Algebraic Codes over Max-Min Algebra

By
Asra Riaz
186-FBAS/MSMA/F14

Department of Mathematics & Statistics
Faculty of Basic & Applied Sciences
International Islamic University, Islamabad
Pakistan
2016

MS

512

ASA

1. Maxima amd minima

2. Algebra

Algebraic Codes over Max-Min Algebra

By

Asra Riaz

Supervised by

Dr. Sajida Kousar

Department of Mathematics & Statistics
Faculty of Basic & Applied Sciences
International Islamic University, Islamabad
Pakistan
2016

Algebraic Codes over Max-Min Algebra

By
Asra Riaz

A Dissertation
Submitted in the Partial Fulfillment of the
Requirements for the Degree of
MASTER OF SCIENCE
IN
MATHEMATICS

Supervised by
Dr. Sajida Kousar

Department of Mathematics & Statistics
Faculty of Basic & Applied Sciences
International Islamic University, Islamabad
Pakistan
2016

Certificate

Algebraic Codes over Max-Min Algebra

By

Asra Riaz

A DISSERTATION SUBMITTED IN THE PARTIAL FULFILLMENT OF THE

REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN MATHEMATICS

We accept this dissertation as confirming to the required standard.

1. ______________________

Dr. Sajida Kousar

(Supervisor)

2. M. Arshad

Prof. Dr. Muhammad Arshad Zia

(Internal Examiner)

3. Khadija

Dr. Khadija Maqbool

(Chairperson)

4. Hussain

Dr. Saqib Hussain

(External Examiner)

Department of Mathematics & Statistics

Faculty of Basic & Applied Sciences
International Islamic University, Islamabad
Pakistan
2016

Forwarding Sheet by Research Supervisor

The Thesis entitled Algebraic Codes over Max-Min Algebra submitted by Asra Riaz Reg. No 186-FBAS/MSMA/F14 in partial fulfillment of MS Degree in Mathematics has been completed under my guidance and supervision. I am satisfied with the quality of his research work and allow him to submit this thesis for further process to graduate with Master of Science degree from the Department of Mathematics & Statistics, as per IIUI rules and regulations.

date 28/09/2016

Dr. Sajida Kousar
Assistant Professor
Department of Maths & Stats,
International Islamic University,
Islamabad.

Abstract

Coding theory is a field of study related with the transmission of data across noisy channels. Claude Shannon's 1948 paper "A Mathematical Theory of Communication" gave the idea of codding theory. Codes are used for data compression, error correction and also for reliable data transformation. All communication channels contain some amount of unreliability. When a massage is encoded in such channel it is effected by a noise and the received massage contain error. We can minimize that error and can get best results by the repetition of massage n times. The basic purpose of this repeating massage is to obtain reliable communication.

The aim of this thesis is study of coding theory over max -min algebra. Max-Min algebra is a semi ring with two binary operations maximum and minimum, where maximum is defined as addition and minimum is defined as multiplication.

This thesis based on three chapters. Chapter 1 is of introductory nature, we include some basics definition which will be required by the reader to understand next two chapters. In last part we define most important topic semi ring and *semi vector space.*

In chapter 2, we consider a finite field and discuss codes over finite dimensional vector space. We also discuss polynomial ring over finite field.

In third chapter, we introduce max-min algebra which is a semi ring, so we consider here semi ring and *semi vector space* and discuss codes over a finite dimensional *semi vector space.*

Contents

Acknowledgement

All the praises to Almighty Allah the most gracious, the most merciful and the creator of all the creations in the creature, who gave me strength, ability and courage to fulfill the requirements of this thesis. I offer Darood pak to Holy prophet Muhammad (PBUH) who showed the right path to the mankind.

I am very thankful to my kind nature nicest supervisor Dr.Sajida kousar for giving me an opportunity to work under her supervision and guidance. She supported me with many encouraging suggestions knowledgeable comments. I will always be proud of working under the supervision of Dr.Sajida kousar who indeed is a source of motivation and inspiration for every student. I pray to Almighty Allah keep happy to my supervisor. I offer special thanks to all my friends.

Finally my Deepest gratitude to my parents who always encouraged me and showed their everlasting love, care and support throughout my life, whose sincere prayers, deep love and support established a spirit of completing the challenging tasks. It would have been impossible for me to complete this work without the prayers of my parents and great support and understanding of my family.

Chapter 1

Preliminaries

The aim of this chapter is to present some basic concepts and to explain terminology which will be used in this work. In section 1.1 we will discuss the most important topic from linear algebra, vector spaces and subspaces. Second section 1.2 is concerned with Max-Min algebra. For the definition and results discussed in this chapter we will refer [5], [6], [9] and [11].

1.1 Vector spaces

We start with the definition of group.

Definition 1.1.1. A non-empty set G together with a binary operation $*$ on G is called a group if the following conditions holds:

1. $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
2. There exist an element $e \in G$ such that $e * a = a * e = a$ for all $a \in G$.
3. For each $a \in G$ there exist an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

The element e is called the identity of G and a^{-1} is called the inverse of a in G. A group G is said to be abelian if $a * b = b * a$ for all $a, b \in G$

Example 1.1.2. 1. The set of integers, rational numbers, real numbers and complex numbers are abelian groups under the operation of usual addition.

2. The set $M_{n\times m}(\mathbb{R})$ of all $n \times m$ matrices over the set of real numbers is a group under the usual addition of matrices.

Definition 1.1.3. Let G be a group and let H be a non-empty subset of G. Then H is called a subgroup of G if H is itself a group under the binary operation of G.

Definition 1.1.4. A non-empty set R with two binary operations usually called addition and multiplication, denoted by "$+$" and "$\cdot$" is called a ring if

1. $(R, +)$ is an abelian group;

2. $(R, \cdot)$ is a semigroup;

3. Left and right distributive laws hold, that is, for all $a, b, c \in R$.

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(b + c) \cdot a = b \cdot a + c \cdot a$$

Remark 1.1.5. If R contains multiplicative identity 1, that is, $1.a = a.1 = a$ for all $a \in R$. Then R is called a ring with identity.
If $a \cdot b = b \cdot a$ for all $a, b \in R$. Then R is called a commutative ring.

Remark 1.1.6. If in the above definition $(R, +)$ is just a semigroup then $(R, +, .)$ is called a semiring.

Example 1.1.7. 1. If $(R, +)$ is any abelian group, .then the operation of multiplication defined by

$$a \cdot b = 0_R, \text{ for all } a, b \in R$$

turns R into a commutative ring.

2. The set of integers, rational numbers, real numbers and complex numbers are commutative rings with identity under the operations of usual addition and usual multiplication.

3. The set $M_{n\times n}(\mathbb{R})$ of all $n \times n$ matrices over the set of real numbers is a ring under usual addition and multiplication of matrices.

Definition 1.1.8. A non-empty subset S of R is called a subring of R if S is itself a ring under the binary operations of R.

Definition 1.1.9. Let R be a ring. A left ideal I of R is a non-empty subset of R such that

1. $(I, +)$ is a subgroup of $(R, +)$, that is, $a - b \in I$ for all $a, b \in I$;

2. $ra \in I$ for all $r \in R$ and $a \in I$.

Similarly, a right ideal I of R is a non-empty subset of R such that

1. $(I, +)$ is a subgroup of $(R, +)$, that is, $a - b \in I$ for all $a, b \in I$;

2. $ar \in I$ for all $r \in R$ and $a \in I$.

If I is both left and right ideal of R, then I is called a two sided or simply an ideal of R. The zero ideal $\{0\}$ and the ring R are examples of two-sided ideals in any ring R.

Definition 1.1.10. A non-empty set F with two binary operations denoted by + and . is called a field if

1. $(F,+)$ is an abelian group;

2. $(F,\cdot)$ is a commutative group;

3. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in F$.

Example 1.1.11. 1. The set of real numbers, rational numbers and complex numbers are fields under addition and multiplication.

2. $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$, where p is a prime, is a field under addition and multiplication modulo p.

3. If number of elements in F is finite, then F is called finite field.

Definition 1.1.12. Let F be a field and V be an additive abelian group, then V is called a vector space over F, if we can define a map from $F \times V \longrightarrow V$(called a scalar multiplication) such that for all $\alpha \in F$ and $v \in V$, $\alpha v \in V$ and the following conditions hold:

1. $\alpha(\mathbf{u}+\mathbf{v}) = \alpha\mathbf{u} + \alpha\mathbf{v}$

2. $(\alpha + \beta)\mathbf{u} = \alpha\mathbf{u} + \beta\mathbf{u}$

3. $\alpha(\beta\mathbf{u}) = (\alpha\beta)\mathbf{u}$

4. $1.\mathbf{u} = u$.

   For all $\alpha, \beta \in F$ and $u, v \in V$.

Example 1.1.13. 1. Every field is a vector space over itself.

2. If F is a field, then $F^n = \{(x_1, x_2, ..., x_n) : x_i \in F^n\}$ is a vector space over F, where the operation of addition and scalar multiplication are defined by

$$\begin{aligned}(x_1, x_2, x_3, ..., x_n) + (y_1, y_2, y_3, ..., y_n) =& (x_1 + y_1, x_2 + y_2, ..., x_n + y_n)\\ \alpha(x_1, x_2, x_3, ..., x_n) =& (\alpha x_1, \alpha x_2, \alpha x_3, ..., \alpha x_n)\end{aligned}$$

3. The set $M_n(\mathbb{F})$ of n-square matrices over F is a vector space over F, where the operations of addition and scalar multiplication are defined by

$$[a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}]$$

$$\alpha[a_{ij}] = [\alpha a_{ij}]$$

Definition 1.1.14. Let V be a vector space over a field F. A non empty subset U of V is called a **subspace** of V if U is itself a vector space under the same operations of V, that is, U is also an additive abelian group and for any $c \in F$, $u \in U$, cu is also in U.

Theorem 1.1.15. *Let* V *be a vector space and F be a field. A subset* U *of* V *is a subspace if and only if:*

1. *For any two vectors* $\mathrm{u}, \mathrm{v} \in \mathrm{U}$, $\mathrm{u} - \mathrm{v}$ *is also in* U.

2. *For any $c \in F$, $\boldsymbol{u} \in U$, $\boldsymbol{cu}$ is also in U.*

Remark 1.1.16. Let U and W be any two subspaces of V. Then the sum

$$U + W = \{u + w : u \in U, w \in W\}$$

and intersection

$$U \bigcap W = \{v \in V : v \in U, W\}$$

are also subspaces of V.

Definition 1.1.17. Two vectors are *Linear indcpendent* if they are not scalar multiples of each other. Otherwise thc vectors are *Linear dcpcndent.*

Definition 1.1.18. A set of vectors $\{v_1, v_2, \ldots, \ldots v_n\}$ in a vector space V is called linearly independent over F if

$$a_1v_1 + a_2v_2 + \ldots + a_mv_m = 0 \text{ implies each } a_i = 0, i = 1, 2, \ldots, m$$

Definition 1.1.19. A set of vector $\{v_1, v_2, \ldots, v_n\}$ is said to generate V if every element in V is expressible as a linear combination

$$a_1v_1 + a_2v_2 + \ldots + a_nv_2$$

where $a_i \in F$.

Definition 1.1.20. A set B of linearly independent vectors that also generates V is called a basis for V. The number of elements in B is called dimension of V.

Note that, a vector space may have more than one basis but the number of elements in every base is same.

The dimension of subspaces of V are less than or equal to the dimension of V. If dimension of a subspace equal to the dimension of V, then that subspace is V itself.

If U and W are any two subspaces of V, then

$$\dim(U+W) = \dim U + \dim W - \dim(U \bigcap W).$$

1.1.1 Polynomial ring

Let F be a field the polynomial $p(x)$ in x over the field F is defined as an expressions of the form

$$p(x) = p_0 + p_1x + p_2x^2 + \ldots + p_nx^n,$$

where the coefficients $p_i \in F$. We will denote the set of all such expressions by $F[x]$. If $p(x) = p_0+p_1x+p_2x^2+\ldots+p_nx^n$ and $q(x) = q_0+q_1x+q_2x^2+\ldots+q_mx^m$ with $m \geq n$ are any two polynomials over F. We can define their sum as

$$p(x) + q(x) = p_0 + q_0 + (p_1 + q_1)x + \ldots + (p_n + q_n)x^n + q_{n+1}x^{n+1} + \ldots q_mx^m.$$

Then, this addition turns $F[x]$ into an abelian group.

Now if we define the multiplication of $p(x)$ and $q(x)$ as

$$p(x)q(x) = c_0 + c_1x + \ldots + c_mx^m,$$

where $c_i = \sum_{i=j+k} p_jq_k$. Then under this multiplication $F[x]$ is a commutative semigroup.

It is not hard to verify that

$$p(x)\{q(x) + r(x)\} = p(x)q(x) + p(x)r(x)$$

and

$$\{p(x) + q(x)\}r(x) = p(x)r(x) + q(x)r(x)$$

Also

$$p(x)q(x) = q(x)p(x)$$

for all $p(x), q(x), r(x) \in F[x]$. Thus we get that $F[x]$is a commutative ring called the polynomial ring over F.

If we define scaler multiplication $F \times F[x] \rightarrow F[x]$ as

$$ap(x) = ap_0 + ap_1x + ap_2x^2 + \ldots + ap_nx^n$$

for $a \in F$ and $p(x) \in F[x]$. Then, $F[x]$ becomes a vector space over F.

1.2 Max-Min Algebra

In this section we will define Max-Min algebra also known as Bottleneck algebra. Before writing the formal definition first we would like to explain partially ordered sets.

Definition 1.2.1. A relation $\leq$ on a set S is said to be a partial order if it is reflexive, antisymmetric and transitive. That is, for all $x, y, z \in S$

1. $x \leq x$ (Reflexive).

2. $x \leq y$ and $y \leq x$ then $x = y$ (Antisymmetric).

3. $x \leq y$ and $y \leq z$ then $x \leq z$ (Transitive).

The set $(S, \leq)$ is called a partially ordered set.

Definition 1.2.2. A Max-Min algebra S is a partially ordered set with maximum and minimum as the two binary operations. Max-Min algebra is a discrete algebraic system in which the max and min operations are defined as addition and multiplication in conventional algebra. Let a ,b $\in S$ then

$$a \oplus b = max\{a, b\}$$

$$a \odot b = min\{a, b\}$$

For these operations, we have

1. $a \oplus (b \oplus c) = max\{a, max\{b, c\}\} = max\{a, b, c\} = (a \oplus b) \oplus c$

2. $a \oplus b = max\{a, b\} = max\{b, a\} = b \oplus a$

3. $a \odot (b \odot c) = min\{a, min\{b, c\}\} = min\{a, b, c\} = (a \odot b) \odot c$

4. $a \odot b = min\{a, b\} = min\{b, a\} = b \odot a$

5. $a \odot (b \oplus c) = min\{a, max\{b, c\}\} = max\{min\{a, b\}, min\{a, c\}\} = a \odot b \oplus a \odot c$

6. $(a \oplus b) \odot c = a \odot c \oplus b \odot c$

Thus, we get that $(S, \oplus, \odot)$ is a commutative semiring.

Let us take examples.

Example 1.2.3. Let $\mathbb{Z}_2 = \{0, 1\}$. The relation $0 \leq 0$, $1 \leq 1$, $0 \leq 1$ is a partial ordered on $\mathbb{Z}_2$. The addition and multiplication are defined as

$\oplus$	0	1
0	0	1
1	1	1

$\odot$	0	1
0	0	0
1	0	1

it is easy to verify that $\mathbb{Z}_2$ is a Max-Min algebra with additive identity 0 and multiplicative identity 1.

Example 1.2.4. Let $\mathbb{Z}_3 = \{0, 1, 2\}$. The relation

$$0 \leq 0, 1 \leq 1, 2 \leq 2$$

$$0 \leq 1, 0 \leq 2, 1 \leq 2$$

is partial order relation on Z_3. The addition and multiplication are defined as

$\oplus$	0	1	2
0	0	1	2
1	1	1	2
2	2	2	2

$\odot$	0	1	2
0	0	0	0
1	0	1	1
2	0	1	2

Then $\mathbb{Z}_3$ is a Max-Min algebra with additive identity 0 and multiplicative identity 2.

Definition 1.2.5. A non-empty set I on S is called an ideal of S if $a + b, \quad sa, \quad as \in I$, for all $a, b \in I$ and $s \in S$.

Now onwrad by S we mean a Max-Min algebra having both additive and multiplicative identities. Just like vector space over a field F, now we will define a *semi vector space* over Max-Min algebra S.

1.2.1 Semi vector Space

Semi vector Space: Let $(V, +)$ be a semigroup and $(S, \oplus, \odot)$ be a Max-Min algebra. Define the scaler multiplication $S \times V \longrightarrow V$ as for all $s \in S$ and $v \in V$, $sv \in V$. If

1. $a(u + w) = au + aw$
2. $(a \oplus b)u = au + bw$
3. $(a \odot b)u = a(bu)$

for all $u, w \in V$ and $a, b \in S$. Then V is called a *semi vector space* over S.

Example 1.2.6. Every Max-Min algebra S is a *semi vector space* over S, where the scalar multiplication is defined as $sv = s \odot v$.

Example 1.2.7. Let S be a Max-Min algebra. Consider $S^n = \{(x_1, x_2, \ldots, x_n) : x_i \in S\}$, define addition and scalar multiplication on S^n as

$$(x_1, x_2, \ldots, x_n) + (x_1', x_2', \ldots, x_n') = (x_1 \oplus x_1', x_2 \oplus x_2', \ldots, x_n \oplus x_n')$$

and

$$a(x_1, x_2, \ldots, x_n) = (a \odot x_1, a \odot x_2, \ldots, a \odot x_n).$$

Then the associativity of Max operation in S imply that S^n is a semigroup. Now for *semi vector space* we have:

1. $\alpha(u + v) = \alpha[(x_1, x_2, \ldots, x_n) + (x'_1, x'_2, \ldots, x'_n)]$

$$\begin{aligned}
&= \alpha(x_1 \oplus x'_1, x_2 \oplus x'_2, \ldots, x_n \oplus x'_n)\\
&= [\alpha \odot (x_1 \oplus x'_1), \alpha \odot (x_2 \oplus x'_2), \ldots, \alpha(x_n \oplus x'_n)]\\
&= [\alpha \odot x_1 \oplus \alpha \odot x'_1, \alpha \odot x_2 \oplus \alpha \odot x'_2, \ldots, \alpha \odot x_n \oplus \alpha \odot x'_n]\\
&= (\alpha \odot x_1, \alpha \odot x_2, \ldots, \alpha \odot x_n) + (\alpha \odot x'_1, \alpha \odot x'_2, \ldots, \alpha \odot x'_n)\\
&= \alpha(x_1, x_2, \ldots, x_n) + \alpha(x_1\prime, x_2\prime, \ldots, x_n\prime)\\
&= \alpha u + \alpha v
\end{aligned}$$

2. $(\alpha_1 \oplus \alpha_2)u$

$$\begin{aligned}
&= (\alpha_1 \oplus \alpha_2)(x_1, x_2, \ldots, x_n)\\
&= [(\alpha_1 \oplus \alpha_2) \odot x_1, (\alpha_1 \oplus \alpha_2) \odot x_2, \ldots, (\alpha_1 \odot \alpha_2)x_n)\\
&= [(\alpha_1 \odot x_1, \alpha_1 \odot x_2, \ldots, \alpha_1 \odot x_n) + (\alpha_2 \odot x_1, \alpha_2 \odot x_2, \ldots, \alpha_n \odot x_n)]\\
&= \alpha_1(x_1, x_2, \ldots, x_n) + \alpha_2(x_1, x_2, \ldots, x^n)\\
&= \alpha_1 u + \alpha_2 u
\end{aligned}$$

3. $(\alpha_1 \odot \alpha_2)u$

$$\begin{aligned}
&= (\alpha_1 \odot \alpha_2)(x_1, x_2, \ldots, x_n)\\
&= [(\alpha_1 \odot \alpha_2) \odot x_1, (\alpha_1 \odot \alpha_2) \odot x_2, \ldots, (\alpha_1 \odot \alpha_2) \odot x_n]\\
&= [\alpha_1 \odot (\alpha_2 \odot x_1), \alpha_1 \odot (\alpha_2 \odot x_2), \ldots, \alpha_1 \odot (\alpha_2 \odot x_n)]\\
&= [\alpha_1(\alpha_2 \odot x_1, \alpha_2 \odot x_2, \ldots, \alpha_2 \odot x_n)]\\
&= \alpha_1[\alpha_2(x_1, x_2, \ldots, x_n)]\\
&= \alpha_1(\alpha_2 u)
\end{aligned}$$

Thus, S^n is a *semi vector space.*

Definition 1.2.8. A non-empty subset U of a *semi vector space* V is called a subspace of V, if it is itself a *semi vector space* under the binary operation and scalar multiplication of V. That is, $(U, +)$ is a semigroup and for all $u \in U$ and $a \in S$, $au \in U$.

Proposition 1.2.9. *A non-empty subset U of a* semi vector space *V is a subspace of V if and only if $au_1 + bu_2 \in U$ for all $a, b \in S$ and $u_1, u_2 \in U$.*

Proof. If U is a subspace then clearly $au_1 + bu_2 \in U$ for all $a, b \in S$ and $u_1, u_2 \in U$.

Conversely, if $au_1 + bu_2 \in U$ for all $a, b \in S$ and $u_1, u_2 \in V$. Then if we take $a = b = 1$, then $u_1 + u_2 \in U$ for all $u_1, u_2 \in U$ imply that $(U, +)$ is a semigroup. If we take $b = 0$, then $au_1 \in U$ imply that scalar multiplication holds in U. Thus, U is a subspace of V. □

1.2.2 Polynomials over Max-Min Algebra

Let S be a Max-Min algebra, then by a polynomials over S we mean an expression of the form

$$p(x) = a_0 + a_1x+, ..., +a_nx^n$$

here $a_i \in S$ and denote the set of all polynomials over S by $S[x]$. If $p(x), q(x) \in S[x]$ and the addition and multiplication are defined as

$$\begin{aligned} p(x) + q(x) =& (a_0 + a_1x + ... + a_nx^n) + (b_0 + b_1x + ... + b_nx^n) \\ =& a_0 \oplus b_0 + (a_1 \oplus b_1)x + ... + (a_n \oplus b_n)x^n \\ =& \sum (a_i \oplus b_i)x^i \end{aligned}$$

$$\begin{aligned} p(x)q(x) =& (a_0 + a_1x + ... + a_nx^n)(b_0 + b_1x + ... + b_nx^n) \\ =& (a_0 \odot b_0) + (a_1 \odot b_0 \odot a_1 \odot b_0)x + ... + (a_0 \odot b_n \odot a_n\ b_0)x^n. \end{aligned}$$

Then for any $f(x) = a_0+a_1x+a_2x^2+\ldots+a_nx^n$, $g(x) = b_0+b_1x+b_2x^2+\ldots+b_nx^n$ and $h(x) = c_0 + c_1x + c_2x^2 + \ldots + c_nx^n$ in $S[x]$ we have

$$\begin{aligned}(f(x) + g(x)) + h(x) =&[(a_0 + a_1x + a_2x^2 + \ldots + a_nx^n) + (b_0 + b_1x + b_2x^2\\ &+ \ldots + b_nx^n)] + (c_0 + c_1x + c_2x^2 + \ldots + c_nx^n)\\ =&[(a_0 \oplus b_0) + (a_1 \oplus b_1)x + (a_2 \oplus b_2)x^2 + \ldots +\\ &(a_n \oplus b_n)x^n] \oplus (c_0 + c_1x + c_2x^2 + \ldots + c_nx^n)\\ =&[max(a_0, b_0) + max(a_1 + b_1)x + max(a_2 + b_2)x^2 + \ldots\\ &+ max(a_n + b_n)x^n] \oplus (c_0 + c_1x + c_2x^2 + \ldots + c_nx^n)\\ =&\{max(a_0, b_0) \oplus c_0\} + \{max(a_1, b_1) \oplus c_1\}x + \{max(a_2, b_2)\\ &\oplus c_2\}x^2 + \ldots + \{max(a_n, b_n) \oplus c_n\}x^n\\ =&max\{max(a_0, b_0), c_0\} + max\{max(a_1, b_1), c_1\}x + max\\ &\{max(a_2, b_2), c_2\}x^2 + \ldots + max\{max(a_n, b_n), c_n\}x^n\\ =&max(a_0, b_0, c_0) + max(a_1, b_1, c_1)x + max(a_2, b_2, c_2)x^2\\ &+ \ldots + max(a_n, b_n, c_n)x^n\\ =&max\{a_0, max(b_0, c_0)\} + max\{a_1, max(b_1, c_1)\}x+\\ &max\{a_2, max(b_2, c_2)\}x^2 + \ldots + max\{a_n, max(b_n, c_n)\}x^n\\ =&f(x) + [g(x) + h(x)]\end{aligned}$$

$$\begin{aligned}f(x) + g(x) =&(a_0 + a_1x + a_2x^2 + \ldots + a_nx^n) + (b_0 + b_1x + b_2x^2 + \ldots + b_nx^n)\\ =&(a_0 \oplus b_0) + (a_1 \oplus b_1)x + (a_2 \oplus b_2)x^2 + \ldots + (a_n \oplus b_n)x^n\\ =&max(a_0, b_0) + max(a_1, b_1)x + max(a_2, b_2)x^2 + \ldots + max(a_n, b_n)x^n\\ =&max(b_0, a_o) + max(b_1, a_1)x + max(b_2, a_2)x^2 + \ldots + max(b_n, a_n)x^n\\ =&g(x) + f(x)\end{aligned}$$

$$\begin{aligned}
[f(x)g(x)]h(x) =& [(a_0 + a_1x + a_2x^2 + \ldots + a_nx^n)(b_0 + b_1x+ \\
& b_2x^2 + \ldots b_nx^n)](c_0 + c_1x + c_2x^2 + \ldots + c_nx^n) \\
=& [a_0 \odot b_0 + (a_1 \odot b_0 \oplus a_0 \odot b_1)x + \ldots + (a_n \odot b_0 \oplus \\
& \ldots \oplus a_0 \odot b_n)x^n](c_0 + c_1x + c_2x^2 + \ldots + c_nx^n) \\
=& [(a_0 \odot b_0 \odot c_0) + \{(a_o \odot b_0) \odot c_1 \oplus (a_1 \odot b_0 \oplus a_0 \odot b_1) \\
& \odot c_0\}x + \ldots + \{(a_0 \odot b_0) \odot c_n \oplus (a_n \odot b_0 \oplus \\
& \ldots \oplus a_0 \odot b_n) \odot c_0\}x^n \\
=& (a_0 \odot b_0 \odot c_0) + (a_1 \odot b_0 \odot c_0 \oplus a_0 \odot b_1 \odot c_0 \oplus a_0 \odot b_0 \odot \\
& c_1)x + \ldots + (a_0 \odot b_0 \odot c_n \oplus a_n \odot b_0 \odot c_0 \oplus a_0 \odot b_n \odot c_0)x^n \\
=& min(a_0, b_0, c_0) + max\{min(a_1, b_0, c_0), min(a_0, b_1c_0), \\
& min(a_0, b_0, c_1)\}x + \ldots + max\{min(a_0, b_0, c_n), min(a_n, \\
& b_0, c_0), \ldots, min(a_0, b_n, c_0)\}x^n \\
=& f(x)[g(x)h(x)]
\end{aligned}$$

$$\begin{aligned}
f(x)g(x) =& (a_0 + a_1x + a_2x^2 + \ldots + a_nx^n)(b_0 + b_1x + b_2x^2 + \ldots + b_nx^n) \\
=& a_0 \odot b_0 + (a_1 \odot b_0 \oplus a_0 \odot b_1)x + \ldots + (a_n \odot b_0 \oplus \ldots \oplus a_0 \odot b_n)x^n \\
=& min(a_0, b_0) + max\{min(a_1, b_0), min(a_0, b_1)\}x + \ldots + max\{min(a_n, b_0) \\
& , \ldots, min(a_0, b_n)\}x^n \\
=& min(b_0, a_0) + max\{min(b_0, a_1), min(b_1, a_0)\}x + \ldots + max\{min(b_0, a_n) \\
& , \ldots, min(b_n, a_0)\} \\
=& g(x)f(x)
\end{aligned}$$

$$\begin{aligned}
f(x)[g(x) + h(x)] =& (a_0 + a_1x + \ldots + a_nx^n)[(b_0 + b_1x+ \\
& \ldots + b_nx^n) + (c_0 + c_1x + \ldots + c_nx^n)] \\
=& (a_0 + a_1x + \ldots + a_nx^n)[(b_0 \oplus c_0) + (b_1 \oplus c_1)x + \cdots + (b_n \oplus c_n)x^n]
\end{aligned}$$

$$\begin{aligned}
&=[a_0 \odot (b_0 \oplus c_0) + \{a_1 \odot (b_0 \oplus c_0) \oplus a_0 \odot (b_1 \oplus c_1)\}x \\
&\quad + \ldots + \{a_n \odot (b_0 \oplus c_0) \oplus a_0 \odot (b_n \oplus c_n)\}x^n] \\
&=(a_0 \odot b_0 \oplus a_0 \odot c_0) + \{a_1 \odot b_0 \oplus a_1 \odot c_0 \oplus a_0 \odot b_1 \oplus a_0 \odot c_1\}x \\
&\quad + \ldots + \{a_n \odot b_0 \oplus \ldots \oplus a_n \odot c_0 \oplus a_0 \odot b_n \oplus \ldots \oplus a_0 \odot c_n\}x^n \\
&=f(x)g(x) + f(x)h(x)
\end{aligned}$$

Thus, we get that $S[x]$ is a semiring.

Remark 1.2.10. If we define scalar multiplication $S \times S[x] \to S[x]$ as

$$ap(x) = a \odot p_0 + a \odot p_1 x + \ldots + a \odot p_n x^n$$

then this scalar multiplication turns $S[x]$ into a semivector space.

Definition 1.2.11. Let $f(x) \in S[x]$ where $f \neq 0$. The degree of $f(x)$ is $\max\{n \mid a_n \neq 0\}$ and it is denoted by $degf(x)$.

Proposition 1.2.12. *If* $f(x), g(x) \in S[x]$, *then*

$$deg(f(x) + g(x)) = max\{degf(x), degg(x)\}.$$

Proof. Let $degf(x) = n$ and $degg(x) = m$ with $m \geq n$. Suppose $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$. Then

$$f(x)+g(x) = a_0 \oplus b_0 + (a_1 \oplus b_1)x + \ldots + (a_n \oplus b_n)x^n + (0 \oplus b_{n+1})x^{n+1} + \ldots + (0 \oplus b_m)x^m.$$

Since $b_m \neq 0$, so $0 \oplus b_m = max\{0, b_m\} = b_m$. We get that

$$deg(f(x) + g(x)) = m = max\{degf(x), degg(x)\}.$$

□

Definition 1.2.13. Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ *where* $a_n \neq 0$ then $f(x)$ is said to be monic polynomial if leading coefficient of $f(x)$ that is $a_n = 1$.

Chapter 2

Algebraic codes over finite fields

In this chapter we will discuss algebraic codes over finite fields. In the first section we discuss Linear codes. Second section deals with dual codes. In the third section we present Reed-Muller Codes. In the last section of this chapter we will discuss relation between polynomail ring and algebraic codes. For the definitions and results discussed in this chapter we will refer [1], [2] , [4] and [10].

2.1 Linear code

We start this section with the definition of linear codes.

Definition 2.1.1. Let F be a finite field, then we know that F^n is an n-dimensional vector space over F (see 1.1.13). A code C over F is simply a subset of F^n. The members of C are called codewords. However, rather then presenting a codeword $(a_1, a_2, \ldots, a_n)$ in the form of an n-tuple, we will prefer to write it as $a_1a_2 \ldots a_n$.

A code C is linear over F. If whenever, $u \in C$ and $v \in C$, then $\alpha u + \beta v \in C$ for all $\alpha, \beta \in F$. That is, C is a subspace of F^n.

If dimension of C is k, then C is called an (n, k)-code.

If $F = \mathbb{Z}_2 = \{0, 1\}$ under addition and multiplication modulo 2, then the codes over F are called binary codes. If the code is linear then it is called a binary linear code.

Let F be a finite field. A code C is called cyclic in the cyclic shift of each codeword in C is also a member in C. For example the code $\{0000, 1010, 0101, 1111\}$ is a cyclic code.

Remark 2.1.2.

1. The zero codeword $00\ldots0$ always belongs to all linear codes.
2. As $dim(F^n) = n$ a finite number so each subspace of F^n is a finite dimensional and thus a linear code over F is a finite dimensional subspace of F^n.

Example 2.1.3.

If $F = \mathbb{Z}_3 = \{0, 1, 2\}$, then $C = \{000, 111, 222\}$ is linear over F. However $C = \{000, 111, 121\}$ is not linear as

$$111 + 121 = (1+1)(1+2)(1+1) = 202 \notin C.$$

Example 2.1.4. The codes $C = \{00, 01, 10, 11\}$ and $C = \{000, 011, 101, 110\}$ are binary linear codes.

2.1.1 Hamming distance

Definition 2.1.5. Let x and y be any two codewords. The Hamming distance $d(x, y)$ is the number of places in which the codewords x and y differ. In other words, $d(x, y)$ represents the component-wise difference of the vectors x and y. That is,

$$d(x, y) = |\{i : x_i \neq y_i\}|.$$

Example 2.1.6. If $x = 000$ and $y = 011$, then $x_1 = 0 = y_1$, $x_2 = 0 \neq 1 = y_2$ and $x_3 = 0 \neq 1 = y_3$

$$\Rightarrow d(000, 011) = 2.$$

Similarly,

$$d(0000, 0111) = 3$$

Definition 2.1.7. The minimum (Hamming) distance of a code C is the minimum distance between any two codewords in the code:

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

Example 2.1.8. Let $C = \{0000, 0101, 1010, 1111\}$ be a code, then

$$d(0000, 0101) = 2, \quad d(0000, 1010) = 2, \quad d(0000, 1111) = 4$$

$$d(0101, 1010) = 4, \quad d(0101, 1111) = 2, \quad d(1010, 1111) = 2.$$

Thus, the minimum distance of code C is 2.

Definition 2.1.9. Hamming weight of a codeword is number of nonzero components in a codeword.

Example 2.1.10.

$$w(0110) = 2$$

$$w(0111) = 3$$

Theorem 2.1.11. *Let C be a linear code. Then the minimum distance of C is equal to the smallest Hamming weight of non-zero codeword in C.*

Example 2.1.12. Let $C = \{0000, 0101, 1010, 1111\}$ be a code then minimum hamming distance is

$$d(0101, 1111) = 2$$

and lowest weight of nonzero codeword is

$$w(0101) = 2.$$

Definition 2.1.13. If an $(n, k)-$ code has minimum distance d, then it is represented by (n, k, d).

Example 2.1.14. The set $C = \{0000, 0101, 1010, 1111\}$ is a binary linear code. Since the sum of any two codewords lies in this set. As

$$0101 + 1010 = 1111, \quad 0101 + 0101 = 0000,$$

we get that C is generated by $0101, 1010$. That is, the dimension of C is 2. From Example 2.1.8 we know that $d = 2$. Thus, C is a (4, 2, 2)- code.

Example 2.1.15.

1. The binary code {000,111} is a linear (3,1,3)-code.
2. The binary code {000,110,101,111} is a linear (3,2,2)-code.

Remark 2.1.16. A q-array (n,k) code consist of q^k codewords. In particular a binary (n,k)-code consist of 2^k codewords.

2.1.2 Generator matrix

Linear codes are used in practice largely due to the simple encoding procedures facilitated by their linearity. A $k \times n$ generator matrix G for an (n, k) linear code C provides a compact way to describe all of the codewords in C and provides a way to encode messages. By performing the multiplication **mG**, a generator matrix maps a length k message string **m** to a length n codeword string. The encoding function $\mathbf{m} \to \mathbf{mG}$ maps the vector space $V(k, q)$ on to a k- dimensional subspace (namely the code C) of the vector space V(n,q).

Definition 2.1.17. A $k \times n$ matrix G whose rows form a basis for an (n, k) linear code C is called a generator matrix of the code C.

Theorem 2.1.18. *Let C be an (n, k)-code over F. Let G be a generator matrix of C. Then*

$$C = \{mG \text{ such that } m \in F^k\}.$$

Proof. Let C be an (n,k) code and G be the generator matrix of C over F. Then by definition the rows of G form basis for C. Let $G_1, G_2, \ldots, G_k$ be the rows of G. So every $x \in C$ can be written as a linear combination of vectors of G.

$$\begin{aligned} x =& m_1G_1 + m_2G_2 + \ldots + m_kG_k \text{ where } m_1, m_2, \ldots, m_k \in F \text{ and} \\ =& [m_1, m_2, \ldots, m_k] \begin{bmatrix} G_1 \\ G_2 \\ \vdots \\ G_k \end{bmatrix} \\ =& mG \end{aligned}$$

Thus $$C = \{mG \text{ such that } m \in F^k\}$$ □

Example 2.1.19. To generate (3,2)-code we have to encode message of length k. Here $k = 2$ that is we have 2^k=2^2=4 codewords. The possible pairs of length 2 are [0 0], [1 0], [0 1], [1 1]. Generator matrix should be an $k \times n = 2 \times 3$ matrix. Let us take

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

at $m = [0\ 0]$

$$\begin{aligned} mG =& \begin{bmatrix} 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ =& [0 \cdot 1 + 0 \cdot 0 \quad 0 \cdot 0 + 0 \cdot 0 \quad 0 \cdot 0 + 0 \cdot 1] \\ =& [0\ 0\ 0] \end{aligned}$$

at $m = [1\ 0]$

$$\begin{aligned} mG =& \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ =& [1 \cdot 1 + 1 \cdot 0 \quad 1 \cdot 0 + 0 \cdot 0 \quad 1 \cdot 0 + 0 \odot 1] \\ =& [1\ 0\ 0] \end{aligned}$$

at $m = [0\ 1]$

$$\begin{aligned} mG = & \begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ = & [0 \cdot 1 + 1 \cdot 0 \ \ 0 \cdot 0 + 1 \cdot 0 \ \ 0 \cdot 0 + 1 \cdot 1] \\ = & [0\ 0\ 1] \end{aligned}$$

at $m = [1\ 1]$

$$\begin{aligned} mG = & \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ = & [1 \cdot 1 + 1 \cdot 0 \ \ 1 \cdot 0 + 1 \cdot 0 \ \ 1 \cdot 0 + 1 \cdot 1] \\ = & [1\ 0\ 1] \end{aligned}$$

Code generated from this generator matrix with four codewords is

$$C = \{000, \quad 100, \quad 001, \quad 101\}.$$

Remark 2.1.20.

1. As basis for a vector space is not unique so the generator matrix of an (n,k)-code is not unique.
2. If C be the code and G be generator matrix of C then G provide a way to encode a message $m \in F^k$ as the codeword vector $mG \in C$ which is contained in F^n. Thus a linear code has a map $E : F^k \to F^n$ which is an encoding map.
3. Each element in F^k is called a message word and there are q^k elements in F^k.

2.2 Dual code

In this section we will define dual codes by using the concept of orthogonal vectors. If $u = (u_1, u_2, \dots u_n)$ and $v = (v_1, v_2, \dots v_n)$ be any two vectors in F^n. Then their product

$$u.v = u_1v_1 + u_2v_2 + \dots u_nv_n.$$

The vectors u and v are orthogonal if

$$u.v = 0.$$

Definition 2.2.1. Let C be (n,k)-code over F. Then the dual code of C is defined to be

$$C^{\perp} = \{u \in F^n \text{ such that } u.v = 0 \; \forall \; v \in C\}.$$

Thus the dual code consists of all codewords that are orthogonal to every codeword in C.

Example 2.2.2. Let $C = \{000, 001\}$

$$(\mathbb{Z}_2)^3 = \{000, 100, 010, 001, 110, 101, 011, 111\}$$

As $C^{\perp} = \{u \in F^n \mid u \cdot v = 0 \; \forall \; v \in C\}$

$$[000] \cdot [000] = [0 \cdot 0 + 0 \cdot 0 + 0 \cdot 0] = 0$$

$$[001] \cdot [000] = [0 \cdot 0 + 0 \cdot 0 + 1 \cdot 0] = 0$$

$$[000] \cdot [100] = [0 \cdot 1 + 0 \cdot 0 + 0 \cdot 0] = 0$$

$$[001] \cdot [100] = [0 \cdot 1 + 0 \cdot 0 + 1 \cdot 0] = 0$$

$$[000] \cdot [010] = [0 \cdot 0 + 0 \cdot 1 + 0 \cdot 0] = 0$$

$$[001] \cdot [010] = [0 \cdot 0 + 0 \cdot 1 + 1 \cdot 0] = 0$$

$$[000] \cdot [001] = [0 \cdot 0 + 0 \cdot 0 + 0 \cdot 1] = 0$$

$$[001] \cdot [001] = [0 \cdot 0 + 0 \cdot 0 + 1 \cdot 1] = 1$$

$$[000] \cdot [110] = [0 \cdot 1 + 0 \cdot 1 + 0 \cdot 0] = 0$$

$$[001] \cdot [110] = [0 \cdot 1 + 0 \cdot 1 + 1 \cdot 0] = 0$$

$$[000] \cdot [101] = [0 \cdot 1 + 0 \cdot 0 + 0 \cdot 1] = 0$$

$$[001] \cdot [101] = [0 \cdot 1 + 0 \cdot 0 + 1 \cdot 1] = 1$$

$$[000]\cdot[011]=[0\cdot 0+0\cdot 1+0\cdot 1]=0$$

$$[001]\cdot[011]=[0\cdot 0+0\cdot 1+1\cdot 1]=1$$

$$[000]\cdot[111]=[0\cdot 1+0\cdot 1+0\cdot 1]=0$$

$$[001]\cdot[111]=[0\cdot 1+0\cdot 1+1\cdot 1]=1$$

hence

$$C^{\perp}=\{000,100,010,110\}$$

As here $n=3$, $k=1$ so $n-k=2$ that is dimension of dual code is 2. So the dual code is (3,2)-code.

Example 2.2.3. Consider $(\mathbb{Z}_3)^2=\{00,01,10,02,20,11,12,21,22\}$ and the code $C=\{11,22\}$. Then

$$[00]\cdot[11]=[0\cdot 1+0\cdot 1]=0$$

$$[00]\cdot[22]=[0\cdot 2+0\cdot 2]=0$$

$$[12]\cdot[11]=[1\cdot 1+2\cdot 1]=0$$

$$[12]\cdot[22]=[1\cdot 2+2\cdot 2]=0$$

$$[21]\cdot[11]=[2\cdot 1+1\cdot 1]=0$$

$$[21]\cdot[22]=[2\cdot 2+1\cdot 2]=0$$

$$[11]\cdot[11]=[1\cdot 1+1\cdot 1]=2$$

$$[22]\cdot[11]=[2\cdot 1+2\cdot 1]=1$$

$$[01]\cdot[11]=[0\cdot 1+1\cdot 1]=1$$

$$[10]\cdot[11]=[1\cdot 1+0\cdot 1]=1$$

$$[02]\cdot[11]=[0\cdot 1+2\cdot 1]=2$$

$$[20]\cdot[11]=[2\cdot 1+0\cdot 1]=2$$

hence

$$C^{\perp}=\{00,12,21\}.$$

Clearly, it is a $(2,1)$- linear code.

Example 2.2.4. Let $C = \{000, 011\}$

$$(\mathbb{Z}_2)^3 = \{000, 100, 010, 001, 110, 101, 011, 111\}$$

then dual code of C is

$$C^{\perp} = \{000, 100, 011, 111\}$$

As here $n = 3$, $k = 1$ so $n - k = 2$ so $n - k = 2$ that is dimension of dual code is 2. Hence the dual code is (3,2)-code.

Remark 2.2.5. Thus each vector in $C^{\perp}$ is orthogonal to each vector in C.

There are codes that are completely contained in their dual code $C^{\perp}$. Such codes are called self orthogonal and if $C = C^{\perp}$ then the code is called self dual.

Proposition 2.2.6. *For any code C, the dual code $C^{\perp}$ is a linear code.*

Proof. As

$$u.0 = 0 \text{ for all } u \in C.$$

We get that

$$0 \in C^{\perp}.$$

Let $u, v \in C^{\perp}$ then by definition of dual code $u \cdot c = 0$ and $v \cdot c = 0$ for every $c \in C$. If $\alpha, \beta \in F$. Then

$$\begin{aligned}(\alpha u + \beta v) \cdot c =& \alpha(u \cdot c) + \beta(v \cdot c)\\ =& \alpha(0) + \beta(0)\\ =& 0\end{aligned}$$

for every $c \in C$ this implies that $\alpha u + \beta v \in C^{\perp}$. Thus, $C^{\perp}$ is linear. □

Proposition 2.2.7. *If C is an (n, k) linear code then $C^{\perp}$ is an $(n, n-k)$ code.*

Proof. Suppose dimension of C is k. If $u = (u_1, u_2, \ldots, u_n) \in C \bigcap C^{\perp}$, then $u.u = u_1u_1 + u_2u_2 + \ldots + u_nu_n = 0$ imply that each $u_i = 0$. Thus, we have

$C \bigcap C^{\perp} = \{0\}$.

Since C and $C^{\perp}$ are linear so, we have

$$n = \dim(F^n) = \dim C + \dim C^{\perp} - \dim C \bigcap C^{\perp} = k + \dim C^{\perp} - 0$$
$$\Rightarrow \dim C^{\perp} = n - k.$$

□

Proposition 2.2.8. *If C is a code and $C^{\perp}$ is dual code of C then $(C^{\perp})^{\perp} = C$.*

Proof. Let C be a code and $C^{\perp}$ is dual code of C then C and $C^{\perp}$ are symmetric. Let $u \in C$. Thus $u.v = 0 \; \forall \; v \in C^{\perp}$ that is if

$$u = [u_1 \, u_2 \, \ldots \, u_n] \;\; and \;\; v = [v_1 \, v_2 \, \ldots \, v_n]$$

then

$$\begin{aligned} u.v =& u_1.v_1 + u_2.v_2 + \ldots + u_n.v_n \\ =& v_1.u_1 + v_2.u_2 \ldots v_n.u_n \; (\because \text{multiplicative is commutative}) \\ =& v.u. \end{aligned}$$

If $u.v = 0$ then $v.u = 0$,$\forall \; u \in C$ and $v \in C^{\perp}$ that is if $v \in C^{\perp}$ then $u \in C$ so $C \subseteq (C^{\perp})^{\perp}$.

If C be a code with dimension k then dimension of dual code is $n - k$, where $C^{\perp}$ is a subspace of F^n. Hence if we take dual of dual code that is $(C^{\perp})^{\perp}$ then it has dimension $n - (n - k) = k$. Thus code C and $(C^{\perp})^{\perp}$ both has same dimension that is k. Thus $C = (C^{\perp})^{\perp}$. □

Lemma 2.2.9. *Let C be a linear code in F^n with generator matrix G. Then $u \in C^{\perp}$ if and only if $uG^{\top} = 0$.*

Proof. Let $G = \begin{bmatrix} G_1 \\ \vdots \\ G_k \end{bmatrix}$ be a generator matrix for linear code C. That is, the rows G_i forms a basis for C. Now

$$uG^{\top} = (u \cdot G_1, \cdots, u \cdot G_k).$$

If $u \in C^{\perp}$ then $u \cdot G_i = 0$ for every i, which implies that

$$uG^{\top} = 0.$$

Conversely, if $uG^{\top} = 0$ then $u \cdot G_i = 0$ for every i. If $c \in C$ then

$$\begin{aligned} c =& \sum_i \lambda_i G_i \text{ for some } \lambda_i \in F \\ u.c =& u.(\sum_i \lambda_i G_i) \\ =& \sum_i \lambda_i (u_i.G_i) \\ =& 0. \end{aligned}$$

Thus, we get that $u \in C^{\perp}$. □

Remark 2.2.10. If G is a generator matrix of C, then the null space of G is $C^{\perp}$ that is $\forall\ u \in C^{\perp}$, $Gu^{\top} = 0$ or equivalently $uG^{\top} = 0$.

Example 2.2.11. let $C = \{000, 001\}$ be (3,1)-code and $C^{\perp} = \{000, 100, 010, 110\}$ be dual (3,2)-code.

$$G = [001]$$

then $\forall\ \ u \in C^{\perp}$ at $u = [000]$

$$\begin{aligned} Gu^{\top} =& \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \\ =& [0 \cdot 0 + 0 \cdot 0 + 1 \cdot 0] \\ =& 0 \end{aligned}$$

at $u = [100]$

$$\begin{aligned} Gu^{\top} =& \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \\ =& [0 \cdot 1 + 0 \cdot 0 + 1 \cdot 0] \\ =& 0 \end{aligned}$$

at $u = [010]$

$$\begin{aligned} Gu^{\top} &= \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \\ &=[0 \cdot 0 + 0 \cdot 1 + 1 \cdot 0] \\ &=0 \end{aligned}$$

at $u = [110]$

$$\begin{aligned} Gu^{\top} &= \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \\ &=[0 \cdot 1 + 0 \cdot 1 + 1 \cdot 0] \\ &=0 \end{aligned}$$

2.3 Parity check matrix

In coding theory a parity check matrix of a linear code C is a matrix which discribes the linear relation that a components of a codeword must satisfy. It can be used to decide wether a particular vector is a codeword.

Definition 2.3.1. Let C be (n,k) code and let H be the generator matrix of the dual code $C^{\perp}$. Then H is called parity check matrix of the code C.

1. As the generator matrix is not unique. So the parity check matrix of a code C is also not unique.

2. As the dual of dual code gives original code that is $(C^{\perp})^{\perp} = C$, so if G is the generator matrix of C then G is the parity check matrix of dual code $C^{\perp}$.

3. If C is an (n,k) code where n is the length and k is the dimension then the dual code is an (n,n-k) code where n is the length and $n - k$ is the

dimension of dual code, so the parity check matrix of an (n,k) code is an $(n-k) \times n$ matrix H which is generator matrix of dual code $C^{\perp}$ and rows of H form basis for $C^{\perp}$.

Example 2.3.2. Let $C = \{000, 001\}$

$$(\mathbb{Z}_2)^3 = \{000, 100, 010, 001, 110, 101, 011, 111\}$$

its dual code becomes

$$C^{\perp} = \{000, 100, 010, 110\}.$$

Here any two vectors on $C^{\perp}$ form basis. Hence we can take

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

also we could take $H = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$ or $H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

Example 2.3.3. Let $C = \{00, 11, 22\}$ where $(\mathbb{Z}_3)^2 = \{00, 01, 10, 02, 20, 11, 12, 21, 22\}$. The dual code becomes

$$C^{\perp} = \{00, 12, 21\}.$$

Here the vectors 12 or 21 forms a basis of $C^{\perp}$. Hence we can take $H = [1 \quad 2]$ or $H = [2 \quad 1]$

Theorem 2.3.4. *Let C be an (n,k) code over F and let H be a parity check matrix of C. Then*

$$C = \{u \in F^n \mid uH^{\top} = 0 = Hu^{\top}\}$$

Proof. As we have seen that if G is a generator matrix of C then the null space of G is $C^{\perp}$. Now H is a generator matrix of $C^{\perp}$ and hence the null space of H is $(C^{\perp})^{\perp} = C$. Hence $u \in C$ if and only if $Hu^{\top} = 0$ or equivalently $uH^{\top} = 0$. □

Example 2.3.5. Let $C = \{000, 001\}$

$$(\mathbb{Z}_2)^3 = \{000, 100, 010, 001, 110, 101, 011, 111\}$$

its dual code is $C^{\perp} = \{000, 100, 010, 110\}$. Let us take $H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

at $u = [000]$

$$\begin{aligned} uH^{\top} =& [000] \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}^{\top} \\ =& [000] \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \\ =& [0\ 0] \end{aligned}$$

at $u = [001]$

$$\begin{aligned} uH^{\top} =& [001] \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}^{\top} \\ =& [001] \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \\ =& [0\ 0] \end{aligned}$$

Theorem 2.3.6. *Let C be an (n,k) code. Let G and H be generator and parity check matrix of C. Then*

$$GH^{\top} = 0 = HG^{\top}$$

conversely, suppose G is a k× n matrix of rank k and H is a $(n-k) \times n$ matrix of rank $n-k$, such that $GH^{\top} = 0$. Then H is a parity check matrix of the code C iff G is the generator matrix of C .

Proof. As by theorem 2.3.4 $\forall\ u \in C$

$$uH^{\top} = 0.$$

Here in particular, $G_iH^\top = 0 \ \forall \ i = 1, 2, \ldots, k$, where each G_i is a row of generator matrix and hence $GH^\top = 0$. Taking transpose, we get $HG^\top = 0$.

To prove second part of the theorem let G be $k \times n$ matrix of rank k and H is an $(n-k) \times n$ matrix of rank $n-k$, with $GH^\top = 0$. Suppose H is a parity check matrix of C. Then $G_iH^\top = 0 \ \forall \ i = 1, 2, \ldots, k$. Hence $G_1, G_2, \ldots, G_k \in C$. Since rank of G is k, $G_1, G_2, \ldots, G_k$ are linearly independent and hence form a basis of C ($\because \dim C = k$) . This proves that G is a generator matrix of C. Now suppose that G is a generator matrix of C. Then G is the parity check matrix of the dual code $C^\perp$ and by the preceding theorem $\forall \ v \in C^\perp \ vG^\top = Gy^\top = 0$

Suppose $GH^\top = 0$ then by taking transpose $HG^\top = 0$, $H_iG^\top = 0 \ \forall \ i = 1, 2, \ldots, n-k$. Hence $H_1, H_2, \ldots H_k \in C^\top$. Since rank of H is $n-k$, $H_1, H_2, \ldots, H_k$ are linearly independent and form basis for $C^\perp$($\because \dim C^\perp = n-k$) . This proves that H is the generator matrix for the dual code $C^\perp$ and hence H is the parity check matrix for C. □

Example 2.3.7. In previous example $C = \{000, 001\}$

$$C^\perp = \{000, 100, 010, 110\}$$

let $G = [001]$ and

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

$$GH^\top = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}^\top$$

$$= [0 \ 0]$$

Let G be generator matrix of C and G' be a matrix obtained as a result of performing elementary row operations on G. Then every row of G is a linear combination of the rows of G' and conversely. So G, G' have same row space C. Hence G' is also a generator matrix of C.

Conversely G and G' are both generating matrix of C then each can be obtained by elementary row operations on the other.

2.3.1 Canonical generator matrix

Here we will define the generator matrices for a code that are obtained by performing row operations on any generator matrix.

Definition 2.3.8. Let C be an (n,k) code and suppose that first k columns of a matrix G are linearly independent. Then by performing elementary row operations, we can transform G to a row -reduced echelon form $G^* = [I_k : A]$, where I_k is the identity matrix of order k and A is some $k \times (n-k)$ matrix. G^* is called the **canonical generator matrix** of C and we say that G is in systematic or standard form.
Now let $H^* = [-A^\top : I_n - k]$. Then H^* is an $(n-k) \times n$ matrix of rank $n-k$ hence H^* is a parity check matrix of C called the **canonical parity check matrix** of C and we say that H is in systematic or standard form.. Also

$$G^*(H^*)^\top = 0$$

as G^* is obtained from the generator matrix G of C. G^* is also a generator matrix of C.

From above discussion and Theorem 2.3.6 we have the following result.

Theorem 2.3.9. *Let C be an (n,k) − code, if C has a canonical generator matrix $G = [I_k : A]$, then $H = [-A^\top : I_{n-k}]$ is the canonical parity check matrix of C. Conversely if $H = [B : I_{n-k}]$ is a parity check matrix of C, then $G = [I_k : -B^\top]$ is a generator matrix of C.*

Example 2.3.10. Let

$$\begin{aligned} C =& \{0000, 1000\} \text{ be } (4,1) \text{ code.} \\ (\mathbb{Z}_2)^4 =& \{0000; 1000, 0100, 0010, 0001, 1100, 1010, 1001, \\ & 0101, 0011, 0110, 1110, 1101, 1011, 0111, 1111\} \\ C^{\perp} =& \{0000, 0100, 0010, 0001, 0101, 0011, 0110, 0111\}, \\ & be(4,3) \, \text{code} \end{aligned}$$

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

be the parity check matrix. By performing elementary row operations we can find canonical generator matrix.

$$H = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} by\, R_1 - R_3$$

$$H = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} by\, R_2 - R_1$$

$$H^* = \begin{bmatrix} 0 & : 1 & 0 & 0 \\ 0 & : 0 & 1 & 0 \\ 0 & : 0 & 0 & 1 \end{bmatrix} by\, R_3 - R_2$$

$$\begin{aligned} H^* =&[B \ : \ I_3] \\ G^* =&[I_1 : -B^{\mathsf{T}}] \\ =&[1 \ : 0\,0\,0] \text{ And also} \end{aligned}$$

$$G^*(H^*)^{\mathsf{T}} = \begin{bmatrix} 1 & : & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & : 1 & 0 & 0 \\ 0 & : 0 & 1 & 0 \\ 0 & : 0 & 0 & 1 \end{bmatrix}$$

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

$$=[0\ 0\ 0]$$

2.4 Reed-Muller codes

Reed- Muller codes were formulated by D.E.Muller and I.S.Reed in 1954. They are among the oldest and well known codes. They have several useful properties. They form an infinite family of codes and larger Reed Muller codes can be constructed from smaller ones. One of the major advantage to creating and using Reed- Muller codes is their relative simplicity to encode messages and decode received messages.

2.4.1 First order Reed-Muller codes

Definition 2.4.1. The (first order) Reed Muller codes $R(1,m)$ are binary codes defined for all integers $m \geq 1$ recursively by:

1. $R(1,1) = \{00, 01, 10, 11\} = Z_2^2$;

2. For $m > 1$ $\;R(1,m) = \{(u,u),(u,u+1) : u \in R(1,m-1)$ and $1 =$ all 1 vector

Example 2.4.2. To find $R(1,2)$ code we have by definition

$$\begin{aligned} R(1,2) =& \{(u,u),(u,u+1)\} \text{ where } u \in R(1,1) \text{ here } m = 2 \\ \text{as } R(1,1) =& \{00,01,10,11\} \\ \text{then } R(1,2) =& \{0000,0101,1010,1111,0011,0110,1001,1100\} \end{aligned}$$

Example 2.4.3. To find $R(1,3)$ code we have by definition

$$\begin{aligned} R(1,3) =& \{(u,u),(u,u+1)\} \text{ where } u \in R(1,2) \text{ here } r = 1, m = 3 \\ \text{as } R(1,1) =& \{00,01,10,11\} \\ R(1,2) =& \{0000,0101,1010,1111,0011,0111,1011\} \\ \text{then } R(1,3) =& \{00000000,01010101,10101010,11111111,00110011,10011001, \\ & 11001100,00001111,01011010,10100101,11110000,00111100, \\ & 01101001,10010110,11000011\} \end{aligned}$$

2.4.2 rth order Reed Muller code

The zeroth order Reed Muller code R(0 , m) is defined to be the repetition code $\{0,1\}$ of length 2^m. For any $r \geq 2$ the rth order Reed Muller code R(r,m) is defined recursively by

$$R(r,m) = \begin{cases} Z_2^{2r} & \text{if } m = r; \\ (u, u+v) : u \in R(r, m-1), v \in R(r-1, m-1) & \text{if } m > r. \end{cases}$$

Example 2.4.4. To find $R(2,3)$ code we need $R(2,2)$ and $R(1,2)$

$$\begin{aligned} R(2,3) =& \{(u,u+v) : u \in R(2,2), v \in R(1,2)\} \\ R(1,2) =& \{0000,0101,1010,1111,0011,0110,1011\} \\ R(2,2) =& \{Z_2^4\} \\ R(2,2) =& \{0000,0001,0010,0011,0100,0101,0110,0111, \\ & 1000,1001,1010,1011,1100,1101,1110,1111\} \end{aligned}$$

v=0000	**v=0101**	**v=1010**	**v=1111**	**v=0011**	**v=0110**	**v=1001**	**v=1100**
00000000	00000101	00001010	00001111	00000011	00000110	00001001	00001100
00010001	00010100	00011011	00011110	00010010	00010111	00011000	00011101
00100010	00100111	00101000	00101101	00100001	00100100	00101011	00101111
00110011	00110110	00111001	00111100	00110000	00110101	00111010	00110011
01000100	01000001	01001110	01001011	01000111	01000010	01001101	01000111
01010101	01010000	01011111	01011010	01010110	01010011	01011100	01010111
01100110	01100011	01101100	01101001	01100101	01100000	01101111	01100111
01110111	01110010	01111101	01111000	01110100	01110001	01111110	01110111
10001000	10001101	10000010	10000111	10001011	10001110	10000001	10001011
10011001	10011100	10010011	10010110	10011010	10011111	10010000	10011011
10101010	10101111	10100000	10100101	10011010	10011111	10010000	10011011
10111011	10111110	10110001	10110100	10111000	10111101	10110001	10111011
11001100	11001001	11000110	11000011	11001111	11001010	11000101	11001111
11011101	11011000	11010111	11010010	11011110	11011011	11010100	11011111
11101110	11101011	11100100	11100001	11101101	11101000	11100111	11101111
11111111	11111010	11110101	11110000	11111100	11111001	11110110	11111111

2.5 Polynomial ring and algebraic codes

Let F be a finite field. We considered it in two different ways in the first chapter we have reviewed the concept of polynomial rings and now in the pervious sections of this chapter we came through the codes over F. So it is a natural question that can we related these two structures depending upon F. We can identify any codeword $a_0a_1, \ldots a_{n-1}$ in F^n with a polynomial

$$a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$$

in $F[x]$. Now what will happen with the set of polynomials $C(x)$ that are related to linear codes. To answer this question we have the following proposition.

Proposition 2.5.1. *If C is a linear code in F^n. Then $C(x)$ is a subspace of $F[x]$.*

Proof. Let C be linear, that is, if $a_0a_1, \ldots a_{n-1}$ and $b_0b_1, \ldots b_{n-1}$ are codewords in C. Then for all $\alpha, \beta \in F$

$$\alpha(a_0a_1, \ldots a_{n-1}) + \beta(b_0b_1, \ldots b_{n-1}) \in C.$$

$$\Rightarrow (\alpha a_0 + \beta b_0)(\alpha a_1 + \beta b_1) \ldots (\alpha a_{n-1} + \beta b_{n-1}) \in C.$$

Thus,

$$\alpha(a_0 + a_1x + \ldots + a_{n-1}x^{n-1}) + \beta(b_0 + b_1x + \ldots + b_{n-1}x^{n-1})$$

$$= (\alpha a_0 + \beta b_0) + (\alpha a_1 + \beta b_1)x + \ldots + (\alpha a_{n-1} + \beta b_{n-1})x^{n-1} \in C(x).$$

We get that $C(x)$ is a subspace of $F[x]$. □

Example 2.5.2. Consider the code $C = \{000, 110, 011, 101\}$ and the corresponding set of polynomials $\{0, 1+x, x+x^2, 1+x^2\}$. In this set the highest power of x is 2. Now what will happen if the power of x is greater than 2. For example if $p(x) = x^3 - 1$ in other words x^3 is equivalent to 1. Then

$$x(1+x) = x + x^2$$

$$x(1+x^2) = x + x^3 = x + 1$$

$$x(x+x^2) = x^2 + x^3 = x^2 + 1.$$

Imply the polynomials are equivalent to each other modulo $p(x)$.

From this example we have the following conclusion.

Remark 2.5.3. In a cyclic code C of length n, the product $xp(x)$ modulo $x^n - 1$ produces another code polynomial in $C(x)$, that is, exactly the right cyclic shift of $p(x)$. Consider the code polynomial

$$p(x) = c_0 + c_1x + \; + c_{n-1}x^{n-1}.$$

Multiplying $p(x)$ by x modulo $x^n - 1$ gives

$$p'(x) = c_0x + c_1x^2 + \; + c_{n-1}x^n = c_0x + c_1x^2 + \; + c_{n-1} \text{ modulo } x^n - 1.$$

The codeword associated with $p'(x)$ is $(c_{n-1}, c_0, \ldots, c_{n-2})$, which is the right cyclic shift of the codeword associated with $p(x)$.

Theorem 2.5.4. *A linear code C of length n over a finite field F is cyclic if and only if C satises the following two conditions:*

- *If $p(x)$ and $q(x)$ are code polynomials in C, then $p(x) - q(x) \in C(x)$;*
- *If $p(x)$ is a code polynomial in $C(x)$ and $r(x)$ is any polynomial of degree less than n, then $r(x)p(x) \in C(x)$.*

Proof. Suppose C is a cyclic linear code. Then from Proposition 2.5.1 we have then $p(x) - q(x) \in C(x)$

Let $p(x) \in C(x)$ and

$$r(x) = r_0 + r_1 x + \ldots + r_{n-1}x^{n-1}$$

be a polynomial in $F[x]$. Now C is cyclic so

$$xp(x) \in C(x)$$

$$\Rightarrow x^2p(x) = x(xp(x)), \ldots, x^{n-1}p(x) = x(x^{n-2}p(x)) \in C(x).$$

The linearity of C gives us

$$r(x)p(x) = r_0p(x) + r_1xp(x) + \ldots + r_{n-1}x^{n-1}p(x) \in C(x).$$

Conversely, assume that $p(x) - q(x) \in C(x)$ and $r(x)p(x) \in C(x)$ for all $p(x), q(x) \in C(x)$ and $r(x)$ the polynomials of degree less than n. If we take $r(x)$ to be a scalar in F, the conditions imply that $C(x)$ is a linear which imply C is linear.

If we take $r(x) = x$, then the second condition implies that $C(x)$ is a cyclic code, that is, C is cyclic. □

Remark 2.5.5. A linear code C is cyclic if and only if $C(x)$ is an ideal in $F[x]$.

From Remark 2.5.3, we have if C is a cyclic code then every polynomial in $C(x)$ is equivalent to another polynomial in $C(x)$ modulo $x^n - 1$. Now we will focus on the set $F[x]/(x^n - 1)$, which can be informally defined as the set of all polynomials of degree less than $n \geq 1$ in the variable x with coefficients from the finite field F under polynomial addition and multiplication modulo $x^n - 1$. The set is a commutative ring with identity polynomial $e(x) = 1$.

Theorem 2.5.6. *The cyclic codes of length n over F correspond precisely to the ideals in the ring $F[x]/(x^n - 1)$.*

Proof. Suppose C is a cyclic code of length n over F. Then, the corresponding set of code polynomials $C(x)$ contains polynomials of degree less than n, also every polynomial in $C(x)$ is equivalent to another polynomial in $C(x)$ modulo $x^n - 1$ which imply that $C(x)$ is contained in $F[x]/(x^n - 1)$. From Theorem 3.5.5, we have $C(x)$ is an ideal in $F[x]/(x^n - 1)$.

On the other hand, suppose that I is an ideal in $F[x]/(x^n - 1)$. Then its elements are polynomials of degree less than n, and by definition of ideals,

$$a(x) - b(x) \in I \text{ whenever } a(x), b(x) \in I;$$

and

$$r(x)a(x) \in I \text{ whenever } r(x) \in F[x]/(x^n - 1) \text{ and } a(x) \in I.$$

Thus, we get that I is cyclic which imply that the corresponding code is cyclic over F. □

Theorem 2.5.7. *Let C be an (n, k) cyclic code corresponding to an ideal I in $F[x]/(x^n - 1)$. Then the following statements are true:*

1. *There exists a unique monic polynomial $g(x) \in I$ of minimal degree $r < n$, called the generator polynomial of C*

2. *I is a principal ideal with generator $g(x)$, so that every code polynomial $p(x)$ can be expressed uniquely as $p(x) = m(x)g(x)$, where $g(x)$ is the generator polynomial and $m(x)$ is a polynomial of degree less than $(n-r)$ in $F[x]$.*

3. *The generator polynomial $g(x)$ divides $x^n - 1$ in $F[x]$.*

Proof. 1. Let I be an ideal in $F[x]/(x^n - 1)$. As the degree of polynomials is bounded below by 0, there is certainly at least one polynomial of minimum degree in I. Since the scalar multiplication of any polynomial in an ideal I remains in I, we can find a monic polynomial of minimum degree in I; denoted by $g(x)$ of degree $r < n$.

Suppose that h(x) is another monic polynomial of minimum degree r in I. Since I is an ideal,

$$\Rightarrow h(x) - g(x) \in I.$$

Since these polynomials have the same degree and are monic, their difference must be of lower degree. However, this contradicts the minimality of r. Therefore, there cannot be two monic polynomials of minimum degree in I.

2. Let $f(x)$ be an arbitrary element of I, so that $f(x)$ is represented by a polynomial of degree less than n. As degree of $g(x)$ is less than degree of $f(x)$. So, by the Division Algorithm in $F[x]$, we can write

$$f(x) = q(x)g(x) + r(x),$$

where $q(x), r(x) \in F[x]$ with $degr(x) < degg(x)$ or $r(x) = 0$.

Since $f(x)$ has degree less than n, clearly $q(x)$ and $r(x)$ must also have degree less than n. From above Theorem I corresponds to a cyclic code and since $g(x)$ is a code polynomial, we get that

$$q(x)g(x) \in I.$$

As $f(x)$ is also in I and I is an ideal

$$\Rightarrow f(x) - q(x)g(x) = r(x) \in I.$$

However, $degr(x) < degg(x)$ contradicts the minimality of the degree of $g(x)$ in I. Therefore, $r(x)$ must be equivalent to 0, implying that $f(x)$ is indeed a multiple of g(x).

3. Suppose that the unique monic polynomial of minimum degree in I does not divide $x^n - 1$ in $F[x]$. By the Division Algorithm, we can write

$$x^n - 1 = q(x)g(x) + r(x),$$

where $q(x), r(x) \in F[x]$ and $degr(x) < degg(x)$. That is,

$$r(x) = x^n - 1 - q(x)g(x) \in F[x],$$

we see that in $F[x]/x^n - 1$, $r(x)$ is congruent to $-q(x)g(x)$. Since $g(x) \in I$ and $-q(x) \in F[x]$, we have $-q(x)g(x) \in I$. Therefore, $r(x)$ must also be in I. However, by the Division Algorithm, $degr(x) < degg(x)$, which contradicts the minimality of the degree of $g(x)$ in I. Therefore, $r(x)$ must be 0, implying that $g(x)$ indeed divides $x^n - 1$. □

Chapter 3

Algebraic codes over Max-Min algebra

This chapter is concerned with the algebraic codes over Max-Min algebra. Recall that a Max-Min algebra is a partially ordered set equipped with maximum and minimum as the two binary operations. Throughout this chapter S is a finite Max-Min algebra endowed with additive and multiplicative identity.

3.1 Linear codes

As we know that S^n is a semivector space over S (see Example 1.2.7). A subspace of S^n is called a linear code of length n over S.

Example 3.1.1. Consider $\mathbb{Z}_2$, then the code $\{000, 111\}$ is linear of length 3. Because

$$000 + 111 = (0 \oplus 1)(0 \oplus 1)(0 \oplus 1) = max\{0,1\}max\{0,1\}max\{0,1\} = 111$$

$$111 + 111 = (1 \oplus 1)(1 \oplus 1)(1 \oplus 1) = max\{1,1\}max\{1,1\}max\{1,1\} = 111.$$

Similarly, $\{000, 110, 101, 111\}$ is a linear code of length 3. However, the set $\{000, 110, 101\}$ is not linear as

$$110 + 101 = (1 \oplus 1)(1 \oplus 0)(0 \oplus 1) = max\{1,1\}max\{1,0\}max\{0,1\} = 111$$

and $111 \notin \{000, 110, 101\}$.

Example 3.1.2. Consider $\mathbb{Z}_3$ as defined in Example 1.2.4 then the code $\{000, 111, 222\}$ is linear of length 3. Similarly, $\{000, 120, 102, 222, 111, 110, 101, 122, 121, 112\}$ is a linear code of length 3.

Proposition 3.1.3. *Every linear code over S contains the zero codeword.*

Proof. Let $\mathcal{C}$ be a code of length p over S. If $a_1a_2, \dots a_p$ be a codeword then

$$0(a_1a_2, \dots a_p) = min\{0, a_1\}min\{0, a_2\} \dots min\{0, a_p\} = 00 \dots 0.$$

The linearity of $\mathcal{C}$ imply that $00 \dots 0 \in \mathcal{C}$. □

3.1.1 Generator matrix

In this section we are going to define generator matrix then we will give some results and example. As we are dealing with S^p, that is, an p-dimensional semivector space over S. So every subspace of S^p is also finite dimensional. By (p,r)-code we mean a code of length p and dimension r.

Definition 3.1.4. Let $\mathcal{C}$ be a linear (p,r)-code. Let $\mathcal{G}$ be a $r \times p$ matrix whose rows form a basis of $\mathcal{C}$. Then $\mathcal{G}$ is called a generator matrix of the code $\rfloor$.

1. If $\mathcal{V}$ be semivector space and $B = \{u_1, u_2, \dots, u_r\}$ is a basis for a semivector space $\mathcal{V}$ then any vector w of $\mathcal{V}$ can be written uniquely as a linear combination of the vectors of of B. Let $x_1, x_2, \dots, x_r \in S$ be scalars such that vector w can be written as

$$w = x_1u_1 + x_2u_2 + \dots + x_ru_r$$

2. Let $\mathcal{G}$ be a matrix which generate code $\mathcal{C}$ than rows of $\mathcal{G}$ are linearly independent.

3. From a generator matrix we can find a entire code.

Following are some results:

Theorem 3.1.5. *Let $\mathcal{C}$ be an (p,r)-code over S. Let $\mathcal{G}$ be a generator matrix of $\mathcal{C}$. Then*

$$\mathcal{C} = \{u\mathcal{G} \text{ such that } u \in S^r\}.$$

Proof. Let $\mathcal{G}$ be the generator matrix of an (p,r)-code over S. Then by definition the rows of $\mathcal{G}$ form basis for $\mathcal{C}$ so every $u \in \mathcal{C}$ can be written as a linear combination of the rows of $\mathcal{G}$ that is,

$$x = u_1\mathcal{G}_1 + u_2\mathcal{G}_2 + \cdots + u_k\mathcal{G}_r$$

where $u_1, u_2, \ldots, u_r \in S$ and $\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_r$ are the rows of $\mathcal{G}$, consider the vector $u = [u_1, u_2, \ldots, u_r] \in S^r$

$$\begin{aligned} x =& u_1\mathcal{G}_1 + u_2\mathcal{G}_2 + \ldots + u_r\mathcal{G}_r \\ =& [u_1, u_2, \ldots, u_r] \begin{bmatrix} \mathcal{G}_1 \\ \mathcal{G}_2 \\ \vdots \\ \mathcal{G}_r \end{bmatrix} \\ =& u\mathcal{G} \end{aligned}$$

Thus $\qquad \mathcal{C} = \{u\mathcal{G} \text{ such that } u \in S^r\}$

□

Let us take an example.

Example 3.1.6. To generate (3,2) code

$$\mathcal{C} = \{000 , 100 , 001 , 101\}.$$

we have to encode message of length r. Here $r = 2$ then we have 2^r=2^2=4 codewords. As $r = 2$ so we have to encode message of length 2. Here possible pairs of length 2 are [0 0], [1 0], [0 1], [1 1]. Generator matrix should be of $r \times p$ matrix, so in this example generator matrix is 2×3 matrix. Let us take

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

at $u = [00]$

$$\begin{aligned} u\mathcal{G} &= \begin{bmatrix} 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ &= [0 \odot 1 \oplus 0 \odot 0 \;\; 0 \odot 0 \oplus 0 \odot 0 \;\; 0 \odot 0 \oplus 0 \odot 1] \\ &= [max\{min\{0,1\}, min\{0,0\}\} \;\; max\{min\{0,0\}, min\{0,0\}\} \\ &\quad max\{min\{0,0\}, min\{0,1\}\}] \\ &= [0\ 0\ 0] \end{aligned}$$

at $u = [10]$

$$\begin{aligned} u\mathcal{G} &= \begin{bmatrix} 1 & 0 \end{bmatrix} \odot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ &= [1 \odot 1 \oplus 1 \odot 0 \;\; 1 \odot 0 \oplus 0 \odot 0 \;\; 1 \odot 0 \oplus 0 \odot 1] \\ &= [1\ 0\ 0] \end{aligned}$$

at $u = [01]$

$$\begin{aligned} u\mathcal{G} &= \begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ &= [0 \odot 1 \oplus 1 \odot 0 \;\; 0 \odot 0 \oplus 1 \odot 0 \;\; 0 \odot 0 \oplus 1 \odot 1] \\ &= [0\ 0\ 1] \end{aligned}$$

at $u = [11]$

$$\begin{aligned} u\mathcal{G} &= \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ &= [1 \odot 1 \oplus 1 \odot 0 \;\; 1 \odot 0 \oplus 1 \odot 0 \;\; 1 \odot 0 \oplus 1 \odot 1] \\ &= [1\ 0\ 1] \end{aligned}$$

Code generated from this generator matrix with four codewords is

$$\mathcal{C} = \{000\ , 100\ , 001\ , 101\}.$$

Example 3.1.7. Consider $\mathbb{Z}_3$ as defined in Example 1.2.4 then the linear code $\{000, 120, 102, 222, 111, 110, 101, 122, 121, 112\}$ is generated by $120, 102, 222$. Thus for

$$\mathcal{G} = \begin{bmatrix} 1 & 2 & 0 \\ 1 & 0 & 2 \\ 2 & 2 & 2 \end{bmatrix}$$

we have

$$\begin{array}{lll}
[000]\mathcal{G} = [000] & [100]\mathcal{G} = [110] & [010]\mathcal{G} = [101] \\
[001]\mathcal{G} = [111] & [110]\mathcal{G} = [111] & [101]\mathcal{G} = [111] \\
[011]\mathcal{G} = [111] & [111]\mathcal{G} = [111] & [002]\mathcal{G} = [222] \\
[020]\mathcal{G} = [102] & [200]\mathcal{G} = [120] & [220]\mathcal{G} = [122] \\
[202]\mathcal{G} = [222] & [022]\mathcal{G} = [222] & [222]\mathcal{G} = [222] \\
[102]\mathcal{G} = [222] & [120]\mathcal{G} = [112] & [012]\mathcal{G} = [222] \\
[112]\mathcal{G} = [222] & [121]\mathcal{G} = [112] & [211]\mathcal{G} = [121] \\
[122]\mathcal{G} = [222] & [212]\mathcal{G} = [222] & [221]\mathcal{G} = [122] \\
[021]\mathcal{G} = [112] & [201]\mathcal{G} = [121] & [210]\mathcal{G} = [121]
\end{array}$$

Remark 3.1.8. 1. The generator matrix of code is unique.

2. If $m \in S^r$ is a message word then we can find a code $\mathcal{C}$ by multiplying this message word by a matrix $\mathcal{G}$ which is generator of code $\mathcal{C}$. Thus we have a mapping $e : S^r \to \mathcal{C}$ which is called encoding mapping.

3.2 Dual code

In this section we define dual code and discuss how code $\mathcal{C}$ and dual code are related.

Definition 3.2.1. Let $\mathcal{C}$ be (p,r)-code over S. Then the dual code of $\mathcal{C}$ is defined to be

$$\mathcal{C}^{\perp} = \{x \in S^p \text{ such that } x.y = 0 \ \forall \ y \in \mathcal{C}\}.$$

Where

$$x.y = x_1 \odot y_1 \oplus x_2 \odot y_2 \oplus \ldots \oplus x_p \odot y_p.$$

Example 3.2.2. Let $\mathcal{C} = \{000, 001\}$

$$(\mathbb{Z}_2)^3 = \{000, 100, 010, 001, 110, 101, 011, 111\}$$

As $\mathcal{C}^{\perp} = \{x \in S^p \mid x \cdot y = 0 \ \forall \ y \in \mathcal{C}\}$. Then

$$[000] \cdot [000] = [0 \odot 0 \oplus 0 \odot 0 \oplus 0 \odot 0] = 0$$

$$[001] \cdot [000] = [0 \odot 0 \oplus 0 \odot 0 \oplus 1 \odot 0] = 0$$

$$[000] \cdot [100] = [0 \odot 1 \oplus 0 \odot 0 \oplus 0 \odot 0] = 0$$

$$[001] \cdot [100] = [0 \odot 1 \oplus 0 \odot 0 \oplus 1 \odot 0] = 0$$

$$[000] \cdot [010] = [0 \odot 0 \oplus 0 \odot 1 \oplus 0 \odot 0] = 0$$

$$[001] \cdot [010] = [0 \odot 0 \oplus 0 \odot 1 \oplus 1 \odot 0] = 0$$

$$[000] \cdot [001] = [0 \odot 0 \oplus 0 \odot 0 \oplus 0 \odot 1] = 0$$

$$[001] \cdot [001] = [0 \odot 0 \oplus 0 \odot 0 \oplus 1 \odot 1] = 1$$

$$[000] \cdot [110] = [0 \odot 1 \oplus 0 \odot 1 \oplus 0 \odot 0] = 0$$

$$[001] \cdot [110] = [0 \odot 1 \oplus 0 \odot 1 \oplus 1 \odot 0] = 0$$

$$[000] \cdot [101] = [0 \odot 1 \oplus 0 \odot 0 \oplus 0 \odot 1] = 0$$

$$[001] \cdot [101] = [0 \odot 1 \oplus 0 \odot 0 \oplus 1 \odot 1] = 1$$

$$[000] \cdot [011] = [0 \odot 0 \oplus 0 \odot 1 \oplus 0 \odot 1] = 0$$

$$[001] \cdot [011] = [0 \odot 0 \oplus 0 \odot 1 \oplus 1 \odot 1] = 1$$

$$[000] \cdot [111] = [0 \odot 1 \oplus 0 \odot 1 \oplus 0 \odot 1] = 0$$

$$[001] \cdot [111] = [0 \odot 1 \oplus 0 \odot \oplus 1 \odot 1] = 1$$

hence

$$\mathcal{C}^{\perp} = \{000, 100, 010, 110\}$$

Example 3.2.3. Consider $\mathcal{C} = \{0000, 0010\}$. As

$$(\mathbb{Z}_2)^4 = \{0000, 1000, 0100, 0010, 0001, 1100, 1010, 1001, 0101, 0011, 0110, 1110,$$

$$1101, 1011, 0111, 1111\}$$

then dual code of $\mathcal{C}$ is

$$\mathcal{C}^{\perp} = \{0000, 1000, 0100, 0001, 1100, 0101, 1001, 1101\}$$

Hence $\mathcal{C}^{\perp}$ is $(4,3)$-code generated by $1000, 0100, 0001$.

Lemma 3.2.4. *Let $\mathcal{C}$ be a linear code in S^p and $\mathcal{G}$ be the matrix which generate $\mathcal{C}$. Then $x \in \mathcal{C}^{\perp}$ if and only if $x\mathcal{G}^{\top} = 0$.*

Proof. Let $\mathcal{G} = \begin{bmatrix} g_1 \\ \vdots \\ g_r \end{bmatrix}$ where g_i is some basis of $\mathcal{G}$ and $x\mathcal{G} = (xg_1, \dots, xg_r)$ if $x \in \mathcal{C}^{\perp}$ then $xg_i = 0$ for every i, which implies that $x\mathcal{G}^{\top} = 0$.
Conversely, if $x\mathcal{G}^{\top} = 0$ then $xg_i = 0$ for every i. If $c \in \mathcal{C}$ then

$$\begin{aligned} c &= \sum_i \lambda_i g_i \text{ for some} \lambda_i \in S \\ x.c &= x(\sum_i \lambda_i g_i) \\ &= \sum_i \lambda_i (x_i \odot g_i) \\ &= 0 \end{aligned}$$

We get that $x \in \mathcal{C}^{\perp}$. □

Remark 3.2.5. If $\mathcal{G}$ is a matrix that is generator of $\mathcal{C}$, then the null space of $\mathcal{G}$ is $\mathcal{C}^{\perp}$ that is $\forall\ x \in \mathcal{C}^{\perp}\ \mathcal{G}x^{\top} = 0$ or equivalently $x\mathcal{G}^{\top} = 0$.

Example 3.2.6. let $\mathcal{C} = \{000, 001\}$ be (3,1)-code $\mathcal{C}^{\perp} = \{000, 100, 010, 110\}$ be dual (3,2)-code.

$$\mathcal{G} = [001]$$

then $\forall\ \ x \in \mathcal{C}^{\perp}$ at $x = [000]$

$$\begin{aligned}\mathcal{G}x^{\top} &= \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \\ &= [0 \odot 0 \oplus 0 \odot 0 \oplus 1 \odot 0] \\ &= 0\end{aligned}$$

at $x = [100]$

$$\begin{aligned}\mathcal{G}x^{\top} &= \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \\ &= [0 \odot 1 \oplus 0 \odot 0 \oplus 1 \odot 0] \\ &= 0\end{aligned}$$

at $x = [010]$

$$\begin{aligned}\mathcal{G}x^{\top} &= \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \\ &= [0 \odot 0 \oplus 0 \odot 1 \oplus 1 \odot 0] \\ &= 0\end{aligned}$$

at $x = [110]$

$$\begin{aligned}\mathcal{G}x^{\top} &= \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \\ &=[0 \odot 1 \oplus 0 \odot 1 \oplus 1 \odot 0] \\ &=0\end{aligned}$$

Let us discuss some results:

Proposition 3.2.7. *$\mathcal{C}^{\perp}$ is a linear code.*

Proof. if $x, y \in \mathcal{C}^{\perp}$ then $x \cdot c = 0$ and $y \cdot c = 0$, for every $c \in \mathcal{C}$ *where* $\alpha, \beta \in S$.

Thus $(\alpha x + \beta y) \cdot c = \{\alpha[x_1, x_2, \ldots, x_p] + \beta[y_1, y_2, \ldots, y_p]\} \cdot [c_1, c_2, \ldots, c_p]$

$$= [\alpha \odot x_1 \oplus \beta \odot y_1, \alpha \odot x_2 \oplus \beta \odot y_2, \ldots, \alpha \odot x_p \oplus \beta \odot y_p] \cdot [c_1, c_2, \ldots, c_p]$$

$$= (\alpha \odot x_1 \oplus \beta \odot y_1) \odot c_1 \oplus (\alpha \odot x_2 \oplus \beta \odot y_2) \odot c_2 \oplus \ldots \oplus (\alpha \odot x_p \oplus \beta \odot y_p) \odot c_p$$

$$= \alpha \odot (x_1 \odot c_1 \oplus x_2 \odot c_2 \oplus \ldots \oplus x_p \odot c_p) + \beta \odot (y_1 \odot c_1 \oplus y_2 \odot c_2 \oplus \ldots \oplus y_p \odot c_p)$$

$$= \alpha \odot 0 \oplus \beta(0) \odot 0$$

$$= max\{min\{\alpha, 0\}, min\{\beta, 0\}\} = 0.$$

This implies that $\mathcal{C}^{\perp}$ is linear. □

Proposition 3.2.8. *If $\mathcal{C}$ is a code and $\mathcal{C}^{\perp}$ is dual code of $\mathcal{C}$ then $(\mathcal{C}^{\perp})^{\perp} \supseteq \mathcal{C}$.*

Proof. We will prove that code $\mathcal{C}$ and dual code $\mathcal{C}^{\perp}$ are symmetric, that is the dual of dual code is original code Let $w \in \mathcal{C}$. Thus $w \cdot z = 0 \ \forall \ z \in \mathcal{C}^{\perp}$ that if

$$w = [w_1\, w_2\, \ldots\, w_n] \text{ and } z = [z_1\, z_2\, \ldots\, z_n]$$

then

$$\begin{aligned} w \cdot z =& w_1 \odot z_1 \oplus w_2 \odot z_2 \oplus \ldots \oplus w_n \odot z_n \\ =& z_1 \odot w_1 \oplus z_2 \odot w_2 \ldots z_n \odot w_n \,(\because \text{ multiplicative is commutative}) \\ =& z \cdot w \end{aligned}$$

From above it can be seen easily that if $u \cdot v = 0$ then $v \cdot u = 0 \; \forall \; u \in \mathcal{C}$ and $v \in \mathcal{C}^{\perp}$, that is if $v \in \mathcal{C}^{\perp}$ then $u \in (\mathcal{C})$ so $\mathcal{C} \subseteq (\mathcal{C}^{\perp})^{\perp}$. □

Example 3.2.9. Let $\mathcal{C} = \{000, 001\}$

$$(\mathbb{Z}_2)^3 = \{000, 100, 010, 001, 110, 101, 011, 111\}$$

dual code of $\mathcal{C}$ is

$$\mathcal{C}^{\perp} = \{000, 100, 010, 110\}.$$

Then $(\mathcal{C}^{\perp})^{\perp} = \{000, 001\}$. Hence $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$.

3.3 Parity check matrix

In this section we discuss definition and some important results related to parity check matrix. From a parity check matrix we can check wether a codeword is valid or not.

Definition 3.3.1. Let $\mathcal{C}$ be (p,r) code. Let $\mathcal{H}$ be the matrix that generates dual code $\mathcal{C}^{\perp}$. Then $\mathcal{H}$ is said to be parity check matrix of the code $\mathcal{C}$.

Remark 3.3.2.

1. As dual of dual code is again a original code $\mathcal{C}$, so if $\mathcal{G}$ generate the code $\mathcal{C}$ than it will be a parity check matrix of dual code.

2. If $\mathcal{C}$ is an (p,r) code where p is the length and r is the dimension then the dual code is an (p,p-r) code where p is the length and $p - r$ is the dimension of dual code, so the parity check matrix of an (p,r) code is an $(p-r) \times p$ matrix $\mathcal{H}$ which is generator matrix of dual code $\mathcal{C}^{\perp}$ and rows of $\mathcal{H}$ form basis for $\mathcal{C}^{\perp}$.

Example 3.3.3. Let $\mathcal{C} = \{000, 001\}$

$$(\mathbb{Z}_2)^3 = \{000, 100, 010, 001, 110, 101, 011, 111\}$$

its dual code becomes

$$\mathcal{C}^{\perp} = \{000, 100, 010, 110\}$$

Hence

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

we can take only above matrix as a parity check matrix because this matrix generate dual code and as by definition $\mathcal{H}$ is generator matrix of dual code $\mathcal{C}^{\perp}$.

Remark 3.3.4. The parity check matrix of a code $\mathcal{H}$ is unique.

Theorem 3.3.5. *Let $\mathcal{C}$ be an (p,r) code over S, and let $\mathcal{H}$ be a parity check matrix of $\mathcal{C}$. Then*

$$\mathcal{C} = \{x \in S^p \mid x\mathcal{H}^\top = 0 = \mathcal{H}x^\top\}$$

Proof. As we have seen that if $\mathcal{C}$ is generated by $\mathcal{G}$ then the null space of $\mathcal{G}$ is $\mathcal{C}^{\perp}$. Now $\mathcal{H}$ is a matrix that generates dual code and hence the null space of $\mathcal{H}$ is $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$. Hence $x \in \mathcal{C}$ if and only if $\mathcal{H}x^\top = 0$ or we can write $x\mathcal{H}^\top = 0$. □

Example 3.3.6. Let $\mathcal{C} = \{000, 001\}$

$$(\mathbb{Z}_2)^3 = \{000, 100, 010, 001, 110, 101, 011, 111\}$$

its dual code is $\mathcal{C}^{\perp} = \{000, 100, 010, 110\}$ let us take $\mathcal{H} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

at $x = [000]$

$$x\mathcal{H}^\top = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}^\top$$

=[0 0]

at $x = [001]$

$$x\mathcal{H}^\top = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}^\top$$

=[0 0]

Theorem 3.3.7. *Let $\mathcal{C}$ be an (p,r) code. Let $\mathcal{G}$ and $\mathcal{H}$ be, generator matrix and parity check matrix of $\mathcal{C}$. Then*

$$\mathcal{G}\mathcal{H}^{\top} = 0 = \mathcal{H}\mathcal{G}^{\top}$$

Proof.

$$\forall\, x \in \mathcal{C} \quad x\mathcal{H}^{\top} = 0.$$

Here in particular, $\mathcal{G}_i\mathcal{H}^{\top} = 0 \ \forall \ i = 1, 2, \ldots, k$. Where each $\mathcal{G}_i$ is a row of generator matrix and hence $\mathcal{G}\mathcal{H}^{\top} = 0$. Taking transpose, we get $\mathcal{H}\mathcal{G}^{\top} = 0$. □

Example 3.3.8. In previous example $\mathcal{C} = \{000, 001\}$

$$\mathcal{C}^{\top} = \{000, 100, 010, 110\}$$

let $\mathcal{G} = [001]$ and $\mathcal{H} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$

$$\mathcal{G}\mathcal{H}^{\top} = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}^{\top}$$

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

$$= [0 \odot 1 \oplus 0 \odot 0 \oplus 1 \odot 0 \quad 0 \odot 1 \oplus 0 \odot 1 \oplus 0 \odot 0]$$

$$= [0\ 0]$$

Definition 3.3.9. Let $\mathcal{C}$ be an (p,r) code then generator matrix of the form $\mathcal{G}^* = [I_r : A]$ is called the **canonical generator matrix** of $\mathcal{C}$ and we say that $\mathcal{G}$ is an systematic form, where I_r is the identity matrix of order r, and A is some $r \times (p-r)$ matrix.Now let $\mathcal{H}^* = [-A^{\top} : I_{p-r}]$. Then $\mathcal{H}^*$ is an $(p-r) \times n$ matrix of rank $p - r$. Also

$$\mathcal{G}^*(\mathcal{H}^*)^{\top} = 0$$

Where $\mathcal{H}^*$ is a parity check matrix of $\mathcal{C}$ called the **canonical parity check matrix** of $\mathcal{C}$ and we say that $\mathcal{H}$ is in systematic form.

Theorem 3.3.10. *Let $\mathcal{C}$ be an $(p,r)-$ code, if $\mathcal{C}$ has a canonical generator matrix $\mathcal{G} = [I_r : A]$, then $\mathcal{H} \doteq [-A^{\top} : I_{p-r}]$ is the canonical parity check matrix of $\mathcal{C}$. conversely if $\mathcal{H} = [B : I_{p-r}]$ is a parity check matrix of $\mathcal{C}$, then $\mathcal{G} = [I_r : -B^{\top}]$ is a generator matrix of $\mathcal{C}$.*

Example 3.3.11. Let

$$\begin{aligned} \mathcal{C} =& \{0000, 1000\} \text{ be } (4,1) \text{ code.} \\ (\mathbb{Z}_2)^4 =& \{0000, 1000, 0100, 0010, 0001, 1100, 1010, 1001, \\ & 0101, 0011, 0110, 1110, 1101, 1011, 0111, 1111\} \\ \mathcal{C}^{\top} =& \{0000, 0100, 0010, 0001, 0101, 0011, 0110, 0111\}, \\ & \text{be}(4,3) \text{ code.} \end{aligned}$$

$$\mathcal{H} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{ be the parity check matrix.}$$

$$\mathcal{H}^* = \begin{bmatrix} 0 & : 1 & 0 & 0 \\ 0 & : 0 & 1 & 0 \\ 0 & : 0 & 0 & 1 \end{bmatrix}$$

$$\mathcal{H}^* = [B \, : \, I_3]$$

$$\begin{aligned} \mathcal{G}^* =& [I_1 : -B^{\top}] \\ =& [1 : 0 0 0] \text{ And also} \end{aligned}$$

$$\mathcal{G}^*(\mathcal{H}^*)^{\top} = \begin{bmatrix} 1 & : & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & : 1 & 0 & 0 \\ 0 & : 0 & 1 & 0 \\ 0 & : 0 & 0 & 1 \end{bmatrix}$$

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

$=[1 \odot 0 \oplus 0 \odot 1 \oplus 0 \odot 0 \oplus 0 \odot 0$

$1 \odot 0 \oplus 0 \odot 0 \oplus 0 \odot 1 \oplus 0 \odot 0 \quad 1 \odot 0 \oplus 0 \odot 0 \oplus 0 \odot 0 \oplus 0 \odot 1]$

$=[0\ 0\ 0]$

Note 3.3.12. In above example of dual code and parity check matrix we discussed one dimensional code consist of one codeword of all zero components and other codeword have nonzero component at one place. Dimension of dual code is specified in these codes. In all other codes we cannot specify dimension.

Let us take examples of other codes:

Example 3.3.13. Let $C = \{000, 011\}$

$$(\mathbb{Z}_2)^3 = \{000, 100, 010, 001, 110, 101, 011, 111\}$$

then dual code of C is

$$C^{\perp} = \{000, 100\}$$

Hence dual code is (3,1)-code. As we considered one dimensional code but here dimension of dual code is 1 which is not $p - r = 2$.

Example 3.3.14. Let $C = \{0000, 1001\}$ be $(3, 1)$-code.

$$(\mathbb{Z}_2)^4 = \{0000, 1000, 0100, 0010, 0001, 1100, 1010, 1001, 0101$$

$$, 0011, 0110, 1110, 1101, 1011, 0111, 1111\}$$

then dual code of C is

$$C^{\perp} = \{0000, 0100, 0010, 0110\}$$

here dimension of dual code is 2 but $p - r = 4 - 1 = 3$.

Example 3.3.15. Let $\mathcal{C} = \{0000, 0100, 1100, 0101\}$

$$(S_2)^4 = \{0000, 1000, 0100, 0010, 0001, 1100, 1010, 1001, 0101$$

$$, 0011, 0110, 1110, 1101, 1011, 0111, 1111\}$$

then dual code of $\mathcal{C}$ is

$$\mathcal{C}^{\perp} = \{0000, 0010\}$$

As here dimension of dual code is 1 not $p - r = 2$.

Hence in these example we cannot specify the dimension.

3.4 Reed Muller code

In this section we define first order and nth order Reed-Muller codes then we discuss some examples related to these codes.

Definition 3.4.1. The (first order) reed muller codes $R(1, k)$are binary codes defined for all integers $k \geq 1$ recursively by:

1. $R(1, 1) = \{00, 01, 10, 11\} = Z_2^2$

2. for $k > 1$ $R(1, k) = \{(x, x), (x, x \oplus 1)$:$x \in R(1, k-1)$ and $1 =$ all 1 vector.

Example 3.4.2. To find $R(1, 2)$ code we have by definition

$$R(1,2) = \{(x, x), (x, x \oplus 1)\} \text{ where } x \in R(1,1) \text{ here } n = 1, k = 2$$

$$\text{as } R(1,1) = \{00, 01, 10, 11\}$$

$$\text{then } R(1,2) = \{0000, 0101, 1010, 1111, 0011, 0111, 1011\}$$

Example 3.4.3: To find $R(1, 3)$ code we have by definition

$$R(1,3) = \{(x, x), (x, x \oplus 1)\} \text{ where } x \in R(1,2) \text{ here } n = 1, k = 3$$

$$\text{as } R(1,1) = \{00, 01, 10, 11\}$$

$$R(1,2) = \{0000, 0101, 1010, 1111, 0011, 0111, 1011\}$$

then R(1,3) will be:

00000000	00001111
01010101	01011111
10101010	10101111
11111111	00111111
00110011	01111111
01110111	10111111
10111011	11111111

That is,

$$R(1,3) = \{00000000, 01010101, 10101010, 00110011,$$

$$01110111, 10111011, 00001111,$$

$$01011111, 10101111, 00111111, 01111111, 10111111, 11111111\}$$

Definition 3.4.4. The zeroth order Reed Muller code R(0,k) is defined to be the repetition code $\{0,1\}$ of length 2^k. For any $n \geq 2$,the nth order Reed Muller code R(n,k) is defined recursively by

$$R(n,k) = \begin{cases} Z_2^{2n} & \text{if } k = n; \\ (x, x \oplus y) : x \in R(n,k-1), y \in R(n-1,k-1) & \text{if } k > n. \end{cases}$$

Example 3.4.5. To find $R(2,3)$ code we need $R(2,2)$ and $R(1,2)$

$$\begin{aligned} R(2,3) =& \{(x, x+y) : x \in R(2,2), y \in R(1,2)\} \\ R(1,2) =& \{0000, 0101, 1010, 1111, 0011, 0111, 1011\} \\ R(2,2) =& \{Z_2^4\} \\ R(2,2) =& \{0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, \\ & 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111\} \end{aligned}$$

y=0000	**y=0101**	**y=1010**	**y=1111**	**y=0011**	**y=0111**	**y=1011**
00000000	00000101	00001010	00001111	00000011	00000111	00001011
00010001	00010101	00011011	00011111	00010011	00010111	00011011
00100010	00100111	00101010	00101111	00100011	00100111	00101010
00110011	00110111	00111011	00111111	00110011	00110111	00111011
01000100	01000101	01001110	01001111	01000111	01000111	01001111
01010101	01010101	01011111	01011111	01010111	01010111	01011111
01100110	01100111	01101110	01101111	01100111	11001111	01101111
01110111	01110111	01111111	01111111	01110111	01110111	01111111
10001000	10001101	10001010	10001111	10001011	10001111	10001011
10011001	10011101	10011011	10011111	10011011	10011111	10011011
10101010	10101111	10101010	10101111	10101011	10101111	10101011
10111011	10111111	10111011	10111111	10111011	10111111	10111011
11001100	11001101	11001110	11001111	11001111	11001111	11001111
11011101	11011101	11011111	11011111	11011111	11011111	11011111
11101110	11101111	11101110	11101111	11101111	11101111	11101111
11111111	11111111	11111111	11111111	11111111	11111111	11111111

It can be shown in above table that the codewords are appearing repeatedly. In Example 2.4.4 of chapter 2 there are 128 codewords but here it reduces to 67 codewords. By writing each codeword only one time we have following table of codewords:

y=0000	**y=0101**	**y=1010**	**y=1111**	**y=0011**	**y=0111**	**y=1011**
00000000	00000101	00001010	00001111	00000011	00000111	00001011
00010001	00010101	00011011	00011111	00010011	00010111	
00100010	00100111	00101010	00101111	00100011	00100111	
00110011	00110111	00111011	00111111	00110011		
01000100	01000101	01001110	01001111	01000111		
01010101	01010101	01011111		01010111		
01100110	01100111	01101110	01101111	01100111		
01110111		01111111				
10001000	10001101	10001010	10001111	10001011		
10011001	10011101	10011011	10011111	10011011		
10101010	10101111	10101010		10101011	10101111	
10111011	10111111	10111011				
11001100	11001101	11001110	11001111			
11011101		11011111				
11101110	11101111					
11111111						

3.5 Polynomial over Max-Min algebra and algebraic codes

As we know that if S is a Max-Min algebra, then $S[x]$, that is, precisely the set of polynomials over S is a commutative semiring (see Section 1.2.2). Let S be a finite Max-Min algebra. Just like finite fields, we can identify any codeword $a_0a_1, \ldots a_{p-1}$ in S^p with a polynomial

$$a_0 + a_1x + \ldots + a_{p-1}x^{p-1}$$

in $S[x]$. Here are some results that relates polynomials and algebraic codes over Max-Min algebra.

Proposition 3.5.1. *If the code C is linear. Then the set of polynomials $C(x)$ is a subspace of $S[x]$.*

Proof. Let C be linear, that is, if $a_0a_1, \ldots a_{p-1}$ and $b_0b_1, \ldots b_{p-1}$ are codewords in C. Then for all $\alpha, \beta \in S$

$$\alpha(a_0a_1, \ldots a_{p-1}) + \beta(b_0b_1, \ldots b_{p-1}) \in C.$$

$$\Rightarrow (\alpha \odot a_0 \oplus \beta \odot b_0)(\alpha \odot a_1 \oplus \beta \odot b_1) \ldots (\alpha \odot a_{p-1} \oplus \beta \odot b_{p-1}) \in C.$$

Thus,

$$\alpha(a_0 + a_1x + \ldots + a_{p-1}x^{p-1}) + \beta(b_0 + b_1x + \ldots + b_{p-1}x^{p-1})$$

$$= (\alpha \odot a_0 \oplus \beta \odot b_0) + (\alpha \odot a_1 \oplus \beta \odot b_1)x + \ldots + (\alpha \odot a_{p-1} \oplus \beta \odot b_{p-1}) \in C(x).$$

We get that $C(x)$ is a subspace of $S[x]$. □

Example 3.5.2. Consider the code $C = \{000, 110, 011, 111\}$, then the corresponding set of polynomials is $\{0, 1 + x, x + x^2, 1 + x + x^2\}$.

Definition 3.5.3. If $(t_0, t_1, \ldots, t_{n-1})$ is a codeword in C and by cyclic shifting there is codeword $(t_{n-1}, t_0 \ldots, t_{n-2})$ which is also a in C then it is called cyclic code.

Remark 3.5.4. In a cyclic code C of length p, if we assume that x^p is equivalent to the multiplicative identity e in S then the product $xa(x)$ modulo $x^p - e$ gives another code polynomial in $C(x)$, that is, exactly the right cyclic shift of $a(x)$. Let us take the code polynomial

$$a(x) = c_0 + c_1x + \; + c_{p-1}x^{p-1}.$$

By multiplying $a(x)$ by x modulo $x^p - 1$ we have

$$a'(x) = c_0x + c_1x^2 + \; + c_{p-1}x^p = c_0x + c_1x^2 + \; + c_{p-1} \text{ modulo } x^p - e.$$

The codeword $(c_{p-1}, c_0, \ldots, c_{p-2})$associated with $a'(x)$, is the right cyclic shift of the codeword associated with $a(x)$.

Theorem 3.5.5. *A linear code C of length p over a finite Max-Min algebra S is cyclic if and only if $\alpha(x) + \beta(x) \in C(x)$ and $\gamma(x)\alpha(x) \in C(x)$ for all $\alpha(x), \beta(x) \in C(x)$ and for all polynomials $\gamma(x)$ of degree less than p.*

Proof. Suppose C is a cyclic linear code. Then from Proposition 3.5.1 we have then $\alpha(x) + \beta(x) \in C(x)$
Let $\alpha(x) \in C(x)$ and

$$\gamma(x) = \gamma_0 + \gamma_1 x + \ldots + \gamma_{p-1}x^{p-1}$$

be a polynomial in $S[x]$. Now C is cyclic so

$$x\alpha(x) \in C(x)$$

$$\Rightarrow x^2\alpha(x) = x(x\alpha(x)), \ldots, x^{p-1}\alpha(x) = x(x^{p-2}\alpha(x)) \in C(x).$$

The linearity of C gives us

$$\gamma(x)\alpha(x) = \gamma_0\alpha(x) + \gamma_1 x\alpha(x) + \ldots + \gamma_{n-1}x^{p-1}\alpha(x) \in C(x).$$

Conversely, assume that $\alpha(x) + \beta(x) \in C(x)$ and $\gamma(x)\alpha(x) \in C(x)$ for all $\alpha(x), \beta(x) \in C(x)$ and $\gamma(x)$ the polynomials of degree less than p. By taking $\gamma(x)$ as a scalar in S,then by condition $C(x)$ is a linear which imply C is linear. By taking $\gamma(x) = x$, then by the second condition $C(x)$ is a cyclic code, that is, C is cyclic. □

Bibliography

[1] S. S. Adams, *"Introduction to Algebraic Coding Theory"*, Cornell University, 2002.

[2] A. A. Andrade and R. Palazzo, *Linear codes over finite rings*, Tend. Computational and Applied Mathmatics **6(2)** (1962), 207-217.

[3] A. O. L. Atkin, E. Boros, K. Cechlarova, and U. N. Peled, *Power of circulants in Bottleneck algebra*, Linear Algebra and its Application **258** (1997), 137-148.

[4] E. R. Berlekamp, *"Algebraic Coding Theory"*, World Scientific Publishing, 2014.

[5] D. M. Burton, *"A First Course in Rings And Ideals"*, Addison-Wesley Educational Publishers Inc, 1970.

[6] J. B. Fraleigh, *"A First Course in Abstract Algebra"*, 7th ed, Addison Wesley Educational Publishers Inc, 2003.

[7] J. S. Golan, *"The Theory of Semirings With Application in Mathematics and Theoretical Computer Science"*, John Wiley and Sons Inc, New York, 1992.

[8] R. Hill, *"A First Course in Coding Theory"*, Oxford University Press, 1986.

[9] P. Petersen, *"Linear Algebra"*, Springer-Verlag, 2000.

[10] J. H. V. Lint, *"Introduction to Coding Theory"*, Springer-Verlag, Berlin, 1999.

[11] D. Speyer and B. Sturmfels, *Tropical mathematics*, Mathematics Magazine,University of California, Berkeley. **82(3)** (2009), 163-173.

[12] N. M. Tran, *"Topics in Tropical Linear Algebra and Applied Probability, Ph.D Thesis"*, University of California, Berkeley, 2013.