Thesis

A Gröbner basis algorithm for effective encoding of Reed-Müller codes

Olle Abrahamsson

The number your thesis gets from administrators

A Gröbner basis algorithm for effective encoding of Reed-Müller codes

Department of Mathematics, Linköping University

Olle Abrahamsson

The number your thesis gets from administrators

Thesis: **16 hp**

Level: **G2**

Supervisor: **Jan Snellman**,
Department of Mathematics, Linköping University

Examiner: **Leif Melkersson**,
Department of Mathematics, Linköping University

Linköping: **September 2015**

Abstract

In this thesis the relationship between Gröbner bases and algebraic coding theory is investigated, and especially applications towards linear codes, with Reed-Müller codes as an illustrative example. We prove that each linear code can be described as a binomial ideal, and that its generating matrix immediately provides a reduced Gröbner basis. Finally, we show how a systematic encoding algorithm for such codes is given by the remainders of the information word computed with respect to the reduced Gröbner basis.

Keywords:
Gröbner basis, coding theory, algebra, Reed-Müller

URL for electronic version:
The url to the thesis

Acknowledgements

First and foremost I would like to thank my supervisor Dr. Jan Snellman for his never ending enthusiasm for this subject and all the support he has given me, and for introducing me to the wonderful subject of abstract algebra in general, and the theory of Gröbner bases in particular. Likewise I want to thank my examiner Dr. Leif Melkersson for the interest he has taken into this thesis, and for his much appreciated lectures in commutative algebra, which have come in handy in trying to understand all the theory in this thesis.

Second, many thanks to my opponent and dear friend, Anton Karlsson, who has given me much constructive criticism and suggestions for improvement during the production of this work. He has also stimulated me with many interesting conversation about almost everything conceivable, but mostly mathematics of course. And fortunately for me, we have shared many laughs together during this process. He is truly a great friend. For all of this I am eternally grateful.

Last and probably least, I would like to thank Johan Åke Nilsson, whose rather dark sense of humour definitely have helped restore my sanity during nights of frustration with either tedious mathematics or problems of a more mundane nature.

Nomenclature

Most of the recurring letters and symbols are described here.

Letters

$x, y, z, \ldots$ or $x_1, x_2, x_3, \ldots$	Variables
$R, S, \ldots$	Sets or rings
$\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$	Ideals
I	Ideal

Symbols

$A \subset B$	A is a proper subset of B
$A \subseteq B$	A is a (possibly nonproper) subset of B
$A \cong B$	A is isomorphic to B
$\mathbb{F}$	Field
$\mathbb{F}_q$	Finite field
$\mathbb{F}_p$	Prime field

Contents

Chapter 1

Introduction

In a world where digital communication is all around us, it is vital to have reliable infrastructure for all this information. Inevitably, the information must be sent through noisy channels due to physical limitations: impurities in wires, interference from other channels and cosmic backgruond radiation are a few examples. In order to overcome these issues, error-correcting codes are introduced. These codes admit a method through with we may encode messages and later correct them when they are transmitted through a noisy channel. The objectives in coding theory are

- efficient encoding of messages,
- smooth transmission of encoded messages,
- efficient and reliable decoding of received messages, and
- transmission of a large number of messages per unit of time.

In this work we will study an algorithm for a fast decoding of special kind of error-correcting codes, so called linear codes. Especially we will restrict our attention to the types of linear error-correcting codes that are called Reed-Müller codes. The algorithm builds on a concept called Gröbner bases, which may be seen as a multivariate, non-linear generalisation of the Euclidian algorithm for computing polynomial greatest common divisors, and Gaussian elimination for linear systems [7].

Chapter 2

Rings and ideals

In this chapter we will introduce some basic terminology and a few important results in abstract algebra that will be needed later. By necessity, the chapter will contain a rather terse and compact list of definitions and theorems in order to quickly get to the more interesting parts of the thesis. However, spending some time to familiarise oneself with this language will really be worth the effort in order to understand the material later on, which this author can testify to!

2.1 Rings

Something interesting about rings. Blablabla.

Definition 1. A **ring** is a set R with two binary operators denoted by $+$, called addition, and $\cdot$, called multiplication, such that for all elements a, b, c in R the following conditions are satisfied.

(i)	$a+b \in R$, $a \cdot b \in R$	(v)	$\exists\ 0 \in R$ s.t. $0+a=a=a+0$
(ii)	$a+b=b+a$	(vi)	$\exists\ -a \in R$ s.t. $a+(-a)=0$
(iii)	$(a+b)+c=a+(b+c)$, $(a\cdot b)\cdot c = a\cdot(b\cdot c)$	(vii)	$a\cdot(b+c)=a\cdot b+a\cdot c$, $(a+b)\cdot c = a\cdot c+b\cdot c$
(iv)	$\exists\ 1 \in R$ s.t. $1\cdot a = a = a\cdot 1$		

Remark. We will often simply write ab for the product $a \cdot b$.

Definition 2. The ring R is said to be **commutative** if $\forall\ a, b \in R, ab = ba$.

Definition 3. A commutative ring $R \neq \{0\}$ in which $ab = 0$ implies $a = 0$ or $b = 0$ is called an **integral domain**.

For example $\mathbb{Z}$, the set of all integers, is an integral domain since if $a, b \in \mathbb{Z}$, then $ab = 0$ implies $a = 0$ or $b = 0$. However, the ring $\mathbb{Z}_2$ of integers with addition and multiplication modulo 2 is not an integral domain since for example $2 \cdot 2 = 4 = 0 \pmod 2$.

Definition 4. A **field** is a commutative ring $R \neq \{0\}$ in which every element $a \neq 0$ has a multiplicative inverse a^{-1}, so that $aa^{-1} = 1$.

Remark. Unless explicitly stated otherwise, the word ring will henceforth mean a commutative ring.

Definition 5. A **finite ring** is a ring with finitely many elements.

An important example of a finite ring is $\mathbb{Z}_n$, which is the set of integers $\mathbb{Z}$ together with addition and multiplication modulo n. For example, $\mathbb{Z}_4$, which has the elements $\{0, 1, 2, 3\}$, yields the following addition and multiplication tables.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

One can easily verify that $\mathbb{Z}_n$ is a ring where n is a positive integer.

Definition 6. A **finite field** is a field with finitely many elements, and is denoted $\mathbb{F}_q$, where q is the number of elements.

We will now turn to a special kind of ring whose elements are polynonmials. This family of rings will be our main focus when dealing with coding theory later on.

Definition 7. A **polynomial ring** $K[x]$ in the variable X over a field K is defined as the set of expressions, called **polynomials** in X, of the form

$$p = p_0 + p_1 x + p_2 x^2 + \cdots + p_{n-1} x^{n-1} + p_n x^n,$$

where $p_0, p_1, \ldots, p_n$ are elements of K, called **coefficients**, and $x, x^2, \ldots, x^n$ are formal symbols. By convention $x^0 = 1$ and $x^1 = x$, and the product of the powers of x is defined by the formula

$$x^k x^l = x^{k+l}, \quad k, l \in \mathbb{N}.$$

Note that the definition of polynomial rings easily generalises to severable variables, and we denote by $K[x_1, \ldots, x_n]$ the polynomial ring over R in n variables, $x_1, \ldots, x_n$.

Definition 8. The **degree** of an element $m = x_1^{i_1} \cdots x_n^{i_n}$ in a polynomial ring $K[x_1, \ldots, x_n]$ is $\deg(\mathrm{m}) \coloneqq i_1 + \cdots + i_n$. The degree of a nonzero polynomial $f(x_1, \ldots, x_n) = \sum r_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$ equals

$$\deg(f) = \max\{\deg(x_1^{i_1} \cdots x_n^{i_n}) : r_{i_1,\ldots,i_n} \neq 0\}.$$

A polynomial of degree zero is called a **constant**.

2.2 Ideals

An ideal is a special subset of a ring. Ideals can be viewed as a generalisation of certain subsets of the integers. Take, for instance, the set of even integers. It is closed under addition and subtraction, and an even integer multiplied with any other integer yields still an even integer. These properties of closure and absorption are defining properties for an ideal. We will also consider a special kind of ideal called *prime ideals*. As the name suggests, they are analogous to prime numbers, and as such are fundamental building blocks. As we will see, ideals can also be generated by subsets of the ring they belong to. All of this will be of importance when constructing Gröbner bases later on.

Definition 9. A nonempty subset $\mathfrak{a}$ of a ring R is called an **ideal** of R if

(i) $a, b \in \mathfrak{a} \implies a + b \in \mathfrak{a}$
(ii) $a \in \mathfrak{a}, r \in R \implies ar \in \mathfrak{a}$.

A few facts follows immediately from the definition. If $\mathfrak{a}$ is an ideal, then the following statements are true.

(iii) $a \in \mathfrak{a} \implies -a = a \cdot (-1) \in \mathfrak{a}$.

(iv) $0 \in \mathfrak{a}$ since $0 = a \cdot 0 \ \forall \ a \in \mathfrak{a}$.

(v) The set $\{0\}$ is an ideal (called the trivial ideal), and so is the entire ring R (called the unit ideal).

(vi) $\mathfrak{a} = R$ if and only if $1 \in \mathfrak{a}$.

Proof. The proofs for (iii)-(v) are trivial. To see (vi), let first $\mathfrak{a} = R$. Since $1 \in R$ we have $1 \in \mathfrak{a}$. And if $1 \in \mathfrak{a}$, then $r = 1 \cdot r \in \mathfrak{a} \ \forall \ r \in R$, so $\mathfrak{a} = R$. □

Definition 10. Let r be an element in a ring R. The set of all multiples of $r, \{rs : s \in R\}$, constitutes an ideal and is called a **principal ideal**, and r is called a **generator** for the ideal. The principal ideal generated by r is denoted by $\langle r \rangle$.

For instance, both R and $\{0\}$ are principal ideals, where $R = \langle 1 \rangle$ and $\{0\} = \langle 0 \rangle$. One can also have ideals generated by multiple generators, using the following definition.

Definition 11. An ideal I of a ring R is said to be generated by a set $X \subseteq R$ if

$$I = \{r_1 x_1 + \cdots + r_n x_n : n \in \mathbb{N}, r_i \in R, x_i \in X\}.$$

The ideal generated by X is denoted $I = \langle x_1, \ldots, x_n \rangle$.

The following theorem is very important since it provides us with a way to uniquely divide polynomials.

Theorem 1 (The Euclidian algorithm)**.** *Let $\mathbb{K}$ be any field and suppose $f, g \in \mathbb{K}[x], f \neq 0$. Then there are uniquely defined polynomials $q, r \in \mathbb{K}[x]$ such that $g = qf + r$ with $deg(r) < deg(f)$ or $r = 0$.*

Proof. If $g = 0$ we can choose $q = r = 0$. Otherwise, let $f = a_n x^n + \cdots + a_0, a_n \neq 0$ and let $g = b_m x^m + \cdots + b_0, b_m \neq 0$. If $m < n$ we can choose $q = 0$ and $r = g$. If $m \geq n$ we see that $g = b_m a_n^{-1} x^{m-n} f + r_1$, where $\deg(r_1) < \deg(g)$ or $r_1 = 0$. If $r_1 \neq 0$ and $\deg(r_1) > \deg(f)$, say $r_1 = c_k x^k + \cdots + c_0$, we can continue and write $r_1 = c_k a_n^{-1} x^{k-n} f + r_2$, with $\deg(r_2) < \deg(r_1)$ or $r_2 = 0$, so $g = (b_m a_n^{-1} x^{m-n} + c_k a_n^{-1} x^{k-n}) f + r_2$. It is clear that in a finite number of steps we get a remainder which either is zero or has a smaller degree than $\deg(f)$. It remains to be shown that q and r are unique. Suppose that $g = q_1 f + r_1 = q_2 f + r_2$. Then $(q_1 - q_2) f = r_2 - r_1$. We have $\deg((q_1 - q_2) f) \geq \deg(f)$ if $q_1 - q_2 \neq 0$, which is a contradiction since $\deg(r_2 - r_1) < \deg(f)$. Thus $q_1 = q_2$. That gives $0 = 0 \cdot f = r_2 - r_1$, so $r_2 = r_1$. □

Definition 12. Let f and g be nonzero polynomials in a polynomial ring $\mathbb{K}[x]$. Then h is a **greatest common divisor** of f and g, denoted by $\gcd(f, g)$, if h divides both f and g, and any other polynomial which divides both f and g, also divides h.

Theorem 2. *The last nonvanishing remainder in the Euclidian algorithm performed on f and g is a greatest common divisor to f and g. If h_1 and h_2 both are $\gcd(f,g)$, then $h_1 = ch_2$ for some $c \in \mathbb{K}$.*

Proof. For a proof, see e.g. [5, pp. 12-13]. □

Theorem 3. *Let f and g be nonzero polynomials in $\mathbb{K}[x]$. Then $\langle f,g\rangle = \langle \gcd(f,g)\rangle$.*

Proof. Let $h = \gcd(f,g)$. We know that h is a linear combination of f and g (see the previous theorem), which gives $h \in \langle f,g\rangle$. This gives that $\langle h\rangle \subseteq \langle f,g\rangle$, since $\langle h\rangle = \{rh : r \in \mathbb{K}[x]\}$, and if $h \in \langle f,g\rangle$, then $rh \in \langle f,g\rangle$. On the other hand, both f and g are multiples of h (since $h = \gcd(f,g)$), and so $f,g \in \langle h\rangle$, which gives $\langle f,g\rangle = \{r_1 f + r_2 g : r_1, r_2 \in \mathbb{K}\} \subseteq \langle h\rangle$. Thus ($\langle f,g\rangle \subseteq \langle h\rangle$ and $\langle h\rangle \subseteq \langle f,g\rangle$), which implies $\langle f,g\rangle = \langle h\rangle = \langle \gcd(f,g)\rangle$. □

Let us now examine some interesting and useful properties of the ideals and their calculus.

Theorem 4. *If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in R, then the following objects are also ideals.*

(i) $\mathfrak{a} + \mathfrak{b} = \{a + b : a \in \mathfrak{a}, b \in \mathfrak{b}\}$,
(ii) $\mathfrak{a} \cap \mathfrak{b}$,
(iii) $\mathfrak{a} \cdot \mathfrak{b} = \{\sum_{i=1}^{k} a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$,
(iv) $\mathfrak{a} : \mathfrak{b} = \{r \in R : rb \in \mathfrak{a}\ \forall\ b \in \mathfrak{b}\}$.

Definition 13. The **radical of an ideal** in a ring R is the set $\sqrt{\mathfrak{a}} = \{r \in R : r^n \in \mathfrak{a},\ \text{for some } n\}$, where n is a positive integer.

Definition 14. An ideal $\mathfrak{a}$ is called a **radical** if $\sqrt{\mathfrak{a}} = \mathfrak{a}$.

2.3 Factor rings and homomorphisms

Definition 15. Let $\mathfrak{a}$ be an ideal in a ring R. An equivalence class $[a]$ consists of the set $\{a + a' : a' \in \mathfrak{a}\}$. These equivalence classes are often called **cosets** of $\mathfrak{a}$. If $a + \mathfrak{a} = b + \mathfrak{a}$, i.e. if $a - b \in \mathfrak{a}$ we say that a is equivalent to $b \mod \mathfrak{a}$. The set of equivalence classes (cosets) is denoted by $R/\mathfrak{a}$. We make $R/\mathfrak{a}$ into a ring by defining

$$(a_1 + \mathfrak{a}) + (a_2 + \mathfrak{a}) = (a_1 + a_2) + \mathfrak{a},\ \text{and}\ (a_1 + \mathfrak{a})(a_2 + \mathfrak{a}) = a_1 a_2 + \mathfrak{a}.$$

With these operations, $R/\mathfrak{a}$ becomes a ring, the **quotient ring** of $R \mod \mathfrak{a}$. (In some literature this is also known as a factor ring, or residue class ring.)

Remark. In mathematical jargon, one often talks about *modding out by* $\mathfrak{a}$.

Definition 16. Let R, S be rings. A map $f\colon R \to S$ is called a **(ring) homomorphism** if it respects the ring structures, i.e. if

$$\begin{aligned} &f(r +_R s) = f(r) +_S f(s) \\ &f(r \cdot_R s) = f(r) \cdot_S f(s),\ \text{and} \\ &f(1_R) = 1_S. \end{aligned}$$

If f is a bijective homomorphism (i.e. a homomorphism that is both surjective and injective), we say that f is an **isomorphism**, and that R and S are **isomorphic**, denoted by $R \cong S$.

Definition 17. The **image** of a (ring) homomorphism $f\colon R \to S$ is defined by

$$\mathrm{im}(f) = \{s \in S : s = f(r), r \in R\}.$$

The **kernel** of a (ring) homomorphism $f\colon R \to S$ is defined by

$$\ker(f) = \{r \in R : f(r) = 0_S\}.$$

Theorem 5. *Let $f\colon R \to S$ be a homomorphism. Then $\ker(f)$ is an ideal in R. If f also is surjective, then $S \cong R/\ker(f)$.*

This is a part of the so called isomorphism theorems. For a proof of this particular theorem, see [5, p. 26]. As an illustration of the theorem, consider the following: If $f\colon R \to R/\mathfrak{a}$ is the canonical homomorphism, defined by $f(r) = r + \mathfrak{a}$, then f is surjective, and by the theorem we have that $\ker(f) = \mathfrak{a}$.

2.4 Prime and maximal ideals

Definition 18. An ideal $\mathfrak{p} \neq R$ in a ring is called a **prime ideal** if $rs \in \mathfrak{p}$ implies that $r \in \mathfrak{p}$ or $s \in \mathfrak{p}$.

Lemma 6. *The ideal $\mathfrak{p}$ is a prime ideal if and only if $\mathfrak{a}_1 \cdots \mathfrak{a}_k \subseteq \mathfrak{p}$ implies that some $\mathfrak{a}_i \subseteq \mathfrak{p}$.*

Proof. Suppose $\mathfrak{p}$ is a prime ideal. By induction on k it is clear that we only need to consider the case $k = 2$. Let $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{p}$ and suppose that $\mathfrak{a}_1 \subset \mathfrak{p}$. Take an $x \in \mathfrak{a}_1 \setminus \mathfrak{p} = \{a \in \mathfrak{a}_1 : a \notin \mathfrak{p}\}$. For each $a \in \mathfrak{a}_2$ we have $xa \in \mathfrak{p}$ which gives $a \in \mathfrak{p}$, so $\mathfrak{a}_2 \subseteq \mathfrak{p}$.
For the converse we note that $xy \in \mathfrak{p}$ is equivalent to $\langle x\rangle\langle y\rangle \subseteq \mathfrak{p}$. Hence if $xy \in \mathfrak{p}$ then $\langle x\rangle\langle y\rangle \subseteq \mathfrak{p}$ which gives $\langle x\rangle \subseteq \mathfrak{p}$ or $\langle y\rangle \subseteq \mathfrak{p}$, i.e. $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. □

Lemma 7 (Prime avoidance)**.** *Let $\mathfrak{a}$ be an ideal and let $\mathfrak{p}_i$ be prime ideals for $i = 1, \ldots, s$. If $\mathfrak{a} \subseteq \cup_{i=1}^{s} \mathfrak{p}_i$, then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i.*

Proof. See [5, p. 29] □

Definition 19. Let R be a ring. An ideal $\mathfrak{m} \neq R$ is called a **maximal ideal** of R if the only ideal of R which strictly contains $\mathfrak{m}$ is R.

Theorem 8. *An ideal $\mathfrak{p}$ in a ring R is a prime ideal if and only if $R/\mathfrak{p}$ is an integral domain. An ideal $\mathfrak{m}$ is a maximal ideal if and only if $R/\mathfrak{m}$ is a field. All maximal ideals are prime.*

Proof. ($\Longrightarrow$) Suppose that $\mathfrak{p}$ is prime, and fix two elements $a + \mathfrak{p}$ and $b + \mathfrak{p}$ of $R/\mathfrak{p}$. Suppose that their product $ab + \mathfrak{p}$ equals $0 + \mathfrak{p}$, the zero element of $R/\mathfrak{p}$. By the definition of coset equivalence, this means that $ab - 0 \in \mathfrak{p}$, i.e. $ab \in \mathfrak{p}$. Now, since $\mathfrak{p}$ is prime, we know that either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. The former case leads quickly to the conlusion that $a + \mathfrak{p} = 0 + \mathfrak{p}$, whereas the latter case leads to $b + \mathfrak{p} = 0 + \mathfrak{p}$. In either case we have shown that the only way a product equals zero is if one of the factors equals zero, which establishes that $R/\mathfrak{p}$ is an integral domain.
($\Longleftarrow$) Conversely, suppose that $R/\mathfrak{p}$ is an integral domain, and fix elements $a, b \in R$ with $ab \in \mathfrak{p}$. We want to show that either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ by essentially

reversing the previous paragraph. We know that $(a+\mathfrak{p})(b+\mathfrak{p}) = ab+\mathfrak{p} = 0+\mathfrak{p}$ in $R/\mathfrak{p}$, and since $R/\mathfrak{p}$ has no zero divisors we conclude that $a+\mathfrak{p} = 0+\mathfrak{p}$ or $b+\mathfrak{p} = 0+\mathfrak{p}$. The former yields $a \in \mathfrak{p}$ while the latter yields $b \in \mathfrak{p}$.

($\implies$) Suppose $\mathfrak{m}$ is maximal and let $b \in R$ but $b \notin \mathfrak{m}$. Consider $\mathfrak{b} = br + a : r \in R, a \in \mathfrak{m}$. This is an ideal properly containing $\mathfrak{m}$. Since $\mathfrak{m}$ is maximal, $\mathfrak{b} = R$. Thus $1 = bc + a'$ for some $a' \in \mathfrak{m}$. Then $1 + \mathfrak{m} = bc + a' + \mathfrak{m} = bc + \mathfrak{m} = (b+\mathfrak{m})(c+\mathfrak{m})$.
($\impliedby$) Now suppose that $R/\mathfrak{m}$ is a field and $\mathfrak{b}$ is an ideal of R that properly contains $\mathfrak{m}$. Let $b \in \mathfrak{b}$ but $b \notin \mathfrak{m}$. Then $b+\mathfrak{m}$ is a nonzero element of $R/\mathfrak{m}$ and therefore there exists an element $c+\mathfrak{m}$ such that $(c+\mathfrak{m})(b+\mathfrak{m}) = 1+\mathfrak{m}$. Since $b \in \mathfrak{b}$ we have $bc \in \mathfrak{b}$. Because $1+\mathfrak{m} = (c+\mathfrak{m})(b+\mathfrak{m}) = bc+\mathfrak{m}$ we have $1-bc \in \mathfrak{m} \subset \mathfrak{b}$. So $1 = (1-bc)+bc \in \mathfrak{b}$. Hence $\mathfrak{b} = R$.

For the last statement, assume $\mathfrak{m}$ is a maximal ideal in a ring R. Suppose $r, s \in R$ s.t. $rs \in \mathfrak{m}$ but $r \notin \mathfrak{m}$. The maximality of $\mathfrak{m}$ implies that $\mathfrak{m} + \langle r \rangle = R = \langle 1 \rangle$. Thus there exists an element $m \in \mathfrak{m}$ and an element $x \in R$ such that $m + xr = 1$. Now m and rs belong to $\mathfrak{m}$ whence

$$s = 1 \cdot s = (m+xr)s = sm + x(rs) \in \mathfrak{m}.$$

So we can say that along with rs, at least one of its factors belong to $\mathfrak{m}$ and therefore $\mathfrak{m}$ is a prime ideal of R. □

2.5 Monomial ideals

Definition 20. An ideal $\mathfrak{a} \subset K[x_1, \ldots, x_n]$ is a **monomial ideal** if there is a subset $A \subset \mathbb{Z}^n_{\geq 0}$ (possibly infinite) such that $\mathfrak{a}$ consists of all polynomials which are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$, where $h_\alpha \in K[x_1, \ldots, x_n]$. In this case, we write $\mathfrak{a} = \langle x^\alpha : \alpha \in A \rangle$. Note that this is equivalent to the condition that $\mathfrak{a}$ is generated only by monomials.

For example, $\langle x^4y^2, x^3y^4, x^2y^5 \rangle \subset K[x,y]$ is a monomial ideal (since the generators are all monomials).

We need to characterise all polynomials that lie in a given monomial ideal. This characterisation is given by the following lemma.

Lemma 9. *Let $I = \langle x^\alpha : \alpha \in A \rangle$ be a monomial ideal. Then a monomial x^β lies in I of and only if x^β is divisible by x^α for some $\alpha \in A$.*

Proof. If x^β is a multiple of x^α for some $\alpha \in A$, then $x^\beta \in I$ by the definition of ideal. Conversely, if $x^\beta \in I$, then $x^\beta = \sum_{i=1}^s h_i x^{\alpha(i)}$, where $h_i \in K[x_1, \ldots, x_n]$ and $\alpha(i) \in A$. If we expand each h_i as a linear combination of monomials, we see that every term on the right side of the equation is divisible by some $x^{\alpha(i)}$. Hence, the left side x^β must have the same property. □

Lemma 10. *Let I be a monomial ideal, and let $f \in K[x_1, \ldots, x_n]$. Then the following are equivalent.*

(i) $f \in I$
(ii) *Every term of f belongs to I*
(iii) *f is a K-linear combination of the monomials in I. (This means that the coefficients belong to K.)*

For a proof of this lemma and the remaining results in this subsection, see [3, p. 71]. It follows immediately from (iii) that a monomial ideal is uniquely determined by the monomial it contains. Thus we get the following corollary.

Corollary 10.1. *Two monomial ideals are identical if and only if they contain precisely the same monomials.*

The main result from this section is that monomial ideals of $K[x_1, \ldots, x_n]$ are finitely generated.

Theorem 11 (Dickson's lemma)**.** *Let $I = \langle x^\alpha : \alpha \in A \rangle \subseteq K[x_1, \ldots, x_n]$ be a monomial ideal. Then I can be written in the form*

$$I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle,$$

where $\alpha(1), \ldots, \alpha(s) \in A$. In particular, I has a finite basis.

2.5.1 Sums and products of monomial ideals

Recall that for any two ideals, $\mathfrak{a} = \langle a_1, \ldots, a_r \rangle$ and $\mathfrak{b} = \langle b_1, \ldots, b_s$, their sum is

$$\mathfrak{a} + \mathfrak{b} = \langle a_1, \ldots, a_r, b_1, \ldots, b_s \rangle$$

and their product is

$$\mathfrak{ab} = \langle a_1 b_1, \ldots, a_1 b_s, \ldots, a_r b_1, \ldots, a_r b_s \rangle.$$

Let us illustrate this with a concrete example:

With $\mathfrak{a} = \langle x^3, xy, y^4 \rangle$ and $\mathfrak{b} = \langle x^2, xy^2 \rangle$, we get

$$\mathfrak{a} + \mathfrak{b} = \langle x^3, xy, y^4, x^2, xy^2 \rangle = \langle xy, x^2, y^4 \rangle$$

since $x^2 | x^3$ and $xy | xy^2$.
Similarily,

$$\mathfrak{ab} = \langle x^5, x^4y^2, x^3y, x^2y^3, x^2y^4, xy^6 \rangle = \langle x^5, x^3y, x^2y^3, xy^6 \rangle.$$

2.5.2 Intersection of monomial ideals

If the ideals $\mathfrak{a} = \langle m \rangle$ and $\mathfrak{b} = \langle n \rangle$ are both principal ideals (i.e. generated by a single element), then $\mathfrak{a} \cap \mathfrak{b} = \langle \mathrm{lcm}(m, n) \rangle$, where lcm stands for least common multiple. Thus, for example,

$$\langle x^2 y \rangle \cap \langle xy^3 \rangle = \langle \mathrm{lcm}(x^2 y, xy^3) \rangle = \langle x^2 y^3 \rangle.$$

For any three ideals, one can easily see that

$$(\mathfrak{a} + \mathfrak{b}) \cap \mathfrak{c} \supseteq (\mathfrak{a} \cap \mathfrak{c}) + (\mathfrak{b} \cap \mathfrak{c}).$$

But if $\mathfrak{a}, \mathfrak{b}$ and $\mathfrak{c}$ are monomial ideals, the relation becomes an equailty,

$$(\mathfrak{a} + \mathfrak{b}) \cap \mathfrak{c} = (\mathfrak{a} \cap \mathfrak{c}) + (\mathfrak{b} \cap \mathfrak{c}).$$

For a proof, see [5, p. 39]. In fact, we get that for monomial ideals,

$$\langle m_1, \ldots, m_r \rangle \cap \langle n_1, \ldots, n_s \rangle = \sum_{i=1}^{r} \sum_{j=1}^{s} \langle m_i \rangle \cap \langle n_j \rangle = \sum_{i=1}^{r} \sum_{j=1}^{s} \langle \operatorname{lcm}(m_i, n_j) \rangle.$$

Returning to our monomial ideals $\mathfrak{a} = \langle x^3, xy, y^4 \rangle$ and $\mathfrak{b} = \langle x^2, xy^2 \rangle$, we find that

$$\begin{aligned} \langle x^3, xy, y^4 \rangle \cap \langle x^2, xy^2 \rangle &= \langle \operatorname{lcm}(x^3, x^2), \operatorname{lcm}(x^3, xy^2), \ldots, \operatorname{lcm}(y^4, xy^2) \\ &= \langle x^3, x^3y^2, x^2y, xy^2, x^2y^4, xy^4 \rangle \\ &= \langle x^3, x^2y, xy^2 \rangle. \end{aligned}$$

2.5.3 Monomial orderings

In order to define polynomial division in severable variables, we must somehow determine what terms in the polynomial are leading over the other terms. In one variable this is very familiar and natural. We just compare exponents and say that $x^{-1} \leq x^0 = 1 \leq x^1 \leq \cdots \leq x^n$. However, should $x^2y \leq xy^2$ or should it be the other way around? To rectify this ambiguity, we introduce the concept of a monomial ordering.

Definition 21. A **monomial ordering** on $K[x_1, \ldots, x_n]$ is any binary relation $>$ on $\mathbb{Z}^n_{\geq 0}$ satisfying

(i) $>$ is a total (or linear) ordering on $\mathbb{Z}^n_{\geq 0}$,
(ii) If $\alpha > \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma > \beta + \gamma$, and
(iii) $>$ is a well-ordering on $\mathbb{Z}^n_{\geq 0}$.

(Condition (iii) means that every non-empty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under $>$.)

Definition 22 (Lexicographic ordering)**.** Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{lex} \beta$, if, in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the leftmost nonzero entry is positive. We will write

$$x^\alpha >_{lex} x^\beta$$

if $\alpha >_{lex} \beta$.

For example,

(i) $(1, 2, 0) >_{lex} (0, 3, 4)$ since $(1, 2, 0) - (0, 3, 4) = (1, 1, -4)$
(ii) $(3, 2, 4) >_{lex} (3, 2, 1)$ since $(3, 2, 4) - (3, 2, 1) = (0, 0, 3)$
(iii) $(1, 0, \ldots, 0) >_{lex} (0, 1, 0, \ldots, 0) >_{lex} \cdots >_{lex} (0, \ldots, 0, 1)$, so $x_1 >_{lex} x_2 >_{lex} \cdots >_{lex} x_n$

Proposition 1. *The lex ordering on $\mathbb{Z}^n_{\geq 0}$ is a monomial ordering.*

Proof. See [3, p. 57]. □

Definition 23 (Graded lex order)**.** Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grlex} \beta$ if $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$, or $|\alpha| = |\beta|$ and $\alpha >_{lex} \beta$.

Definition 24 (Graded reverse lex order)**.** Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grevlex} \beta$ if $|\alpha| > |\beta|$, or if $|\alpha| = |\beta|$ and the rightmost non-zero entry of $\alpha - \beta \in \mathbb{Z}^n$ is negative.

It is not hard, albeit a bit tedious, to verify that both the *grlex* and *grevlex* orders on $\mathbb{Z}^n_{\geq 0}$ are monomial orderings on $K[x_1, \ldots, x_n]$. Which ordering to choose depends on the particular situation; in some cases the choice is rather arbitrary, while in other cases certain algorithms works better with certain orderings [1]. (Note also that there are many other monomial orderings not covered here.)

Let us illustrate the grevlex ordering with a few examples:

(i) $(4,7,1) >_{grevlex} (4,2,3)$ since $|(4,7,1)| = 12 > 9 = |(4,2,3)|$
(ii) $(1,5,2) >_{grevlex} (4,1,3)$ since $|(1,5,2)| = 8 = |(4,1,3)|$ and $(1,5,2) - (4,1,3) = (-3,4,-1)$
(iii) $(1,0,\ldots,0) >_{grevlex} (0,1,0,\ldots,0) >_{grevlex} \cdots >_{grevlex} (0,\ldots,0,1)$, so $x_1 >_{grevlex} x_2 >_{grevlex} \cdots >_{grevlex} x_n$

Definition 25. Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $K[x_1, \ldots, x_n]$ and let $>$ be a monomial ordering.

(i) The **multidegree** of f is

$$\text{multideg}(f) = \max(\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0)$$

where max is taken w.r.t. $>$.
(ii) The **leading coefficient** of f is

$$\text{LC}(f) = a_{\text{multideg}(f)} \in K.$$

(iii) The **leading monomial** of f is

$$\text{LM}(f) = x^{\text{multideg}(f)}$$

(with coeffeicient 1).
The **leading term** of f is

$$\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f).$$

As an example, let $f = 4xy^2z - 5x^3 + 7x^2z^2$ and let $>$ denote lex order. Then

$$\begin{aligned} \text{multideg}(f) &= (3,0,0), \\ \text{LC}(f) &= -5, \\ \text{LM}(f) &= x^3, \\ \text{and } \text{LT}(f) &= -5x^3. \end{aligned}$$

[1] For example, the grevlex order has a reputation for producing, almost always, the Gröbner bases (see Chapter 3) that are the easiest to compute (this is enforced by the fact that, under rather common conditions on the ideal, the polynomials in the Gröbner basis have a degree that is at most exponential in the number of variables; no such complexity result exists for any other ordering).

We are getting close to start delving into Gröbner bases, but we are missing one major building block which all the previous theory have prepared us for. We will now study a generalised division algorithm designed for multivariate polynomials. It will take some time "getting used to", but we will thoroughly go through several examples to understand the algorithm properly. First let us look at what the theorem actually says.

Theorem 12. *Fix a monomial ordering $>$ on $\mathbb{Z}^n_{\geq 0}$, and let $F = (f_1, ..., f_s)$ be an ordered s-tuple of polynomials in $K[x_1, \ldots, x_n]$. Then every $f \in K[x_1, \ldots, x_n]$ can be written as*

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

where $a_i, r \in K[x_1, \ldots, x_n]$, and either $r = 0$ or r is a K-linear combination of monomials, none of which is divisible by any of $LT(f_1), \ldots, LT(f_s)$. We will call r a remainder of f on division by F. Furthermore, if $a_i f_i \neq 0$, then we have

$$multideg(f) \geq multideg(a_i f_i).$$

Proof. For quite a verbose proof, see [3, pp. 64-66]. □

As promised, we will investigate this algorithm with the help of a few examples. Let us first divide $f = xy^2 + 1$ by $f_1 = xy + 1$ and $f_2 = y + 1$, using lex order with $x > y$.

$$\begin{array}{rl} & a_1: \\ & a_2: \\ xy+1 & \overline{} \\ y+1 & xy^2+1 \end{array}$$

The leading terms $\mathrm{LT}(f_1) = xy$ and $\mathrm{LT}(f_2) = y$ both divides the leading term $\mathrm{LT}(f) = xy^2$. Since f_1 is listed first, we will use it. Thus we divide xy^2 by xy, leaving y, and then subtract $y \cdot f_1$ from f.

$$\begin{array}{rl} & a_1: \quad y \\ & a_2: \\ xy+1 & \overline{} \\ y+1 & xy^2+1 \\ & \underline{-(xy^2+y)} \\ & -y+1 \end{array}$$

Now we repeat the procedure on $-y + 1$. This time we must use f_2 since $\mathrm{LT}(f_1) = xy$ does not divide $\mathrm{LT}(-y + 1) = -y$. We obtain the following.

$$\begin{array}{rl} & a_1: \quad y \\ & a_2: \quad -1 \\ xy+1 & \overline{} \\ y+1 & xy^2+1 \\ & \underline{-(xy^2+y)} \\ & -y+1 \\ & \underline{-(-y-1)} \\ & 2 \end{array}$$

Since $\mathrm{LT}(f_1)$ and $\mathrm{LT}(f_2)$ do not divide 2, the remainder is $r = 2$ and we are done. Thus, we have written $f = xy^2 + 1$ in the form

$$xy^2 + 1 = y \cdot (xy + 1) + (-1) \cdot (y + 1) + 2.$$

Now, let us try a littler trickier example. We shall divide $f = x^2y + xy^2 + y^2$ by $f_1 = xy - 1$ and $f_2 = y^2 - 1$, once again with lexicographic ordering.

$$\begin{array}{rl} & a_1: \quad x + y \\ & a_2: \\ xy - 1 & \overline{\qquad\qquad x^2y + xy^2 + y^2} \\ y^2 - 1 & \end{array}$$

Only $\mathrm{LT}(f_1) = xy$ divides $\mathrm{LT}(f) = x^2y$, so we divide x^2y by xy, leaving x, and then subtract $x \cdot f_1$ from f. Both $\mathrm{LT}(f_1)$ and $\mathrm{LT}(f_2)$ divides $\mathrm{LT}(xy^2 + x + y^2)$, but f_1 is listed first, so we use it, which yields

$$xy^2 + x + y^2 - \frac{xy^2}{xy}(xy - 1) = xy^2 + xy + y^2 - xy^2 + y = x + y^2 + y.$$

Now neither $\mathrm{LT}(f_1)$ nor $\mathrm{LT}(f_2)$ divides $\mathrm{LT}(x+y^2+y) = x$. However, $x+y^2+y$ is *not* the remainder, since $\mathrm{LT}(f_2)$ divides y^2. Thus, if we move x to the remainder, we can continue dividing. To this end, we create a remainder column r where we put the terms belonging to the remainder. If we can divide by $\mathrm{LT}(f_1)$ or $\mathrm{LT}(f_2)$, we continue as usual, and if neither divides, we move the leading term of the intermidate dividend to the remainder column. Thus

$$\begin{array}{rl} & a_1: \quad x + y \\ & a_2: \quad 1 \\ xy - 1 & \overline{\qquad\qquad x^2y + xy^2 + y^2} \\ & \\ y^2 - 1 & \overline{\qquad\qquad -(x^2y - x)} \\ & \overline{\qquad\qquad xy^2 + x + y^2} \\ & \overline{\qquad\qquad -(xy^2 - y)} \qquad\qquad \overline{\qquad\qquad r} \\ & \overline{\qquad\qquad x + y^2 + y} \quad \to \qquad\qquad x \\ & \overline{\qquad\qquad y^2 + y} \\ & \overline{\qquad\qquad -(y^2 - 1)} \\ & \overline{\qquad\qquad y + 1} \quad \to \qquad x + y \\ & \overline{\qquad\qquad 1} \quad \to \quad x + y + 1 \\ & \overline{\qquad\qquad 0} \end{array}$$

Thus the remainder is $x + y + 1$, and we obtain

$$x^2 + y + xy^2 + y^2 = (x + y)(xy - 1) + 1 \cdot (y^2 - 1) + x + y + 1.$$

Note that the remainder is a sum of monomials, none of which is divisible by the leading terms $\mathrm{LT}(f_1)$ or $\mathrm{LT}(f_2)$, which the theorem promised us.

Chapter 3

Gröbner bases

Definition 26. Let $I \subset K[x_1, \ldots, x_n]$ be a monomial ideal. We denote by $\mathrm{LT}(I)$ the set of leading terms of the elements of I. We denote by $\langle \mathrm{LT}(I) \rangle$ the ideal generated by the elements of $\mathrm{LT}(I)$.

Proposition 2. *Let $I \subset K[x_1, \ldots, x_n]$ be an ideal. Then*

(i) $\langle LT(I) \rangle$ *is a monomial ideal.*
(ii) *There are $g_1, \ldots, g_t \in I$ such that $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$.*

Proof. For a proof, se [3, p. 76] □

Theorem 13 (Hilbert basis theorem)**.** *Every ideal $I \subset K[x_1, \ldots, x_n]$ has a finite generating set. That is, $I = \langle g_1, \ldots, g_t \rangle$ for some $g_1, \ldots, g_t \in I$.*

Proof. For a proof, se [3, pp. 76-77] □

Definition 27. Fix a monomial order. A finite subset $G = \{g_1, \ldots, g_t\}$ of a monomial ideal is said to be a **Gröbner basis** if $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle$.

Corollary 13.1. *Fix a monomial order. Then every ideal $I \subset K[x_1, \ldots, x_n]$ other than $\{0\}$ has a Gröbner basis. Furthermore, any Gröbner basis for an ideal I is a basis for I.*

Proof. See [3, p. 77] □

3.1 Properties of Gröbner bases

Proposition 3. *Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner bases for an ideal $I \subset K[x_1, \ldots, x_n]$ and let $f \in K[x_1, \ldots, x_n]$. Then there is a unique $r \in K[x_1, \ldots, x_n]$ with the following two properties.*

(i) *No term of r is divisible by $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$.*
(ii) *There is $g \in I$ such that $f = g + r$.*

Proof. The division algorithm gives $f = a_1 g_1 + \cdots + a_t g_t + r$, where r satisfies (i). We can also satisfy (ii) by setting $g = a_1 g_1 + \cdots + a_t g_t \in I$. To prove uniqueness, suppose that $f = g + r = g' + r'$ satisfy (i) and (ii). Then $r - r' = g' - g \in I$, so that if $r \neq r'$, then $\mathrm{LT}(r - r') \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. By Lemma

9 it follows that $\mathrm{LT}(r - r')$ is divisible by some $\mathrm{LT}(g_i)$, but this is absurd since no term of r, r' is divisible by one of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$. Thus $r - r' = 0$. □

Theorem 14. *Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner bases for an ideal $I \subset K[x_1, \ldots, x_n]$ and let $f \in K[x_1, \ldots, x_n]$. Then $f \in I$ if and only if the remainder on division of f by G is zero.*

Proof. If the remainder is zero, then we have already observed that $f \in I$. Conversely, given $f \in I$, then $f = f+0$ satisfies the two conditions of Proposition 3. It follows that 0 is the reaminder of f on division by G. □

Definition 28. We will write $\bar{f}^F$ for the remainder on division of f by the ordered s-tuple $F = (f_1, \ldots, f_s)$. If F is a Gröbner basis for $\langle f_1, \ldots, f_s \rangle$, then we can regard F as a set (without any particular order) by Proposition 3.

Let us illustrate the definition with an example. Let $F = (x^2y - y^2, x^4y^2 - y^2) \subset K[x, y]$. Using the lex order, we have

$$\overline{x^5y}^F = xy^3$$

since the division algorithm yields

$$x^5y = (x^3 + xy)(x^2y - y^2) + 0 \cdot (x^4y^2 - y^2) + xy^3.$$

Definition 29. Let $f, g \in K[x_1, \ldots, x_n]$ be nonzero polynomials.

(i) If $\mathrm{multideg}(f) = \alpha$ and $\mathrm{multideg}(g) = \beta$, then $\gamma = (\gamma_1, \ldots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i. We call x^γ the **least common multiple** of $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$, written $x^\gamma = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$.

(ii) The **S-polynomial** of f and g is the combination

$$S(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g.$$

Let $f = x^3y^2 - x^2y^3 + x$ and $g = 3x^4y + y^2$ in $R[x, y]$ with the grlex order. Then $\gamma = (4, 2)$ and

$$\begin{aligned} S(f, g) &= \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g \\ &= x \cdot f - (1/3) \cdot y \cdot g \\ &= -x^3y^3 + x^2 - (1/3)y^3. \end{aligned}$$

An S-polynomial is constructed to produce cancellation of leading terms. In fact, the following lemma shows that every cancellation of leading terms among polynomials of the same multidegree results from this cancellation.

Lemma 15. *Suppose we have a sum $\sum_{i=1}^s c_i f_i$, where $c_i \in K$ and $\mathrm{multideg}(f_i) = \delta \in \mathbb{Z}^n_{\geq 0}$ for all i. If $\mathrm{multideg}(\sum_{i=1}^s c_i f_i) < \delta$, then $\sum_{i=1}^s c_i f_i$ is a K-linear combination, of the S-polynomials $S(f_j, f_k)$ for $1 \leq j, k \leq s$. Furthermore, each $S(f_j, f_k)$ has multidegree $< \delta$.*

Proof. See [3, p. 84]. □

Theorem 16 (Buchberger's criterion)**.** *Let I be a polynomial ideal. Then a basis $G = \{g_1, \ldots, g_t\}$ for I is a Gröbner basis for I if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G (listed in some order) is zero.*

Proof. See [3, pp. 85-87]. □

As an example, let $I = \langle y - x^2, z - x^3 \rangle$ of the twisted cubic in $\mathbb{R}^3$. We can check that $G = \{y - x^2, z - x^3\}$ is a Gröbner basis for lex order with $y > z > x$ by considering the S-polynomial

$$S(y - x^2, z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) = -zx^2 + yx^3.$$

Using the division algorithm, we find

$$-zx^2 + yx^3 = x^3(y - x^2) + (-x^2)(z - x^3) + 0,$$

so that $\overline{S(y - x^2, z - x^3)}^{G} = 0$. Thus, by Theorem 16, G is a Gröbner basis for I.

Theorem 17 (Bucberger's algorithm)**.** *Let $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ be a polynomial ideal. Then a Gröbner basis for I can be constructed in a finite number of steps by the following algorithm.*

Algorithm 1 Buchberger's algorithm

```
Input: F = (f_1, ..., f_s)
Output: a Gröbner basis G = (g_1, ..., g_t) for I, with F ⊂ G.
G := F
repeat
    G' := G
    for each pair {p, q}, p ≠ q in G' do
        S := remainder of S(p, q) on division by G'
        if S ≠ 0 then
            G := G ∪ {S}
until G = G'
```

Proof. See [3, p. 90] □

We should point out at this stage that this is only a rudimentary version of Buchberger's algorithm. We can eliminate some unnecessary generators by using the following result.

Lemma 18. *Let G be a Gröbner basis for the polynomial ideal I. Let $p \in G$ be a polynomial such that $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\}) \rangle$. Then $G - \{p\}$ is also a Gröbner basis for I.*

Proof. We know that $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(I) \rangle$. If $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\}) \rangle$, then we have $\mathrm{LT}(G - \{p\}) \rangle = \mathrm{LT}(G) \rangle$. By definition, it follows that $G - \{p\}$ is also a Gröbner basis for I. □

By adjusting constants to make all leading coefficients 1 and removing any p with $\mathrm{LT}(p)\rangle \in \mathrm{LT}(G - \{p\})\rangle$ from G, we arrive at what we call a *minimal* Gröbner basis for I.

Definition 30. A **minimal Gröbner basis** for a polynomial ideal I is a Gröbner basis for I such that

(i) $\mathrm{LC}(p) = 1 \ \forall \ p \in G$
(ii) $\mathrm{LT}(p) \neq \langle \mathrm{LT}(G - \{p\})\rangle \ \forall \ p \in G$.

The last condition is equivalent to requiring that $\mathrm{LM}(g_i)$ does not divide $\mathrm{LM}(g_j)$ for all $g_i, g_j \in G, i \neq j$. As an example of a minimal Gröbner basis, consider for example the ring $K[x, y]$ with grlex order, and let

$$I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle.$$

A computation gives the Gröbner basis

$$\begin{aligned} f_1 &= x^3 - 2xy \\ f_2 &= x^2y - 2y^2 + x \\ f_3 &= -x^2 \\ f_4 &= -2xy \\ f_5 &= -2y^2 + x. \end{aligned}$$

First, we multiply the generators by suitable constants to make all leading coefficients equal to 1.

$$\begin{aligned} \tilde{f}_1 &= x^3 - 2xy \\ \tilde{f}_2 &= x^2y - 2y^2 + x \\ \tilde{f}_3 &= x^2 \\ \tilde{f}_4 &= xy \\ \tilde{f}_5 &= y^2 - (1/2)x. \end{aligned}$$

Then note that $\mathrm{LT}(\tilde{f}_1) = x^3 = x \cdot \mathrm{LT}(\tilde{f}_3)$, so we can dispense with $\tilde{f}_1$ in the minimal Gröbner basis. Similarily, since $\mathrm{LT}(\tilde{f}_2) = x^2y = x \cdot \mathrm{LT}(\tilde{f}_4)$, we can also make rid of $\tilde{f}_2$. There are no more cases where the leading term of one generator divides the leading term of another generator. Hence,

$$\tilde{f}_3 = x^2, \tilde{f}_4 = xy, \tilde{f}_5 = y^2 - (1/2)x$$

is a minimal Gröbner basis for I. Unfortunately, a given ideal can have several minimal Gröbner bases. As an illustration, in the ideal I above, one can easily check that

$$\hat{f}_3 = x^2 + axy, \hat{f}_4 = xy, \hat{f}_5 = y^2 - (1/2)x$$

is also a minimal Gröbner basis for I, where $a \in K$ is an arbitrary constant. Thus there may exist infinitely many minimal Gröbner bases for the same ideal. In order to pick a unique minimal Gröbner basis which also exhibits the nicest possible properties, we introduce the following term.

Definition 31. A **reduced Gröbner basis** for a polynomial ideal I is a Gröbner basis G for I such that

(i) $\mathrm{LC}(p) = 1$ for all $p \in G$.
(ii) For all $p \in G$, no monomial of p lies in $\langle \mathrm{LT}(G - \{p\})$.

Reuced Gröbner bases exhibits the following nice property.

Proposition 4. *Let $I \neq \{0\}$ be a polynomial ideal. Then, for a given monomial order, I has a unique reduced Gröbner basis.*

Proof. See [3, pp. 92-93] □

Chapter 4

Algebraic coding theory

In this chapter we will introduce the basic concepts of algebraic coding theory, which essentially are techniques for reliable delivery of digital data over noisy information channels. We will then combine the results from Chapter 3 on Gröbner bases with the theory of linear (and especially cyclic) error correcting codes, and eventually prove some interesting properties that arise from this fusion. Especially we will see how Gröbner bases can be used to construct an effective representation of an encoding function, and how these Gröbner bases can be read directly from the generating matrix of certain ideals. But let's begin with a primer on algebraic coding theory.

Definition 32. A **word** is a string of some fixed length k, using symbols from a fixed alphabet. All information that is to be transmitted is divided into words, and all encoded messages are in turn divided into **codewords** of a fixed block length n, using symbols from thte same alphabet as the original words.

In order to detect/correct errors in the received transmission, some redundancy must be introduced in the encoding process, so we will always have $n > k$. Since this thesis is about a practical application in digital communication, it might be useful to consider the alphabet $\{0, 1\}$ and identify this alphabet with the finite field $\mathbb{F}_2$. But the constructions we will present are valid with an arbitrary finite field $\mathbb{F}_q$.

Definition 33. The **encoding** of a string from the message is a one-to-one function $E\colon \mathbb{F}_q^k \to \mathbb{F}_q^n$. The image $C = E\left(\mathbb{F}_q^k\right) \subset \mathbb{F}_q^n$ is called **the set of codewords** or simply **the code**.

Definition 34. The **decoding** of a string from the encoded message can be viewed as a function $D\colon \mathbb{F}_q^n \to \mathbb{F}_q^k$ such that $D \circ E$ is the identity on $\mathbb{F}_q^k$.

Remark. In real-world applications the decoder will typically also return something like an error value in certain situations [4, p. 460].

Definition 35. A code is called a **linear code** if the set of codewords C forms a vector subspace of $\mathbb{F}_q^n$ of dimension k.

In the case of linear codes, we may use a linear mapping, with image C, as our encoding function $E\colon \mathbb{F}_q^k \to \mathbb{F}_q^n$.

Definition 36. The matrix of E w.r.t the standard basis in the domain and target is called the **generator matrix** G corresponding to E. We write G as a $k \times n$ matrix and view the strings in $\mathbb{F}_q^k$ as row vectors w in G.

The encoding operation is thus akin to matrix multiplication of a row vector on the right by the generator matrix G, and the rows of G form a basis for C.

Definition 37. The subspace C can be described as the set of solutions of a system of $n-k$ linear independent system of equations in n variables. The matrix of coefficients of such a system is called a **parity check matrix**.

Let us illustrate this with an example. Consider the following linear code C with $n = 4, k = 2$ given by the generator matrix

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

There are exactly four elements in C:

$$\begin{aligned} (0,0)G &= (0,0,0,0), & (1,0)G &= (1,1,1,1), \\ (0,1)G &= (1,0,1,0), & (1,1)G &= (0,1,0,1). \end{aligned}$$

One can easily check that

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

is a parity check matrix for C by verifying that $xH = 0$ for all $x \in C$.

We need a metric to describe how close elements of $\mathbb{F}_q^n$ are, and for this we will use the following definition.

Definition 38. Let $x, y \in \mathbb{F}_q^n$. Then the **Hamming distance** between x and y is defined to be

$$d(x,y) = \|\{i, 1 \leq i \leq n \colon x_i \neq y_i\}\|,$$

i.e the number of positions where the elements differ.

For example, let $x = (0,0,1,1,0)$ and $y = (1,0,1,0,0)$ in $\mathbb{F}_2^5$. Then $d(x,y) = 2$ since only the first and fourth bits in x and y differ.

Definition 39. Let $\bar{0}$ denote the zero vector in $\mathbb{F}_q^n$ and let $x \in \mathbb{F}_q^n$ be arbitrary. Then $d(x, \bar{0})$, the number of nonzero components in x, is called the **Hamming weight**, or simply the **weight** of x, and is denoted by $\mathrm{wt}(x)$.

Even though the Hamming distance is simple to describe and understand, it provides a very useful tool to measure the error-correcting capabilities of a code. Suppose namely that every pair of distinct codewords x and y in a code $C \subset \mathbb{F}_q^n$ satisfies $d(x,y) \geq d$ for some integer $d \geq 1$. If a codeword x is transmitted and errors are introduced, we can view the received codeword as $z = x + e$, for some nonzero error vector e. If $\mathrm{wt}(e) = d(x,z) \leq d-1$, then under our hypothesis z is *not* another codeword. Hence any error vector of weight at most $d-1$ can be *detected*.

Definition 40. The **minimum distance** is defined as

$$d = \min\{d(x, y) \colon x \neq y \in C\}.$$

Proposition 5. *Let C be a code with minimum distance d. All error vectors e of weight $\mathrm{wt}(e) \leq d - 1$ can be detected. Moreover, if $d \leq 2t + 1$, then all error vectors e of weight $\mathrm{wt}(e) \leq t$ can be corrected by nearest neighbour decoding, which is given by*

$$\min_{y \in C} d(x + e, y),$$

where $d(x, y)$ is the Hamming distance. [4, p. 462, Proposition 2.1]

4.1 Cyclic codes

Definition 41. A **cyclic code** is a linear code with the property that the set of codewords is closed under cyclic permutation of the components of vectors in $\mathbb{F}_q^n$.

This is best understood by an example. From hereon, let $[n, k, d]$ denote a linear code with block length n, dimension k and minimum distance d. In $\mathbb{F}_2^4$, consider the $[4, 2, 2]$ code C with generator matrix

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

As we have seen before, $|C| = 4$, and the codewords $(1, 1, 1, 1) = (1, 0)G$ and $(0, 0, 0, 0) = (0, 0)G$ are both invariant under all cyclic permutations. The codewords $(1, 0, 1, 0) = (0, 1)G$ is not itself invariant; shifting one position to the left (or right) results in $(0, 1, 0, 1)$. However, $(0, 1, 0, 1) = (1, 1)G$ is indeed another codeword in C. Similarily, shifting $(0, 1, 0, 1)$ one place to the left (or right) returns the codeword $(1, 0, 1, 0)$ again. It follows that the set C is closed under all cyclic permutations, and thus C is a cyclic code.

Let us now use the isomorphism between $\mathbb{F}_q^n$ and the vector space of polynomials of degree at most $n - 1$ with coefficients in $\mathbb{F}_q$,

$$(a_0, a_1, \ldots, a_{n-1}) \leftrightarrow a_0 + a_1 x + \cdots + a_{n-1} x^{n-1},$$

and identify a cyclic code C with the corresponding set of polynomials of degree at most $n - 1$. Then a cyclic shift to the right, sending $(a_0, a_1, \ldots, a_{n-1})$ to $(a_{n-1}, a_0, \ldots, a_{n-2})$, corresponds to the multiplication

$$x \cdot (a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) \pmod{x^n - 1}.$$

Proposition 6. *Let $R = \mathbb{F}_q[x]/\langle x^n - 1 \rangle = \{p(x) \in \mathbb{F}_q \pmod{x^n - 1}\}$. A vector subspace $C \subset R$ is a cyclic code if and only if C is an ideal in the quotient ring R.*

The ring R shares a nice property with $\mathbb{F}_q[x]$.

Proposition 7. *Each ideal $I \subset R$ s.t. $I \neq \{0\}$ is principal, generated by the coset of a single polynomial g of degree $n - 1$ or less. Moreover, g is a divisor of $x^n - 1$ in $\mathbb{F}_q[x]$.*

Proof. For a proof, see [4, p. 469]. □

Definition 42. The polynomial g in Proposition 7 is called a **generator polynomial** for the cyclic code.

We will study a special class of cyclic codes, called Reed-Müller codes, which are interesting because of their nice decoding properties. We will define Reed-Müller codes via Boolean polynomials and Boolean functions. There are however several other ways to define them.

Definition 43. A **Boolean function** of m variables is a function

$$f(x_1, \ldots, x_m) \colon \mathbb{F}_2^m \to \mathbb{F}_2.$$

A **Boolean monomial** p in variables $(x_1, \ldots, x_m)$ is an expression of the form $x_1^{r_1} x_2^{r_2} \cdots x_m^{r_m}$ where $r_i \in \mathbb{N}_{\geq 0}$ and $1 \leq i \leq m$.

The reduced form of p is obtained by applying the rule $x_i^2 = x_i$ until the factors are distinct.

Definition 44. A **Boolean polynomial** is an $\mathbb{F}_2$-linear combination of Boolean monomials.

Definition 45. Let $0 \leq r \leq m, r, m \in \mathbb{N}$. Then the r^{th} order **Reed-Müller code** RM(r,m) is the set of all binary strings of length 2^m associated with the Boolean polynomials of degree at most r.

Remark. The 0^{th} order Reed-Müller code is just the repetition code of length 2^m. This means that the set of codewords is

$$C = \{\underbrace{1 \ldots 1}_{2^m}, \underbrace{0 \ldots 0}_{2^m}\},$$

and a message would be encoded such that each bit of the message is replaced by its corresponding codeword. For example, if $m = 2$ so that $2^m = 4$, then the message 101 would be encoded as $E(101) = 111100001111$. It also follows that the 1^{st} order Reed-Müller codes $\text{RM}(1, m)$ are defined recursively by

(i) $\text{RM}(1, 1) = \{00, 01, 10, 11\}$
(ii) for $m > 1, \text{RM}(1, m) = \{(\mathbf{u}, \mathbf{u}), (\mathbf{u}, \mathbf{u} + \mathbf{1}) \colon u \in \text{RM}(1, m-1)\}$, where $\mathbf{1} = (\underbrace{1 \cdots 1}_{m})$ and the addition is binary.

Thus, for instance

$$\text{RM}(1, 2) = \{0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100\}$$

and

$$\text{RM}(1, 3) = \begin{array}{c} \{00000000, 00001111, 01010101, 01011010, \\ 10101010, 10100101, 11111111, 11110000, \\ 00110011, 00111100, 01100110, 01101001, \\ 10011001, 10010110, 11001100, 11000011\} \end{array}$$

The following theorem gives a recursive definition of Reed-Müller codes.

Theorem 19. *Let r, m be integers s.t. $0 \leq r \leq m$. The $(r+1)^{\text{th}}$ order Reed-Müller code of length 2^{m+1} is*

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

If $G(r,m)$ is the generator matrix of the Reed-Müller code $\mathrm{RM}(r,m)$, then

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

is the generator matrix of $\mathrm{RM}(r+1, m+1)$.

As an example, consider the generator matrix for $\mathrm{RM}(1,1)$.

$$GM(1,1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Now, let us calculate the generator matrix for $\mathrm{RM}(1,5)$.

$$GM(1,5) = \begin{bmatrix} G(1,4) & G(1,4) \\ 0 & G(0,4) \end{bmatrix}.$$

Note that $G(0,4)$ is just the generator matrix for the repetition code of length 2^4. Thus we only need to compute the generator matrix $G(1,4)$.

$$GM(1,4) = \begin{bmatrix} G(1,3) & G(1,3) \\ 0 & G(0,3) \end{bmatrix}$$

which leads to the calculation of $G(1,3), G(1,2)$ and finally $G(1,1)$ which we already know. Thus,

$$GM(1,2) = \begin{bmatrix} G(1,1) & G(1,1) \\ 0 & G(0,1) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

so

$$GM(1,3) = \begin{bmatrix} G(1,2) & G(1,2) \\ 0 & G(0,2) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},$$

$$GM(1,4) = \begin{bmatrix} G(1,3) & G(1,3) \\ 0 & G(0,3) \end{bmatrix} = \begin{bmatrix} 1111 & 1111 & 1111 & 1111 \\ 0101 & 0101 & 0101 & 0101 \\ 0011 & 0011 & 0011 & 0011 \\ 0000 & 1111 & 0000 & 1111 \\ 0000 & 0000 & 1111 & 1111 \end{bmatrix}$$

and finally,

$$G(1,5) = \begin{bmatrix} G(1,4) & G(1,4) \\ 0 & G(0,4) \end{bmatrix} =$$

$$= \begin{bmatrix} 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 \\ 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 \\ 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 \\ 0000 & 1111 & 0000 & 1111 & 0000 & 1111 & 0000 & 1111 \\ 0000 & 0000 & 1111 & 1111 & 0000 & 0000 & 1111 & 1111 \\ 0000 & 0000 & 0000 & 0000 & 1111 & 1111 & 1111 & 1111 \end{bmatrix} = \begin{bmatrix} \mathbf{1} \\ v_5 \\ v_4 \\ v_3 \\ v_2 \\ v_1 \end{bmatrix}.$$

4.2 Construction of reduced Gröbner bases

In this section we will construct a reduced Gröbner basis, which will later be used to define a class of codes which contain the primitive Reed-Müller codes. Let $\mathbb{K}$ be a field and let $\mathbb{K}[x] = K[x_1, \ldots, x_n]$ be a polynomial ring over $\mathbb{K}$. Take a nonempty subset $S \in \mathbb{Z}^n_{\geq 0}$ and consider the ideal $I = I(S)$ generated by the set

$$\{\eta(\mathbf{a})\colon \mathbf{a} \in S\},$$

where

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

Let $M = M(S)$ be the set of n-tuples $\mathbf{a} \in S$ that are minimal w.r.t. componentwise natural $\leq$-ordering. In particular, if we choose $S = \mathbb{Z}^n_{\geq 0}$, then the set of minimal elements will be $M(S) = \{0\}$ and $I(S) = \mathbb{K}[x]$ since $1 \in I(S)$. Secondly, if $S = \mathbb{N} \setminus \{0\}$, then $M(S)$ consists of the unit vectors and the ideal $I(S)$ is generated by the terms $x_j - 1, 1 \leq j \leq n$. The following theorem constructs a reduced Gröbner basis for the ideal.

Theorem 20. *For any monomial ordering on $\mathbb{K}[x]$, the ideal $I = I(S)$ in $\mathbb{K}[x]$ has the reduced Gröbner basis*

$$G = \{\eta(\mathbf{a})\colon \mathbf{a} \in M\}.$$

The ideal of leading terms of the ideal I equals $\langle\{x^{\mathbf{a}}\colon \mathbf{a} \in M\}\rangle$.

Proof. For a proof, se [8, pp. 40-43]. □

Note that for each monomial ordering on $\mathbb{Z}^n_{\geq 0}$, the leading term of $\eta(\mathbf{a}), \mathbf{a} \in \mathbb{Z}^n_{\geq 0}$ is $x^{\mathbf{a}}$. Indeed, each monomial in $\eta(\mathbf{a})$ is of the form $x^{\mathbf{b}}$ for some $\mathbf{b} \in \mathbb{Z}^n_{\geq 0}$ with $\mathbf{b} \leq \mathbf{a}$. Thus $\mathbf{a} = \mathbf{b} + \mathbf{c}$ for some $\mathbf{c} \in \mathbb{Z}^n_{\geq 0}$. But $\mathbf{0} \leq c$ and so $\mathbf{b} \leq \mathbf{b} + \mathbf{c} = \mathbf{a}$.

4.3 Variants of Reed-Müller codes

It has been established by Berman [1] that binary Reed-Müller codes correspond to powers of the radical of the quotient ring

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

In this section we will explore a strong link between the theory of Gröbner bases and cyclic codes, defined in terms of ideals in quotient rings. Then we give an outline of a general encoding process for a cyclic code via Gröbner bases. Lastly, we present some variants of Reed-Müller codes and their decoding process.

4.3.1 Encoding linear codes using Gröbner bases

Consider the quotient ring R of the form

$$R = \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^q - 1, \ldots, x_n^q - 1\rangle.$$

As an $\mathbb{F}_q$-algebra, R is isomorphic to the group algebra $\mathbb{F}_q G$ of an elementary abelian q-group G of order q^n. As an $\mathbb{F}_q$-vector space, R is isomorphic to the space $\mathbb{F}_q^{q^n}$. It is clear that $H = \{x_1^q - 1, \ldots, x_n^q - 1\}$ is a Gröbner basis for the

ideal it generates, w.r.t. all monomial orders, since all leading monomials of the generators are relatively prime, and hence the S-polynomial goes to zero for any two generators, which proves that H is indeed a Gröbner basis.

Thus we can compute the standard representation for the elements of R by applying the division algorithm in $\mathbb{F}_q[x_1, \ldots, x_n]$ and computing remainder w.r.t. H. Thus the representation of the elements of R are given by the polynomials whose degree in x_i is at least $q - 1 \leq i \leq n$. These polynomials are called standard forms of the elements of R. Now 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 $\mathbb{F}_q[x_1, \ldots, x_n]$. 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 $\mathbb{F}_q[x_1, \ldots, x_n]$ is given as

$$J = \langle f_1, \ldots, f_m \rangle + \langle x_1^q - 1, \ldots, x_n^q - 1 \rangle.$$

The code C equals $J/\langle x_1^q - 1, \ldots, x_n^q - 1 \rangle$, and thus by the standard isomorphism theorems there is an $\mathbb{F}_q$-algebra isomorphism

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

If we represent the ambient space R by the set of polynomials in standard form, then the ideal C can be viewed as a linear code in R. An $\mathbb{F}_q$-basis of R is given by all monomials in standard form that is all monomials in which x_i appears to a power of at most $p - 1, 1 \leq i \leq p - 1$. The ambient space R has dimension q^n and so, by definition, the code C has length q^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 given by the number of involved monomials in standard form.

Given a monomial ordering on $\mathbb{F}_q[x_1, \ldots, x_n]$ and a Gröbner basis G for the ideal J, we may use the following theorem to determine whether an element of R is a codeword or not.

Proposition 8. *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 Gröbner basis for J yields a unique remainder (in standard form). Since we have established that $R/C \cong \mathbb{F}_q[x_1, \ldots, x_n]/J$, it follows that this remainder is zero if and only if $f \in C$. □

The following proposition gives the parameters of the considered code.

Proposition 9. *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 $\mathbb{F}_q[x_1, \ldots, x_n]$ can be divided by the Gröbner basis G of J such that the remainder is a linear combination of standard monomials. These monomials are linearly independent in $\mathbb{F}_q[x_1, \ldots, x_n]/J$. Thus, since $R/C \cong \mathbb{F}_q[x_1, \ldots, x_n]/J$, 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. □

We have thus proved that the information components of C are the coefficients of the non-standard monomials for J, while the parity check components of C are the coefficients of the standard monomials for J. This extra structure of the code induced bt a reduced Gröbner basis G for the ideal J provides us with a compact encoding function.

Proposition 10. *If w is an information word given as an $\mathbb{F}_p$-linear combination of non-standard monomials for J, then $w - \bar{w}^G$ is a codeword in C.*

Proof. The polynomials w and $\bar{w}^G$ are in standard form. The difference $w - \bar{w}^G$ lies in J. As this difference is in standard form it belongs to the code C. □

4.3.2 Variants of primitive Reed-Müller codes

In this section we will apply some of the results we have recently disucssed. Consider the ideal $J(S)$ in the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_n]$ given as

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

and the corresponding code $C(S)$ defined as $J(S)/\langle x_1^q - 1, \ldots, x_n^q - 1 \rangle$. 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 $a \in S'$ that are minimal w.r.t. the component-wise natural $\leq$-ordering. Henceforth we assume that $S' \neq \emptyset$. By Theorem 20, we obtain the following result.

Corollary 20.1. *The set $G = \{\eta(\mathbf{a}) \colon \mathbf{a} \in M'\}$ forms a reduced Gröbner basis for the ideal $J(S')$ and the corresponding ideals of leading terms equals*

$$\langle \{x^a \colon \mathbf{a} \in M'\} \rangle.$$

The main properties of the code $C(S')$ may be summarised as follows.

Theorem 21. *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 $\eta(\mathbf{a})$ for which there is an element $\mathbf{m} \in M'$ such that $\mathbf{m} \leq \mathbf{a}$, and minimum distance d is given by the minimum Hamming weight of the generators $\eta(\mathbf{m})$, where $\mathbf{m} \in M'$. The information components of the code $C(S')$ are the coefficients of the monomials in the set $\{x^a \colon \exists\ \mathbf{m} \in M', \mathbf{m} \leq \mathbf{a}\}$.*

Proof. First, the set $\{\eta(\mathbf{a}) \colon \mathbf{a} \in P^n\}$ is linearly independent [1, 2]. By definition, each codeword $c \in C(S')$ can be written, according to the Gröbner basis, as follows.

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

where $f_{\mathbf{a}}$ 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 $x^{\mathbf{a}}$ is given as a linear combination of elements of the form $\eta(\mathbf{b})$, where $\mathbf{b} \in P^n$. However, $\eta(\mathbf{a})\eta(\mathbf{b}) = \eta(\mathbf{a} + \mathbf{b})$ and thus the codeword c can be written as a linear combination of elements $\eta(\mathbf{a})$, where $\mathbf{a} \in S'$. The result on the dimension follows.

Second, the code C is visible in the sense that the minimum distance equals the minimum Hamming weight if its generators $\eta(\mathbf{a})$, where $\mathbf{a} \in S'$ [1, 2, 9]. But

for each generator $\eta(\mathbf{a})$ with $\mathbf{a} \in S'$, there is a generator $\eta(\mathbf{m})$ with $\mathbf{m} \in M'$ such that $\mathbf{m} \leq \mathbf{a}$; that is, $\eta(\mathbf{a})$ is divisible by $\eta(\mathbf{m})$. Thus the minimum Hamming weight is attained by some generator $\eta(\mathbf{m})$ with the property that $m \in M'$.

Finally, the information positions of $C(S')$ are given by the non-standard monomials, which by definition correspond to the monomials in the ideal of leading terms, $\langle \mathrm{LT}(I) \rangle$. But by Corollary 20.1, this ideal is generated by the monomials $x^{\mathbf{a}}, \mathbf{a} \in M'$, and the result follows. □

The considered class of codes contain the so called primitive Reed-Müller codes. To see this, put $N = n(p-1)$ and consider the set $S_l = \{\mathbf{a} \in P^n \colon \sum_{i=1}^n a_i \geq l\}, 0 \leq l \leq N$. The associated code $C(S_l)$ is called the primitive Reed-Müller code of order $N - l$.

For example,
The code $C(S_0)$ is the full code R.
The code $C(S_1)$ is the radicala of R, $\sqrt{R}$.
The code $C(S_N)$ is the constant-weight code [1, 2].
The corresponding se of minimal elements is $M(S_l) = \{\mathbf{a} \in P^n \colon \sum_{i=1}^n a_i = l\}, 0 \leq l \leq N$. By Corollary 20.1, the set $\{\eta\mathbf{a} \colon \sum_{i=1}^n a_i = l\}$ is a reduced Gröbner basis for the ideal $J(S_l), 0 \leq l \leq N$.

4.4 Linear codes of monomial ideals

Definition 46. A **binomial ideal** is an ideal generated by a polynomial with at most two terms.

Their structure can be interpreted directly from their generators, a very nice property. Another interesting class of polynomial ideals are the toric ideals, which are prime ideals with a generating set of binomials. In this section we will relate 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 Gröbner basis for the corresponding ideal. Moreover, minimal generators are also described for the binomial ideal.

4.4.1 Gröbner basis of the ideal $I_{A,P}$

Recall that a binomial in a polynomial ring $K[x_1, \ldots, x_n]$ is a difference of two monomials, say $x^a - x^b$, where $a, b \in \mathbb{Z}^n_{\geq 0}$. The special form of their generators makes it possible to tackle problems like computation of Gröbner bases and primary decomposition in much easier ways and helps in generating effective algorithms for better understanding of the structure. Some basic results about binomial ideals are given in the following proposition.

Proposition 11. *let $>$ be a term order on $K[x_1, \ldots, x_n]$ and let $I \subseteq K[x_1, \ldots, x_n]$ be a binomial ideal. Then*

(i) *The reduced Gröbner basis G of I w.r.t. $>$ consists of binomials.*
(ii) *The elimination ideal $I \cap K[x_1, \ldots, x_r]$ 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 with A is

$$I_A = \langle x^a - x^b \colon Aa = Ab, a, b \in \mathbb{Z}^n_{\geq 0} \rangle.$$

Definition 47. The zero set of I_A in affine n-space is called the **affine toric variety** defined by I_A [6]. If all columns of A have the same coordinate sum, then the ideal I_A is homogenous and defines a **projective toric variety**.

The following proposition describes the form of generators for the l^{th} power of a toric ideal.

Proposition 12. *Let $\mathbb{F}$ be a field and let A be a matrix in $\mathbb{Z}^{m \times n}_{\geq 0}$. The toric ideal I_A in $\mathbb{F}_q[x_1, \ldots, x_n]$ is generated by pure binomials,*

$$I_A = \langle x^{\alpha^+} - x^{\alpha^-} : Aa^+ = Aa^-, \gcd(x^{\alpha^+}, x^{\alpha^-}) = 1 \rangle.$$

Let $l \geq 1$ be an integer. The l^{th} power of I_A is generated by elements of the form

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

where $\alpha_i \in \mathbb{Z}^n_{\geq 0}, Aa_i^+ = Aa_i^-$, and $\gcd(x^{\alpha_i^+}, x^{\alpha_i^-}) = 1$.

Proof. For a proof, see [8, pp. 52-53]. □

We associate with the toric ideal I_A in $\mathbb{F}_q[x_1, \ldots, x_n]$ the binomial ideal

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

This ideal is clearly not toric, since it is not a prime as the polynomials $x_i^P, 1 \leq i \leq n$, are reducible. In order to utilise the structure of toric ideals for the purpose of constructing linear codes, we need to study them from the context of finite fields. To this end, we consider the **saturation** of an ideal I in $\mathbb{F}_q[x_1, \ldots, x_n]$, given as

$$\bar{I} = \{ f \in \mathbb{F}_q[x_1, \ldots, x_n] \colon x_i^m \cdot f \in I \text{ for some } m \text{ and all } i \}.$$

It is clear that $\bar{I}$ is an ideal, and we have $I \subseteq \bar{I}$ and $\bar{\bar{I}} = \bar{I}$. Moreover, for any ideals I and J in $\mathbb{F}_q[x_1, \ldots, x_n]$, $\bar{I} + \bar{J} = \overline{I + J}$. As an example, if $I = \langle fx_1, \ldots, fx_n \rangle$, then $\bar{I} = \langle f \rangle$. The following proposition establishes an equality betweeen a general toric ideal and the toric ideal defined over a field.

Proposition 13. *Let $\mathbb{F}$ be a field, let p be a prime number, and let A be a $d \times n$ matrix with non-negative integral entries. The ideal $I_{A,P}$ in $\mathbb{F}_q[x_1, \ldots, x_n]$ equals the ideal*

$$\begin{aligned} J_{A,P} = \langle x^{a'} - x^{b'} \colon Aa' \equiv Ab' \mod p, a', b' \in \underline{p-1}^n, \gcd(x^{a'}, x^{b'}) = 1 \rangle \\ + \langle x_i^p - 1 \colon 1 \leq i \leq n \rangle. \end{aligned}$$

Proof. For a proof, see [8, pp. 53-54]. □

As an illustrative example, consider the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

The toric ideal I_A in $\mathbb{F}_2[x]$ has the reduced Gröbner 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 non-prime ideal $I_{A,2}$ in $\mathbb{F}_2[x]$ has the reduced Gröbner basis

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

As we can see, we get a different set of generators when we extend a toric to a non-prime ideal.

4.4.2 Reduced Gröbner basis of I_C

In this section we provide a reduced Gröbner basis to each binomial ideal associated with a linear code. The associated monomial ordering is rather arbitrary and only requires that any monomial containing one of the information symbols is larger than any monomial containing only check parity symbols. We will also show that Gröbner bases for linear codes provides a very compact representation of the encoding function. The following result shows that for monomial ordering the reduced Gröbner basis for an ideal corresponding to a code can be constructed directly from its generator matrix.

Reconsider the ideal associated with the code C as

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

where each element $c \in \mathbb{F}_p^n$ is considered as an integral vector in the monomial x^c. Henceforth, 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 i^{th} row of the matrix A over $\mathbb{F}_p, 1 \leq i \leq k$.

Theorem 22. *Given a monomial ordering on $\mathbb{F}_q[x_1, \ldots, x_n]$ such that*

$$x_1 > \cdots > x_n,$$

then the binomial ideal I_C has the reduced Gröbner basis

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

Proof. By definition, the elements in G lie in the idel I_C. Conversely, let $x^c - x^d$ be an element in I_C with $c - d \in C$. The reduction of $x^c - xd$ w.r.t. G results in another binomial $x^l - x^m$, where $l = c_1a_1, \ldots, c_ka_k + c', m = d_1a_1, \ldots, d_ka_k + d', c' = (0, \ldots, 0, c_{k+1}, \ldots, c_n)$, 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 zeroes 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 to 0 by G.

Continuing, 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-polynomial of the elements in G. First, let $1 \leq i < j \leq k$. We have $S(x_i - x^{a_i}, x_j^{a_j}) = x_i x^{a_j} - x_j x^{a_i}$. Division by G yields

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

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. Finally, let $1 \leq i \leq k$ and $k+1 \leq j \leq n$. We have $S(x_j - x^{a_i}, x_j^p - 1) = x_i - x_j^p x^{a_i}$. Division by G yields

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

It follows that the set G is a Gröbner basis for the ideal I_C, and it is clear that G is a reduced Gröbner basis. □

The above theorem illustrates the fact that the reduced Gröbner basis for the ideal I_C can be read directly from its generator matrix. The extra structure of the linear code C given by a reduced Gröbner basis for the idel I_C provides a compact encoding procedure. An immediate consequence of Theorem 22 is a systematic encoding algorithm for linear codes using division w.r.t. a Gröbner basis, and by this theorem the binomial ideal I_C has the associated initial ideal

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

Theorem 23. *Let C be an $[n, k]$ code over $\mathbb{F}_p$, and let G be the reduced Gröbner basis for C given in (5.5). Then*

(i) *The information components are given by the non-standard monomials for I_C in which each x_i appears to a power of at most $p - 1, 1 \leq i \leq n$.*

(ii) *The parity check components are provided by the standard monomials for I_C in which each x_i appears to a power of at most $p - 1, 1 \leq i \leq n$.*

(iii) *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 G by x^w and form $E(w) = (x^w - 1) - \overline{x^w - 1}^G$. 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 the Gröbner basis G by $x^w - 1$ gives

$$\overline{x^w - 1}^G = \overline{x^{w_1 a_1 + \cdots + w_k a_k} - 1}^G = x^{w_1 a_1 + \cdots + w_k a_k} - 1,$$

where the exponent in the last binomial is computed over $\mathbb{F}_p$. It follows that the remainder only involves parity check components so that the information components are not changed in the process of computing the remainder. The encoded binomial

$$E(w) = (x^w - 1) - \overline{x^w - 1}^G = x^w - x^{w_1 a_1 + \cdots + w_k a_k}$$

is an elemet of the ideal I_C and represents the codeword wG. Thus the reduction of w by the Gröbner 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 thesis 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 Gröbner basis for the ideal I_C, and we have shown that this basis can simply be read directly from the generator matrix.

Bibliography

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

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

[3] Cox, D., Little, J., O'Shea, D. *Ideals, varieties and algorithms.* (Springer, 2007).

[4] Cox, D., Little, J., O'Shea, D. *Using algebraic geometry.* (Springer, 2005).

[5] Fröberg, R. *An Introduction to Gröbner bases.* (Wiley, 1997).

[6] Fulton, W. *Introduction to toric varieties.* (Princeton Univ Pr, 1993). **131**.

[7] Lazard, D. *Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations.* (Computer Algebra. Lecture Notes in Computer Science 162, 1983), pp. 146–156.

[8] Saleemi, M. (2012). *Coding Theory via Groebner Bases* (Doctoral dissertation). Institute for Security in Distributed Applications, Technical University of Hamburg.

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

Index