbol{e}_2 - g_2\boldsymbol{e}_1,\\
\boldsymbol{s}_{123} &= g_1\boldsymbol{e}_{23} - g_2\boldsymbol{e}_{13} + g_3\boldsymbol{e}_{12},\\
\boldsymbol{s}_{1234} &= g_1\boldsymbol{e}_{234} - g_2\boldsymbol{e}_{134} + g_3\boldsymbol{e}_{124} - g_4\boldsymbol{e}_{123},\\
\boldsymbol{s}_{12345} &= g_1\boldsymbol{e}_{2345} - g_2\boldsymbol{e}_{1345} + g_3\boldsymbol{e}_{1245} - g_4\boldsymbol{e}_{1235} + g_5\boldsymbol{e}_{12346},\\
\boldsymbol{s}_{123456} &= g_1\boldsymbol{e}_{23456} - g_2\boldsymbol{e}_{13456} + g_3\boldsymbol{e}_{12456} - g_4\boldsymbol{e}_{12356} + g_5\boldsymbol{e}_{123467} - g_6\boldsymbol{e}_{12345},\\
\boldsymbol{s}_{1234567} &= g_1\boldsymbol{e}_{234567} - g_2\boldsymbol{e}_{134567} + g_3\boldsymbol{e}_{124567} - g_4\boldsymbol{e}_{123567} + g_5\boldsymbol{e}_{123467}\\
&\quad -g_6\boldsymbol{e}_{123457} + g_7\boldsymbol{e}_{123456}.
\end{aligned}$$

♦

Chapter 7

Conclusions and Future Directions

In this work Groebner basis corresponding to ideal codes have been constructed in order to provide systematic encoding procedure which is often desired in practice. Benefits of studying linear codes lie in the fact that their algebraic structure helps in developing better encoding and decoding methods. Our approach in this work was as follows:

- Cyclic codes as ideals in a quotient ring were considered and their structure was explored via Groebner bases.
- A binomial ideal, given as a sum of a toric ideal and a non prime ideal has been associated to a linear code.
- Groebner basis theory was used to study this ideal deeply. Many useful results regarding the encoding procedure of the code corresponding to this ideal were found.

A very useful result has been proven which enables one to describe reduced Groebner basis directly from a generator matrix of a given code. Once Groebner basis are defined, the standard encoding method can be applied. Furthermore, minimal generators of the binomial ideal have been presented. Also this binomial ideal has been described in terms of its syzygy module and the corresponding finite free resolutions were given. Although many algebraic aspects of the binomial ideal corressponding to a linear code have been explored, still there are some issues which are worthy of further investigation:

- Development of a decoding procedure with respect to the Groebner basis constructed for the ideal corresponding to code.
- It would be valuable to further investigate the structure of the binomial ideal which may result into better encoding and decoding procedures.
- In this work, binomial ideal has been considered over a prime field. Considering it over some other field may turn out to be more beneficial.

The aim of algebraic coding theory is to construct effectively good codes, by assuming some algebraic structure on the code. In this work efforts are being made to show that how the Groebner bases theory can be used effectively for this purpose.

Bibliography

[1] W.W. Adams and P. Loustaunau. *An introduction to Gröbner bases*. Amer Mathematical Society, 1994.

[2] E.F. Assmus and J.D. Key. Polynomial codes and finite geometries. *Handbook of coding theory*, 2:1269–1343, 1998.

[3] D. Augot, M. Bardet, and J.C. Faugere. Efficient decoding of binary cyclic codes above the correction capacity of the code using gröbner bases. In *IEEE international symposium on information theory*, pages 362–362. Citeseer, 2003.

[4] T. Becker, V. Weispfenning, and H. Kredel. *Gröbner bases: a computational approach to commutative algebra*, volume 141. Springer-Verlag, 1993.

[5] S.D. Berman. On the theory of group codes. *Cybernetics and Systems Analysis*, 3(1):25–31, 1967.

[6] A.M. Bigatti, R. La Scala, and L. Robbiano. Computing toric ideals. *Journal of Symbolic Computation*, 27(4):351–365, 1999.

[7] M. Borges-Quintana, M.A. Borges-Trenard, P. Fitzpatrick, and E. Martinez-Moro. Gröbner bases and combinatorics for binary codes. *Applicable Algebra in Engineering, Communication and Computing*, 19(5):393–411, 2008.

[8] R.C. Bose and D.K. Ray-Chaudhuri. On a class of error correcting binary group codes*. *Information and control*, 3(1):68–79, 1960.

[9] B. Buchberger. An algorithmic criterion for the solvability of algebraic systems of equations. *Aequationes mathematicae*, 4(3):374–383, 1970.

[10] B. Buchberger. Bruno buchberger's phd thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of symbolic computation*, 41(3-4):475–511, 2006.

[11] B. Buchberger and F. Winkler. *Gröbner bases and applications*. Cambridge Univ Pr, 1998.

[12] S. Bulygin and R. Pellikaan. Bounded distance decoding of linear error-correcting codes with gröbner bases. *Journal of Symbolic Computation*, 44(12):1626–1643, 2009.

[13] P. Charpin. Une generalisation de la construction de berman des codes de reed et muller p-aires. *Communications in algebra*, 16(11):2231–2246, 1988.

[14] k. Clark and T. Marley. The perfect code: Golay codes. `http://usna.edu/Users/math/wdj/teach/`, 2005.

[15] S. Collart, M. Kalkbrener, and D. Mall. Converting bases with the groebner walk. *Journal of Symbolic Computation*, 24:465–469, 1997.

[16] B. Cooke. Reed-muller error correcting codes. *MIT Undergraduate journal of mathematics*, 1(6):21–26, 1999.

[17] A.B. Cooper. Toward a new method of decoding algebraic codes using Gröbner bases. Technical report, DTIC Document, 1993.

[18] D.A. Cox, J. Little, D. O'Shea, and M. Sweedler. *Ideals, varieties, and algorithms*. Springer, 1992.

[19] D.A. Cox, J.B. Little, and D. O'Shea. *Using algebraic geometry*. Springer Verlag, 1998.

[20] P. Delsarte, J.M. Goethals, and F.J. Mac Williams. On generalized reed muller codes and their relatives. *Information and Control*, 16(5):403–442, 1970.

[21] M. Drton, B. Sturmfels, and S. Sullivant. *Lectures on algebraic statistics*. Birkhauser, 2009.

[22] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*. Springer, 1995.

[23] D. Eisenbud and B. Sturmfels. Binomial ideals. *Duke Mathematical Journal*, 84(1):1–46, 1996.

[24] C. Fernandez. *On Reed Muller and related quaternary codes*. PhD thesis, Universitat Autonoma de Barcelona, 2005.

[25] R. Fröberg. *An introduction to Gröbner bases*. Wiley, 1997.

[26] W. Fulton. *Introduction to toric varieties*, volume 131. Princeton Univ Pr, 1993.

[27] A. Gathmann. Algebraic geometry. *Lecture Notes*, 2004.

[28] M.J.E. Golay. Notes on digital coding. *Proc. ire*, 37(6):657, 1949.

[29] G.M. Greuel and G. Pfister. *A singular introduction to commutative algebra. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann*. Springer-Verlag, Berlin, 2002.

[30] R.W. Hamming. Error detecting and error correcting codes. *Bell System Technical Journal*, 29(2):147–160, 1950.

[31] R. Hartshorne. *Algebraic geometry*. springer Verlag, 1977.

[32] A. Hocquenghem. Codes correcteurs derreurs. *Chiffres*, 2(2):147–56, 1959.

[33] A.D. Jensen. Computing Groebner fans of toric ideals. Master's thesis, University of Aarhus, Denmark, 2002.

[34] A.M. Kasprzyk. A short introduction to toric varieties. `http://magma.maths.usyd.edu.au/users/kasprzyk/calf/`.

[35] M. Kreuzer and L. Robbiano. *Computational commutative algebra*, volume 2. Springer, 2005.

[36] F. Kschischang. Error correcting codes, 2007.

[37] P. Landrock and O. Manz. Classical codes as ideals in group algebras. *Designs, Codes and Cryptography*, 2(3):273–285, 1992.

[38] O. Lezama. Groebner basis for the modules over noetherian polynomial commutative rings. *Georgian mathematical jounal*, 15(1):121–137, 2008.

[39] R. Lidl, H. Niederreiter, and P.M. Cohn. *Finite fields*, volume 20. Cambridge Univ Pr, 1997.

[40] S. Ling and C. Xing. *Coding Theory: A First Course*. Cambridge University Press, 2004.

[41] D. Maclagan, R.R. Thomas, S. Faridi, L. Gold, AV Jayanthan, A. Khetan, and T. Puthenpurakal. Computational algebra and combinatorics of toric ideals. *Commutative algebra and combinatorics*, 2005.

[42] F.J. MacWilliams and N.J.A. Sloane. *Error correcting codes*. North–Holland, New York, 1977.

[43] D.E. Muller. Application of boolean algebra to switching circuit design and to error detection. *IRE Trans*, 1:6–12, 1954.

[44] L. Pottier. Grobner bases of toric ideals. *INRIA Rapport de recherche*, 2224, 1994.

[45] I.S. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.

[46] B. Reinert. A systematic study of gröbner basis methods. *Arxiv preprint arXiv:0903.2462*, 2009.

[47] S. Roman. *Coding and information theory*. Springer, 1992.

[48] M. Sala. Gröbner bases, coding, and cryptography: a guide to the state-of-art. *Gröbner Bases, Coding, and Cryptography*, pages 1–8, 2009.

[49] M. Saleemi and K.H. Zimmermann. Linear codes as binomial ideals. *Int. J. Pure Appl. Math*, 61:147–156.

[50] M. Saleemi and K.H. Zimmermann. Syzygies and free resolutions of linear codes. *Int. J. Pure Appl. Math., to appear*.

[51] M. Saleemi and K.H. Zimmermann. Groebner bases for a class of ideals in commutative polynomial rings. *Int. J. Pure Appl. Math*, 58:1–9, 2010.

[52] M. Saleemi and K.H. Zimmermann. Groebner bases for linear codes. *Int. J. Pure Appl. Math*, 62:481–491, 2010.

[53] F.O. Schreyer. *Die Berechnung von Syzygien mit dem verallgemeinerten Weierstraßschen Divisionssatz und eine Anwendung auf analytische Cohen-Macaulay Stellenalgebren minimaler Multiplizität*. PhD thesis, Hamburg, 1980.

[54] C. Shannon. Ea mathematical theory of communication. *The Bell System Technical Journal*, 27(7):379–423, 1948.

[55] N.J.A. Sloane. A survey of constructive coding theory, and a table of binary codes of highest known rate. *Discrete Mathematics*, 3(1-3):265–294, 1972.

[56] B. Sturmfels. *Gröbner bases and convex polytopes*. Amer Mathematical Society, 1996.

[57] W. Trinks. über b. buchbergers verfahren, systeme algebraischer gleichungen zu lösen. *Journal of Number Theory*, 10(4):475–488, 1978.

[58] J.H. Van Lint. *Introduction to coding theory*, volume 86. Springer Verlag, 1999.

[59] H.N. Ward. Visible codes. *Archiv der Mathematik*, 54(3):307–312, 1990.

[60] Volker Weispfennig. Constructing universal groebner bases. In *Proceedings of the 5th International Conference on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, AAECC-5, pages 408–417. Springer-Verlag, 1989.

[61] G. Zacharias. Generalized Groebner bases in commutative polynomial rings. Master's thesis, Massachusetts Institute of Technology, Cambridge, Massachusetts, 1978.

Tables

Table 7.1: Table of small seven-bit Reed-Muller codes and corresponding quinary Reed-Muller codes with designed distances that have the same length and minimum distance, but higher dimension.

		Reed-Muller code (original) $C(S_l)$			Reed-Muller code (designed distance δ) $C(T_\delta)$		
p	p^n	l	k	d	δ	k	d
7	49	1	48	2			
		2	46	3			
		3	43	4	4	44	4
		4	39	5	5	41	5
		5	34	6	6	39	6
		6	28	7	7	35	7
		7	21	14	13	24	14
		8	15	21			
		9	10	28			
		10	6	35			
		11	3	42			
		12	1	49			

Table 7.2: Table of small ternary Reed-Muller codes and Reed-Muller codes with designed distances whose parameters differ from the original Reed-Muller codes.

		Reed-Muller code (original) $C(S_l)$			Reed-Muller code (designed distance δ) $C(T_\delta)$		
p	p^n	l	k	d	δ	k	d
3	9	1	8	2			
		2	6	3			
		3	3	6			
		4	1	9			
	27	1	26	2			
		2	23	3			
		3	17	6	7	11	8
		4	10	9	10	7	12
		5	4	18			
		6	1	27			
	81	1	80	2			
		2	76	3			
		3	66	6	7	54	8
		4	50	9	10	44	12
		5	31	18	13	32	16
		6	15	27	19	19	24
		7	5	54	28	11	36
		8	1	81			

Table 7.3: Table of small quinary Reed-Muller codes and corresponding quinary Reed-Muller codes with designed distances that have the same length and minimum distance, but higher dimension.

		Reed-Muller code (original) $C(S_l)$			Reed-Muller code (designed distance δ) $C(T_\delta)$		
p	p^n	l	k	d	δ	k	d
5	25	1	24	2			
		2	22	3			
		3	19	4	4	20	4
		4	15	5	5	17	5
		5	10	10			
		6	6	15			
		7	3	20			
		8	1	25			
	125	1	124	2			
		2	121	3			
		3	115	4			
		4	105	5	5	112	5
		5	90	10	10	93	10
		6	72	15	13	78	15
		7	53	20	19	63	20
		8	35	25	25	48	25
		9	20	50			
		10	10	75			
		11	4	100			
		12	1	125			

List of Publications

- M. Saleemi, K.-H. Zimmermann, Groebner bases for a class of ideals in commutative polynomial rings, *Int J Pure Appl Math*, 58(1):1-9, 2010.
- M. Saleemi, K.-H. Zimmermann, From ideals in polynomial rings to linear codes using Groebner bases, *Int. J. Pure Appl. Math*, 65(1): 41-54, 2010.
- M. Saleemi, K.-H. Zimmermann, Linear codes as binomial ideals. *Int J Pure Appl Math*, 61(2);147-156, 2010.
- M. Saleemi, K.-H. Zimmermann, Groebner bases for linear codes, *Int J Pure Appl Math*, 62(4):481-491, 2010.
- M. Saleemi, K.-H. Zimmermann: Syzygies and free resolutions of linear codes. *Int Electr J Pure Appl Math*, to appear.

Curriculum Vitae

Born on 18th May 1974 in Islamabad, Pakistan.

Jan. 1995 – Jan. 1997	M. Sc. Mathematics	Quaid-e-Azam University, Islamabad
Jan. 1997 – Jan. 1999	M. Phil. Mathematics	Quaid-e-Azam University, Islamabad
Mar. 1999 – Aug. 2001	Lecturer	University College of Islamabad
Feb. 2002 – Dec. 2002	research collaboration	UMIST, Manchester, England
Jan. 2003 – Dec. 2007	parental leave	
Jan. 2008 – date	Ph. D. Student	Hamburg University of Technology TUHH, Germany.