Tropical Linear Algebra and Coding Theory

By

Gul Freen

Supervised by

Dr. Sajida Kousar

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

1. Algebras, linear

2. Mathematics

Tropical Linear Algebra and Coding Theory

By
Gul Freen

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

Tropical Linear Algebra And Coding Theory

By

Gul Freen

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 ______________________
Dr Maliha Rashid
(Internal Examiner)

3 ______________________
Dr Khadija Maqbool
(Chairperson)

4 ______________________
Dr Tariq Mehmood
(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 Tropical Linear Algebra and Coding Theory submitted by Gul Freen Reg No 198-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 28/07/2016

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

Abstract

The last twenty-five years have witnessed the growth of one of the most elegant and esoteric branches of applied mathematics. Algebraic coding theory. Claude Shannon's 1948 paper A Mathematical Theory Of Communication gave the idea of coding theory, A Survey of Error-control Codes, by P.G. Farrell (the University of Kent, Great Britain) is an excellent compilation and condersation of numerous results on error-correcting codes.

In algebraic coding theory we are mainly concerned with developing methods for detecting and correcting errors that typically occur during transmission of information over a noisy channel. The main aim of this dissertation is to study the algebraic codes over Max-Plus algebra commonly known as tropical linear algebra. The study of this dissertation examines the differences between approaches adopted by algebraic codes over finite field and Max-Plus algebra. In Max-Plus algebra we work with the Max-Plus semiring together with two binary operations maximum and plus.

This dissertation consists of the three Chapters.

Chapter 01 is introductory which contains some basic definitions and related results of linear algebra and Max-Plus algebra which we will use in later Chapters.

Chapter 02 is literature review, which gives briefly concepts of algebraic codes over finite field. Finite fields are used in construction of codes and then the study of their properties. In this Chapter we review the linear codes, dual codes and their generator matrices over finite field. We will also review the

concept of Reed-Muller codes over algebraic codes by using the examples
Chapter 03 provides an introduction to the Max-Plus algebra and explain how it can be used to analyze the behavior of the algebraic codes and Reed-Muller codes over Max-Plus algebra Finally we will analyze that how we can relate ideals with codes in Max-Plus algebra

Contents

Acknowledgement

First of all, I just thank Almighty **Allah** the greatest and the kindest for all of the blessings

I would like to special thank my Supervisor **Dr.Sajida Kouser** for her guidance, advice and backing me through all my time spent under her supervision

I consider myself blessed to have such a meritorious teacher who cared so much about my work and who always responded to everything asked, with vast knowledge and kind words I can never thank her enough for everything she done for me, not for giving me knowledge only but her guidance towards life social evils and relationships and for giving me the vision to spent life in the best way possible Thank you very much for your inspiration and thoughtfulness over the past four years inclusive of MSc and MS

Very special thanks to **Dr. Khadija Maqbool** for her appreciation, her acceptance and the capability of making this academic journey so joyful Her time and above all her smile Thank you madam for being an excellent educator and I admit that its just being lucky to have a teacher like you

None of this could have been happened without my family For me family is not an important thing, its everything My sister Nadia has always been kind and supportive to me I am really thankful to her for all the times My parents, Mr and Mrs **Sher Jang** who been there for me every single time I needed them and never let me quit even in the worst case scenarios I am really thankful to my family Today I am what I am because yesterday my family stood by me a million thanks to my family

It would have been impossible to go through this significant and challenging phase of life without having friends like **Rabia**, **Asiya** and **Asra** Thanks for always being on my side for your friendship and support for sharing my dreams I do thank you my friends!

Finally, a bundle of thanks to all those who made this journey successful through their help or their criticism you gave me strength either way Especially thankful to the Department of Mathematics and Statistics IIUI for providing me the pleasant environment to embark on this research voyage and being helpful whenever need be

Author's Declaration

I, hereby declare that thesis neither as a whole nor as a part has been copied from any source. It is further declared that I have prepared this thesis entirely on the basis of my personal efforts made under the sincere guidance of my kind supervisor. No portion of the work presented in this thesis has been submitted in support of an application for any degree or qualification of this or any other institute of learning.

Gul Freen
MS Mathematics
Reg No 198-FBAS/MSMA/F14
Department of Mathematics and statistics
Faculty of Basic and Applied Sciences
International Islamic University Islamabad Pakistan

Definition 1.1.2. *A group $(G, *)$ is said to be* **abelian group** *if $a * b = b * a$ for all $a,\ b\ \in G$.*

Example 1.1.3. 1. *The Integers form a group under the operation of addition. The Real Numbers and the Complex Numbers are groups under addition and their non-zero elements form a group under multiplication.*

2. *The set of non-zero Rational Numbers form a group under the operation of multiplication.*

3. *The set of n-by-n non-singular matrix form a group under matrix multiplication.*

Definition 1.1.4. *A non-empty subset H of a group G is a* **subgroup** *if*

1. $e \in H$,

2. *If $a,\ b \in H$, then $a * b \in H$,*

3. *If $a \in H$, then $a^{-1} \in H$.*

Definition 1.1.5. *A* **ring** *is a set R together with two binary operators $+$ and $*$ satisfying the following conditions*

1. *Additive associativity: For all $a, b, c \in R$, $(a + b) + c = a + (b + c)$*

2. *Additive commutativity: For all $a, b \in R$, $a + b = b + a$,*

3. *Additive identity: There exists an element $0 \in R$ such that for all $a \in R$, $0 + a = a + 0 = a$*

4. *Additive inverse: For every $a \in R$ there exists $-a \in R$ such that*

$$a + (-a) = (-a) + a = 0$$

5. *Multiplicative associativity: For all $a, b, c \in R$,*

$$(a * b) * c = a * (b * c)$$

6. *Left and right distributivity For all $a, b, c \in R$*

$$a * (b + c) = (a * b) + (a * c) \text{ and } (b + c) * a = (b * a) + (c * a)$$

Ring may also satisfy various properties

1. Multiplicative commutativity For all $a, b \in R$, $a * b = b * a$ (a ring satisfying this property is termed a **commutative ring**)

2. Multiplicative identity There exists an element $1 \in R$ such that for all $a \neq 0 \in R$, $1 * a = a * 1 = a$ (a ring satisfying this property is termed a **ring with identity**)

Definition 1.1.6. *A **semiring** is a set together with two binary operators $(S, +, *)$ satisfying the following conditions*

1. *Additive associativity For all $a, b, c \in S$, $(a + b) + c = a + (b + c)$,*

2. *Additive commutativity For all $a, b \in S$, $a + b = b + a$,*

3. *Multiplicative associativity For all $a, b, c \in S$, $(a * b) * c = a * (b * c)$*

4. *Left and right distributivity For all $a, b, c \in S$*

$$a * (b + c) = (a * b) + (a * c) \text{ and } (b + c) * a = (b * a) + (c * a)$$

Example 1.1.7. 1. *$\mathbb{Z}$, $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ are commutative rings under the appropriate addition and multiplication*

2. *The set of all 2×2 real matrices forms a ring under the usual matrix addition and multiplication*

3. *$\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a commutative ring under usual addition and scalar multiplication*

Definition 1.1.8. *Let $(R, +, *)$ be a ring and P be a subset of R which is itself a ring under $+$ and $*$, then we call P a **subring** of R*

Definition 1.1.9. *A subset I of a ring R is called a* **left ideal** *if it is an additive subgroup of R and for all $r \in R$ and $a \in I$ we have $ra \in I$. Similarly, an additive subgroup I of R, I is called a* **right ideal** *if for all $a \in I$ and $r \in R$, $ar \in I$. An additive subgroup I of R is called an* **ideal** *if it is a left and right ideal.*

Example 1.1.10. *The zero ideal $\{0\}$ and the whole ring R are examples of two-sided ideals in any ring R.*

Definition 1.1.11. *A ring $(\mathbb{F}, +, *)$ is called a field if $(\mathbb{F}\backslash\{0\}, *)$ is a commutative group.*

Example 1.1.12. *1. The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ are examples of fields.*

2. ***Finite fields*** *(also called* ***Galois fields****) are fields with finitely many elements.*

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

Definition 1.1.13. *Let $\mathbb{F}$ be a field. A set V of element called vectors is a* ***Vector space*** *if for any $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in V$ and for any $\alpha, \beta \in \mathbb{F}$ and define a scalar multiplication $\mathbb{F} \times V \rightarrow V$ then the following axioms are satisfied.*

1. *V is an additive abelian group,*

2. $\alpha \boldsymbol{v} \in V$

3. $\alpha(\boldsymbol{u}+\boldsymbol{v}) = \alpha\boldsymbol{u} + \alpha\boldsymbol{v}$,

4. $(\alpha + \beta)\boldsymbol{u} = \alpha\boldsymbol{u} + \beta\boldsymbol{u}$,

5. $\alpha(\beta\boldsymbol{u}) = (\alpha.\beta)\boldsymbol{u}$,

6. $1\,\boldsymbol{u}=\boldsymbol{u}$.

Example 1.1.14 *1. $V = M_{m,n}(\mathbb{F})$ = all m-by-n matrices with entries in $\mathbb{F}$, where the operation of addition and scalar multiplication are defined by*

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

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

2. $V = \mathbb{F}^n = \{(x_1, x_2, \ldots, x_n\}$ all n-tuples with entries in $\mathbb{F}$, where the operation of addition and scalar multiplication are defined by

$$(x_1, x_2, x_3, \ldots, x_n) + (y_1, y_2, y_3, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

$$\alpha(x_1, x_2, x_3, \ldots, x_n) = (\alpha x_1, \alpha x_2, \alpha x_3, \ldots, \alpha x_n)$$

Definition 1.1.15. *Let V be a vector space. A non empty subset U of V is called a* **subspace** *of V if U is itself a vector space over $\mathbb{F}$ under the same operations of V.*

Theorem 1.1.16 *Let V be a vector space and $\mathbb{F}$ be a field. A subset U of V is a subspace if and only if*

1. *For any two vectors u, v ∈ U, u − v is also in U.*
2. *For any $\alpha \in \mathbb{F}$, $\mathbf{u} \in U$, $\alpha\mathbf{u}$ is also in U.*

Combining these two conditions, we have U is a subspace if and only if

$$\alpha_1 u_1 + \alpha_2 u_2 \in U$$

Example 1.1.17. *Given the vector space V, the subspaces V and {0} are each called a trivial subspace.*

Definition 1.1.18. *The vectors in a subset $T = \{v_0, v_1, \ldots, v_{n-1}\}$ of a vector space V are said to be* **linearly dependent**, *if there exists scalars, not all zero such that*

$$a_1v_1 + a_2v_2 + a_3v_3 + \ldots a_kv_k = 0$$

Where zero denote the zero vector.

Definition 1.1.19 *The vectors in set $W = \{v_0, v_1, \ldots, v_{n-1}\}$ are said to be* ***linearly independent*** *if the equation*

$$a_1v_1 + a_2v_2 + a_3v_3 + \ldots, a_kv_k = 0$$

can only be satisfied by $a_i = 0$ for $i = 0, 1, 2, \ldots, n$. This implies that no vector in the set can be represented as a linear combination of the remaining vectors in the set.

Definition 1.1.20. *Let V denote a vector space and $U = \{u_1, u_2, \ldots, u_n\}$ a subset of V. We say that U is a* ***spanning set*** *of V or that U spans V if for every vector v in V, v can be written as a linear combination of the vectors in U.*

$$span(U) = \{\Sigma_{i=0}^{n} c_iu_i \,|\, c_i \in \mathbb{R} \text{ and } u_i \in U\}$$

Definition 1.1.21 *Let V be a vector space. A linearly independent spanning set for V is called a* ***basis***

Definition 1.1.22. *The* ***dimension*** *of a vector space V is the cardinality that is, the number of vectors of a basis of V over its base field*

1.1.1 Polynomial ring

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

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

where the coefficients $p_i \in \mathbb{F}$. We will denote the set of all such expressions by $\mathbb{F}[x]$. 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 $\mathbb{F}$ and we 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 $\mathbb{F}[x]$ 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 $c_i = \sum_{i=j+k} p_j q_k$ Then under this multiplication $\mathbb{F}[x]$ 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 $p(x), q(x), r(x) \in \mathbb{F}[x]$ Thus, we get that $\mathbb{F}[x]$ is a commutative ring called the polynomial ring over F

If we define scale multiplication $\mathbb{F} \times \mathbb{F}[x] \to \mathbb{F}[x]$ as

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

for $a \in \mathbb{F}$ and $p(x) \in \mathbb{F}[x]$ Then $\mathbb{F}[x]$ becomes a vector space over $\mathbb{F}$

1.2 Max-plus Algebra

In this section we will introduce the basic definitions of Max-Plus algebra which is commonly known as tropical linear algebra semi vector spaces and semi subspaces which we will use in Chapter 03 First of all we will discuss about partially ordered sets

Definition 1 2 1 *Let S be a set A partial ordering of S is a binary relation $\leq$ satisfying the following axioms*

1 *For all $x \in S$, $x \leq x$ (reflexivity),*

2 *if $x \leq y$ and $y \leq x$, then $x = y$ (antisymmetry),*

3 *if $x \leq y$ and $y \leq z$ then $x \leq z$ (transitivity)*

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

Definition 1 2 2. *Let $\mathbb{R}$ be the set of real numbers For a $b \in \mathbb{R}^* = \mathbb{R} \cup \{-\infty\}$ then*

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

$$a \otimes b = a + b$$

The triple ordered paired $(\mathbb{R}^*, \oplus \ \otimes)$ is called Max-Plus algebra

As $\mathbb{R}$ is a partially ordered set so if S is any partially ordered set then we can define the operation of maximum and plus on S as well Now if S satisfy the following axioms

1 Addition is commutative

2 Addition and multiplication is associative

3 Multiplication distributes under addition

4 There exists an additive identity,

5 No additive inverses

Then $(S, \oplus \ \otimes)$ is a semiring (we may call it semi field)

Example 1.2 3 *Let $\mathbb{Z}_2 = \{0 \ 1\}$ Then the relation $\mathbb{Z}_2$ on S is*

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

is the partially ordered set, and under addition and multiplication is defined by

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

$\otimes$	*0*	*1*
0	*0*	*0*
1	*0*	*1*

it can be easily see that $\mathbb{Z}_2$ is semiring

Now S, we mean semiring having both additive and multiplicative identities just like vector space over $\mathbb{F}$ First We will define the semi vector space over tropical linear algebra S

1.2.1 Semi Vector spaces

Definition 1.2.4. *Let $(V, \oplus)$ be a semi group and $(S, \oplus, \otimes)$ be a semi field and define a scalar multiplication $S \times V \to V$ as for all $s \in S$, $v \in V$, $sv \in V$. Then V is called a semi vector space if*

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

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

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

Example 1.2.5 *Let S be a semifield. Consider $S^n = \{(x_1, x_2, \ldots, x_n) : x_i \in S\}$. Let $u = (x_1, x_2, \ldots, x_n)$ and $v = (x'_1, x'_2, \ldots, x'_n)$ be two vectors. Addition and scalar multiplication are defined as*

$$u + v = (x_1, x_2, \ldots, x_n) + (x'_1, x'_2, \ldots, x'_n) = (x_1 \oplus x'_1, x_2 \oplus x'_2, \ldots, x_n \oplus x'_n)$$

$$tu = t(x_1, x_2, \ldots, x_n) = (t \otimes x_1, t \otimes x_2, \ldots, t \otimes x_n)$$

Now for semi vector spaces we have

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

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

$$=(\alpha_1 \oplus \alpha_2)(x_1, x_2, \ldots, x_n)$$

$$=[(\alpha_1 \oplus \alpha_2) \otimes x_1, (\alpha_1 \oplus \alpha_2) \otimes x_2, \ldots, (\alpha_1 \otimes \alpha_2) x_n)$$

$$=[(\alpha_1 \otimes x_1, \alpha_1 \otimes x_2, \ldots, \alpha_1 \otimes x_n) + (\alpha_2 \otimes x_1, \alpha_2 \otimes x_2, \ldots, \alpha_n \otimes x_n)]$$

$$=\alpha_1(x_1, x_2, \ldots, x_n) + \alpha_2(x_1, x_2, \ldots, x^n)$$

$$=\alpha_1 u + \alpha_2 u$$

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

$$=(\alpha_1 \otimes \alpha_2)(x_1, x_2, \ldots, x_n)$$

$$=[(\alpha_1 \otimes \alpha_2) \otimes x_1, (\alpha_1 \otimes \alpha_2) \otimes x_2, \ldots, (\alpha_1 \otimes \alpha_2) \otimes x_n]$$

$$=[\alpha_1 \otimes (\alpha_2 \otimes x_1), \alpha_1 \otimes (\alpha_2 \otimes x_2), \ldots, \alpha_1 \otimes (\alpha_2 \otimes x_n)]$$

$$=[\alpha_1(\alpha_2 \otimes x_1, \alpha_2 \otimes x_2, \ldots, \alpha_2 \otimes x_n)]$$

$$=\alpha_1[\alpha_2(x_1, x_2, \ldots, x_n)]$$

$$=\alpha_1(\alpha_2 u)$$

So, it is a ***semi-vector space***

1.2.2 Semisubspace

Definition 1.2.6. *Let V be a semi vector space. A subset U of V is called a* ***Semi subspace*** *of V if U is itself a semi vector space under the same operations as V*

Theorem 1.2.7 *Let V be a semi vector space and S be a semi field. A subset U of V is a semi subspace if*

1. *For any two vectors u, v ∈ U, u + v is also in U*

2. *For any $a \in S$, **u** $\in U$, **au** is not in U*

Definition 1.2.8. *A* ***monic polynomial*** *is a univariate polynomial in which the leading coefficient (the nonzero coefficient of highest degree) is equal to 1*

1.2.3 Ideals of a Max-Plus algebra

In this section we will discuss a special type of subsets of S called ideals of S.

Definition 1.2.9. *Let S be a Max-Plus algebra, that is, a semiring. A left ideal I of S is a non-empty subset of S such that*

1. *$(I, \oplus)$ is a subsemigroup $(S, \oplus)$, that is, $a \oplus b \in I$ for all $a, b \in I$,*

2. *$s \otimes a \in I$ for all $s \in S$ and $a \in I$.*

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

1. *$(I, \oplus)$ is a subsemigroup $(S, \oplus)$, that is, $a \oplus b \in I$ for all $a, b \in I$.*

2. *$a \otimes s \in I$ for all $s \in S$ and $a \in I$.*

If I is both left and right ideal of S, then I is called a two sided or simply an ideal of S. Here multiplication is commutative so every left ideal is also a right ideal.

Proposition 1.2.10 *Intersection of any collection of ideals of S is an ideal of S.*

Proof. Let $\{I_i : i \in \Lambda\}$ be collection of ideals in S. As $0_{\oplus} \in I_i$ for all $i \in \Lambda \Rightarrow 0_{\oplus} \in \cap_{i \in I} I_i$. Let $x, y \in \cap_{i \in \Lambda} I_i \Rightarrow x, y \in I_i$ for all $i \in \Lambda$, as each I_i is an ideal

$$\Rightarrow x \oplus y \in I_i \text{ for all } i \in \Lambda$$

$$\Rightarrow x \oplus y \in \cap_{i \in \Lambda} I_i$$

Similarly,

$$\Rightarrow s \otimes x \in I_i \text{ for all } s \in s \text{ and for all } i \in \Lambda$$

$$\Rightarrow s \otimes x \in \cap_{i \in \Lambda} I_i$$

Thus, we get that $\cap_{i \in \Lambda} I_i$ is an ideal. However, union of two ideals need not to be an ideal. □

Proposition 1.2.11 *If I_1 and I_2 be any two ideals of a semiring S. Then $I_1 + I_2 = \{i_1 \oplus i_2 : i_1 \in I_1, i_2 \in I_2\}$ is also an ideal of S.*

Proof. As $0_\oplus \in I_1, I_2$. So,

$$0_\oplus \oplus 0_\oplus = 0_\oplus \in I_1 + I_2$$

Let $a = i_1 \oplus i_2, b = i'_1 \oplus i'_2 \in I_1 + I_2$, then

$$a \oplus b = (i_1 \oplus i_2) \oplus (i'_1 \oplus i'_2)$$

since addition is commutative so we have

$$a \oplus b = (i_1 \oplus i'_1) \oplus (i_2 \oplus i'_2) \in I_1 + I_2$$

Let $s \in S$ and $a = i_1 \oplus i_2 \in I_1 + I_2$. Then

$$s \otimes a = s \otimes (i_1 \oplus i_2) = s \otimes i_1 \oplus s \otimes i_2 \in I_1 + I_2$$

□

Proposition 1.2.12 *If I and J are ideals of S, then*

$$IJ = \{\bigoplus_{finite} a_i \otimes b_i : a_i \in I \quad and \quad b_i \in J\}$$

is an ideal of S.

Proof. As $0_\oplus \in I, J$. So

$$0_\oplus \otimes 0_\oplus = 0_\oplus \in IJ$$

Let $a = \bigoplus_{finite} a_i \otimes b_i, b = \bigoplus_{finite} a'_i \otimes b'_i \in IJ$, then

$$a \oplus b = \bigoplus_{finite} a_i \otimes b_i \oplus \bigoplus_{finite} a'_i \otimes b'_i \in IJ$$

Let $s \in S$ and $a = \bigoplus_{finite} a_i \otimes b_i \in IJ$. Then

$$s \otimes a = s \otimes (\bigoplus_{finite} a_i \otimes b_i) = \bigoplus_{finite} (s \otimes a_i) \otimes b_i \in IJ$$

Clearly

$$IJ \subseteq I \bigcap J$$

□

Chapter 2

Algebraic Codes Over Finite Field

In this chapter, we will explain basic definition and results mostly taken from [1], [2] and [10]. In the first section of this chapter we will discuss linear code and generator matrix of linear codes. In the next section we will discuss dual codes and the parity check matrix of linear code. In later sections we will discuss Reed Muller codes and Tropical algebra.

2.1 Linear Code

In this section we will study linear codes and related results.

Definition 2.1.1 *A subset C of $\mathbb{F}^n$ is called a* ***linear code****, if C is the subspace of $\mathbb{F}^n$ (that is, C is closed under addition and scalar multiplication). A linear code of dimension k contains precisely 2^k codewords. Rather than writing a codeword in the form of n-tuple we will use the notation $a_1a_2\ldots a_n$ for a codeword. Thus a code C is linear if for all $a_1a_2\ldots a_n$, $b_1b_2\ldots b_n \in C$ and $\alpha, \beta \in \mathbb{F}$*

$$\alpha(a_1a_2\ldots a_n) + \beta(b_1b_2\ldots b_n) = (\alpha a_1 + \beta b_1)(\alpha a_2 + \beta b_2)\ldots(\alpha a_n + \beta b_n)$$

belongs to C.

Definition 2.1.2. *A* ***binary linear code*** *C of length n is a set of binary n-tuples such that the componentwise modulo 2 sum of any two codewords is contained in C.*

Example 2.1.3. *The set $C = \{000, 011\}$ is a binary linear code, since the sum of any two codewords lies in this set.*

$$000 + 000 = 000 \in C$$

$$000 + 011 = 011 \in C$$

$$011 + 011 = 000 \in C$$

Example 2.1.4. *Consider $\mathbb{Z}_3$, then the set*

$$C = \{0000, 0111, 1011, 1110, 0222, 2022, 2220\}$$

is not a linear code since ny two codewords lies in this set.

$$0111 + 2022 = 2100 \notin C$$

Definition 2.1.5. *The* ***Hamming distance*** *between two codewords $d(x, y)$ is the number of places in which the codewords x and y differ.*

Definition 2.1.6. *The* ***minimum Hamming distance*** *of a code C is the minimum distance between any two codewords in the code.*

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

A linear code can be represented by (n, k, d) where n is the *length of the code*, that is, the number of the bits in any codeword, k is the *dimension of the code C* and d is the *minimum distance* of the code C.

Example 2.1.7. *The set $\{000, 111\}$ is a binary linear code, since the sum of any two codewords lies in this set. Note that this is a $(3, 1, 3)$-code because the codewords have length 3, dimension of code is 1 and the minimum distance between codewords is 3.*

Example 2.1 8 *The set {000 111} is a binary linear code since the sum of any two codewords lies in this set Note that this is a (3 1 3)-code because the codewords have length 3, dimension of code is 1 and the minimum distance between codewords is 3*

Example 2 1 9 *The set $C = \{00\ 11\ 22\ 33\ 44\}$ is a linear code since the sum of any two codewords lies in this set Note that this is a (2 1 2)-code over $\mathbb{Z}_5$ because the codewords have length 2, dimension of code is 1 (as the codeword in C is a multiple of 11) and the minimum distance between codewords is 2*

Theorem 2.1.10 *Let C be a linear code Then the linear combination of any set of codewords in C is a codeword in C*

Proof Since C is a subspace of $\mathbb{F}^n$ so by definition of subspace we have $u + v \in C$ for all u v in C and $\alpha u \in C$ for all $u \in C$ and $\alpha \in \mathbb{F}^n$ □

2.1.1 Generator matrix

Linear codes are used in practice largely due to the simple encoding procedures facilitated by their linearity A $k \times n$ matrix G is a generator matrix for some linear code C A linear code is generated by a $k \times n$ generator matrix G is called a $(n\ k)$ code An $(n\ k)$ code with distance d is said to be an $(n\ k\ d)$ code The generator matrix $G_1 = [I_k \quad B]$ is said to be in *Standard form* Where I_k is the $k \times k$ identity matrix and B is a $k \times (n-k)$ matrix and the code C generated by G is called a *systematic code* Not all linear codes have a generator matrix in standard form For example the linear code $C = \{000\ 100\ 001\ 101\}$ has six generator matrices

$$G_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad G_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad G_3 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

$$G_4 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \quad G_5 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad G_6 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

None of these matrices are in standard form

Definition 2.1.11. *A **generating matrix** G for a linear code C of block length n is an m-by-n matrix G (for some m) whose row space is C*

Theorem 2.1.12. *Let C be an (n,k)-code over $\mathbb{F}$ Let G be a generator matrix of C Then*

$$C = \{uG \quad u \in \mathbb{F}^k\}$$

Proof Let G be the generator matrix of an (n k)-code over $\mathbb{F}$ then the rows of G forms basis for C so every $x \in C$ is a linear combination of the rows of G that is

$$x = u_1G_1 + u_2G_2 + \dots + u_kG_k$$

Where u_1 u_2 $\dots$ $u_k \in \mathbb{F}$ and $G_1, G_2, \dots G_k$ are the rows of G Consider the vector $u = [u_1, u_2 \dots u_k] \in \mathbb{F}^k$

$$\begin{aligned} x =& u_1G_1 + u_2G_2 + \dots + u_kG_k \\ =& [u_1 \ u_2, \dots u_k] \begin{bmatrix} G_1 \\ G_2 \\ \vdots \\ G_k \end{bmatrix} \\ =& uG \end{aligned}$$

Thus $C = \{uG \quad u \in F^k\}$ □

Example 2.1.13 *Let G be the generator matrix of code C Then it generates the codewords of a linear code C by encoding the message of length k As generator matrix is of* 2 × 3 *then we need to generate the* (3 2) *code Here* $k = 2$ *so the possible pairs of length 2 are [0 0], [1 0], [0 1] [1 1] Let us take*

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

at $u = [0\ 0]$

$$\begin{aligned} uG =& [0\ 0] \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \\ =& [0\ 0\ 0] \end{aligned}$$

at $u = [1\ 0]$

$$\begin{aligned} uG =& [1\ 0] \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \\ =& [1\ 1\ 0] \end{aligned}$$

at $u = [0\ 1]$

$$\begin{aligned} uG =& [0\ 1] \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \\ =& [1\ 0\ 1] \end{aligned}$$

at $u = [1\ 1]$

$$\begin{aligned} uG =& [1\ 1] \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \\ =& [0\ 1\ 1] \end{aligned}$$

Code generated from this generator matrix with four codewords is

$$C = \{000\ 110\ 101\ 011\}$$

Example 2 1 14. *Let G be the generator matrix of code C Then it generates the codewords of a linear code C by encoding the message of length k As the following generator matrix is of 2×3 then we need to generate the $(3\ 2)$ code Here $k = 2$ so the possible pairs of length 2 over Z_3 are [0 0], [1 0], [0 1] [1 1] [2 0], [0 2], [2 2] [1 2], [2 1] Let us take*

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

Then

$$[00]G = [000] \quad [10]G = [120] \quad [01]G = [001]$$

$$[11]G = [121] \quad [02]G = [002] \quad [20]G = [210]$$

$$[22]G = [212] \quad [12]G = [122] \quad [21]G = [211]$$

Thus, the corresponding code is

$$\{000, 001, 120, 121, 002, 210, 212, 122, 211\}$$

Remark 2.1.15 If C is an (n,k) linear code then generator matrix G is of order $k \times n$ and C the linear (n,k)-code is the row space of its generator matrix G.

2.2 Dual code

In this section we will deal with duality. The notion of dual codes is one of the most interesting topics in coding theory. However, it is also often confusing at first read. The concept of dual codes has been widely studied and the best codes are, indeed, self dual codes.

Definition 2.2.1 *The dual code $C^\perp$ of an (n,k) C is the $(n,n-k)$ code being the orthogonal space of C with respect to a specified inner product*

$$C^\perp = \{x \in \mathbb{F}^n \mid x \cdot y = 0 \text{ for all } y \in C\}$$

Example 2.2.2. *Let $C = \{000, 011\}$ is $(3,1)$-code and*

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

As $C^\perp = \{x \in F^n \mid x \cdot y = 0 \ \forall \ y \in C\}$

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

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

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

$$[011]\quad[100] = [0\quad 1+1\quad 0+1\quad 0] = 0$$

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

$$[011]\quad[010] = [0\quad 0+1\quad 1+1\quad 0] = 1$$

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

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

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

$$[011]\quad[110] = [0\quad 1+1\quad 1+1\quad 0] = 1$$

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

$$[011]\quad[101] = [0\quad 1+1\quad 0+1\quad 1] = 1$$

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

$$[011]\quad[011] = [0\quad 0+1\quad 1+1\quad 1] = 0$$

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

$$[011]\quad[111] = [0\quad 1+1\quad 1+1\quad 1] = 0$$

Hence

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

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

Proposition 2.2 3. *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 2.2.4 *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 $u = (u_1, u_2, \dots, u_n) \in C\bigcap C^{\perp}$ then $u\cdot u = u_1u_1 + u_2u_2 + \dots + u_nu_n = 0$ imply that each $u_i = 0$. Thus, we have $C\bigcap C^{\perp} = \{0\}$
Since C and $C^{\perp}$ are linear so we have

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

$$\Rightarrow \dim C^{\perp} = n - k$$

□

Remark 2.2.5. If G is a generator matrix of C then the null space of G is $C^{\perp}$ that is, $\forall\ x \in C^{\perp}$, $Gx^{\top} = 0$ or equivalently $xG^{\top} = 0$.

Example 2.2.6. *let $C = \{000, 011\}$ be $(3,1)$-code. Then $C^{\perp} = \{000, 100, 011, 111\}$ be dual $(3,2)$-code and G is the generator matrix of the code C that is*

$$G = [011]$$

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

$$\begin{aligned}Gx^{\top} =&[011]\begin{bmatrix}0\\0\\0\end{bmatrix}\\ =&0\end{aligned}$$

at $x = [100]$

$$
\begin{aligned}
Gx^{\top} =& [011]\begin{bmatrix}1\\0\\0\end{bmatrix}\\
=& 0
\end{aligned}
$$

at $x = [011]$

$$
\begin{aligned}
Gx^{\top} =& [011]\begin{bmatrix}0\\1\\1\end{bmatrix}\\
=& 0
\end{aligned}
$$

at $x = [111]$

$$
\begin{aligned}
Gx^{\top} =& [011]\begin{bmatrix}1\\1\\1\end{bmatrix}\\
=& 0
\end{aligned}
$$

This example proves the above remark

Corollary 2.2 7. *Let C be a linear code Then $(C^{\perp})^{\perp} = C$*

Proof The relation between C and $C^{\perp}$ is symmetric that is the dual code of $C^{\perp}$ is C Let $x \in C$ thus $x\ y = 0\ \forall\ y \in C^{\perp}$ that is, if

$$x = [x_1\, x_2 \qquad x_n]\ \textit{and}\ \ y = [y_1\, y_2 \qquad y_n]$$

Then

$$
\begin{aligned}
x\ y =& x_1\, y_1 + x_2\, y_2 + \qquad + x_n\, y_n\\
=& y_1\, x_1 + y_2\, x_2 \quad y_n\, x_n\ (\quad \text{multiplicative}\ \ \text{is}\ \ \text{commutative}\ )\\
=& y\ x
\end{aligned}
$$

if $x\ y = 0$ then $y\ x = 0\ \forall\ x \in C$ and $y \in C^{\perp}$ that is, if $y \in C^{\perp}$ then $x \in C$ so $C \subseteq (C^{\perp})^{\perp}$ As $C^{\perp}$ is a subspace of $\mathbb{F}^n$ with dimension $n-k$ if dim C is k Hence $(C^{\perp})^{\perp}$ has dimension $n-(n-k)=k$ Thus $dim\,(C) = k = dim(C^{\perp})^{\perp}$ Thus $C = (C^{\perp})^{\perp}$ □

Remark 2 2 8

- A linear code C is self orthogonal if every vector in C is orthogonal to itself and to every other vector in C that is $C \subset C^{\perp}$
- A linear code C is self dual if $C = C^{\perp}$

2.2.1 Parity check matrix

In this section we will discuss parity check matrix, a code can not only be defined by the generator matrix G but also by the parity check matrix H However, the two matrices can be derived from each other A generator matrix for $C^{\perp}$ is called a parity check matrix for C If C is an (n k)-code then a parity check matrix for C will be an $n-k \times n$ matrix If H is a parity check matrix for C we can recover the vectors of C from H because they must be orthogonal to every row of H (basis vectors of $C^{\perp}$) The parity check matrix in *Standard form* is $H = [P \quad I_{n-k}]$

Definition 2 2 9. *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*

Example 2.2 10. *Let $C = \{000\ 011\}$ is (3,2)-code and*

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

then its dual code becomes

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

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

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

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

Note that the parity check matrix of a code C is not unique

Remark 2 2 11

- If G is the generator matrix of the code C then G is the parity check matrix of the dual code $C^{\perp}$ because $(C^{\perp})^{\perp} = C$
- The dual of an $(n\ k)$ code is an $(n\ n-k)$ code so the parity check matrix of an $(n\ k)$ code is an $(n-k) \times n$ Matrix H whose rows form a basis for $C^{\perp}$
- A parity check matrix completely determines the code

Theorem 2.2.12. *Let C be an (n k) code over F and let H be a parity check matrix of C Then*

$$C = \{x \in C \qquad xH^{\top} = 0 = Hx^{\top}\}$$

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 $x \in C$ iff $Hx^{\top} = 0$ or equivalently $xH^{\top} = 0$ □

Example 2.2 13. *Let* $C = \{000\ 011\}$ *be a linear code and*

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

Then its dual code is $C^{\perp} = \{000, 100\ 011\ 111\}$

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

at $x = [000]$

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

at = [011]

$$xH^T = [011]\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 1\end{bmatrix}^T$$
$$= [0\ 0]$$

Theorem 2.2.14 *Let C be an (n,k) code. Let G and H be generator matrix and parity check matrix of C respectively. Then*

$$GH^T = 0 = HG^T$$

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 $GH^T = 0$. Then H is a parity check matrix of the code C if and only if G is the generator matrix of C.

Proof. As by previous theorem $\forall\ x \in C$

$$xH^T = 0$$

Here in particular, $G_iH^T = 0\ \forall\ i = 1, 2, \ldots, k$. Where each G_i is a row of generator matrix and hence $GH^T = 0$. Taking transpose, we get $HG^T = 0$.
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 $GH^T = 0$. Suppose H is a parity check matrix of C. Then $G_iH^T = 0\ \forall\ i = 1, 2, \ldots, k$. 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 preceding theorem $\forall\ y \in C^\perp$ $yG^T = Gy^T = 0$. Suppose $GH^T = 0$ then by taking transpose $HG^T = 0, H_iG^T = 0\ \forall\ i = 1, 2, \ldots, n-k$. Hence $H_1, H_2, \ldots, H_k \in C^\perp$. 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 2.2.15 *In previous example $C = \{000, 011\}$ is $(3, 1)$-code then the dual of C is*

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

let $G = [011]$ is the generator matrix of the code C

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

is the parity check matrix of code C. Then

$$\begin{aligned} GH^{\top} =& [011] \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}^{\top} \\ =& [0\ 0] \end{aligned}$$

Definition 2.2.16. *Let C be an (n, k)-code, if C has a* ***canonical generator matrix*** *$G = [I_k \quad A]$, then $H = [-A^{\top} \quad I_{n-k}]$ is the canonical parity check matrix of C. Conversely, if $H = [B \quad I_{n-k}]$ is a parity check matrix of C, then $G = [I_k \quad -B^{\top}]$ is a generator matrix of C.*

Example 2.2.17. *Let*

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

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

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

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

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

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

$$\begin{aligned} H^* &= [B \quad I_3] \\ G^* &= [I_1 \quad -B^T] \\ &= [1 \quad 0\,0\,0] \end{aligned}$$

Where G^* is the generator matrix of code C

2.2.2 Cyclic and Constacyclic codes

Let $\mathbb{F}$ be a finite filed. A code C of length n over $\mathbb{F}$ is called Constacyclic if for each $\alpha \in \mathbb{F}$ and codeword $(c_0, c_1, \ldots, c_{n-1}) \in C$, the vector $(\alpha c_{n-1}, c_0, \ldots, c_{n-2})$ is again a codeword in C. A constacyclic code is called cyclic if $\alpha = 1$.

Example 2.2.18. *Consider the code* $C = \{00, 11, 22, 33, 44\}$ *over* $\mathbb{Z}_5$. *Then* C *is cyclic but not constacyclic as for* $\alpha = 2$, $(21) \notin C$

2.3 Reed-Muller Codes

Reed-Muller codes are among the oldest known codes and have found widespread applications. Reed-Muller codes were formulated by I. S. Reed and D. E. Muller in 1954. These codes were initially given as binary codes, but modern generalizations to q-ary codes exist. We will restrict our investigation to the binary case. One of the interesting things about these codes is that there are several ways to describe them and we shall look at one of these.
For each positive integer m and each integer r with $0 \leq r \leq m$, there is an r^{th} order Reed-Muller Code $R(r,m)$. We start our definition by considering the 1^{st} order case $(r = 1)$.

Definition 2.3.1. *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 2.3.2. *To find $R(1,2)$ code we have by definition*

$$R(1,2) = \{(u,u), (u,u+1)\} \quad \textit{where } u \in R(1,1) \textit{ here } r = 1, m = 2$$

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

$$\textit{then} \quad R(1,2) = \{0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100\}$$

Example 2.3.3. *To find $R(1,3)$ code, we have by definition*

$$R(1,3) = \{(u,u), (u,u+1)\} \quad \textit{where } u \in R(1,2) \textit{ here } r = 1, m = 3$$

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

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

$$\textit{then} \quad R(1,3) = \{00000000, 01010101, 10101010, 11111111, 00110011, 10011001, 11001100, 00001111, 01011010, 10100101, 11110000, 00111100, 01101001, 10010110, 11000011\}$$

2.3.1 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

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

2.3.2 Example

To find R(2,3) code we need R(2,2) and R(1,2)

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

v=0000	**v=0101**	**v=1010**	**v=1111**
00000000	00000101	00001010	00001111
00010001	00010100	00011011	00011110
00100010	00100111	00101000	00101101
00110011	00110110	00111001	00111100
01000100	01000001	01001110	01001011
01010101	01010000	01011111	01011010
01100110	01100011	01101100	01101001
01110111	01110010	01111101	01111000
10001000	10001101	10000010	10000111
10011001	10011100	10010011	10010110
10101010	10101111	10100000	10100101
10111011	10111110	10110001	10110100
11001100	11001001	11000110	11000011
11011101	11011000	11010111	11010010
11101110	11101011	11100100	11100001
11111111	11111010	11110101	11110000

v=0011	**v=0110**	**v=1001**	**v=1100**
00000011	00000110	00001001	00001100
00010010	00010111	00011000	00011101
00100001	00100100	00101011	00101111
00110000	00110101	00111010	00110011
01000111	01000010	01001101	01000111
01010110	01010011	01011100	01010111
01100101	01100000	01101111	01100111
01110100	01110001	01111110	01110111
10001011	10001110	10000001	10001011
10011010	10011111	10010000	10011011
10011010	10011111	10010000	10011011
10111000	10111101	10110001	10111011
11001111	11001010	11000101	11001111
11011110	11011011	11010100	11011111
11101101	11101000	11100111	11101111
11111100	11111001	11110110	11111111

Chapter 3

Algebraic Codes Over Max Plus Algebra

In this chapter we will discuss some algebraic codes over Max-Plus algebra. In the first section we will deal with linear codes and generator matrix. In next section we will check dual codes and parity check matrix. Further more we will discuss Reed Muller codes over Max-Plus. In the last section, we will related ideals and polynomials over Max-Plus algebra with algebraic codes.

Recall that a Max-Plus algebra is a semi ring equipped with maximum and plus as the two binary operations. Let a and b be any two elements operation maximum(implied by the max operator $\oplus$)and plus (implied by the plus operator $\otimes$) for these scalers are defined as

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

$$a \otimes b = a + b$$

Now we will define algebraic codes for these two Max-Plus algebras

3.1 Linear Code

In this section we will define some basic definitions and examples of linear codes over Max-Plus algebra

Definition 3.1.1. *A code $\mathbb{C}$ of length n is **linear** if for each $u, v \in \mathbb{C}$ and $\alpha, \beta \in S$*

$$\alpha u + \beta v \in \mathbb{C}$$

That is, $\mathbb{C}$ is a linear semi subspace of S. If code $\mathbb{C}$ is a subspace of dimension k, then $\mathbb{C}$ is called an (n, k)-code

Example 3.1.2. *Consider $\mathbb{Z}_2$ with $a \otimes b = a\, b$. Then the set $\mathbb{C} = \{000, 100, 110\}$ is a linear code. As the tropical sum of any two codeword in*

$$100 + 100 = 1 \oplus 1, \quad 0 \oplus 0, \quad 0 \oplus 0 = max\{1, 1\}, \quad max\{0, 0\}, \quad max\{0, 0\} = 100$$

$$100 + 110 = 1 \oplus 1, \quad 0 \oplus 1, \quad 0 \oplus 0 = max\{1, 1\}, \quad max\{0, 1\}, \quad max\{0, 0\} = 110$$

$$110 + 110 = 1 \oplus 1, \quad 1 \oplus 1, \quad 0 \oplus 0 = max\{1, 1\}, \quad max\{1, 1\}, \quad max\{0, 0\} = 110$$

Example 3.1.3. *Consider $\mathbb{R}^* = \mathbb{R} \bigcup \{-\infty\}$ and the set $\mathbb{C} = \{(\chi, 2 + \chi, 3 + \chi) \mid \chi \in \mathbb{R}^*\}$. Then for any $(\chi, 2 + \chi, 3 + \chi), (\omega, 2 + \omega, 3 + \omega) \in \mathbb{C}$ and $\alpha, \beta \in \mathbb{R}^*$*

$$\alpha(\chi, 2 + \chi, 3 + \chi) + \beta(\omega, 2 + \omega, 3 + \omega)$$
$$= (\alpha \otimes \chi \oplus \beta \otimes \omega, \quad \alpha \otimes (2 + \chi) \oplus \beta \otimes (2 + \omega), \quad \alpha \otimes (3 + \chi) \oplus \beta \otimes (3 + \omega))$$
$$= (max\{\alpha + \chi, \beta + \omega\}, max\{\alpha + 2 + \chi, \beta + 2 + \omega\}, max\{\alpha + 3 + \chi, \beta + 3 + \omega\})$$

Now if

$$max\{\alpha + \chi, \beta + \omega\} = \alpha + \chi$$

then

$$max\{\alpha + 2 + \chi, \beta + 2 + \omega\} = \alpha + 2 + \chi$$

and

$$max\{\alpha + 3 + \chi, \beta + 3 + \omega\} = \alpha + 3 + \chi$$

Thus, we get that $\alpha(\chi\ 2 + \chi\ 3 + \chi) + \beta(\omega\ 2 + \omega, 3 + \omega) \in \mathsf{C}$ *Hence* C *is a linear code over* $\mathbb{R}^*$

3.1.1 Generator Matrix

In this section we will discuss generator matrix of a binary linear code C over Max-Plus algebra

Definition 3.1 4. *A* ***generating matrix*** $\mathcal{G}$ *for a linear code* C *of block length* n *is an* m*-by-*n *matrix* $\mathcal{G}$ *(for some* m*) whose row space is* C

Theorem 3 1 5. *Let* C *be an* $(r\ k)$*-code over* $\boldsymbol{S}$ *Let* $\mathcal{G}$ *be a generator matrix of* C *Then*

$$\mathsf{C} = \{u\mathcal{G} \mid u \in S^k\}$$

Proof Let $\mathcal{G}$ be the generator matrix of an (r, k)-code over $\mathbf{S}$, whose rows of $\mathcal{G}$ form basis for C So every $x \in \mathsf{C}$ is a linear combination of the rows of $\mathcal{G}$ that is

$$x = u_1G_1 + u_2G_2 + \quad + u_kG_k$$

where $u_1\ u_2 \quad u_k \in \mathbf{S}$ and $G_1\ G_2 \quad G_k$ are the rows of $\mathcal{G}$

Consider the vector $u = [u_1\ u_2 \quad , u_k] \in S^k$

$$\begin{aligned} x &= u_1G_1 + u_2G_2 + \quad + u_kG_k \\ &= [u_1, u_2, \quad u_k]\begin{bmatrix} G_1 \\ G_2 \\ \\ G_k \end{bmatrix} \\ &= u\mathcal{G} \end{aligned}$$

Thus

$$\mathsf{C} = \{u\mathcal{G} \mid u \in S^k\}$$

□

Example 3.1.6 *Consider $\mathbb{Z}_2$ with $a \otimes b = a \cdot b$. Let $\mathcal{G}$ be the matrix that generate code $\mathbb{C}$. Then, it generates the codewords of a linear code $\mathbb{C}$ by encoding the message of length k. As generator matrix is of 1×3 then we need to generate the $(3,1)$ code. Here $k = 1$ so the possible pairs of length 2 are [0], [1]. Let*

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

At $u = [0]$

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

At $u = [1]$

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

The code generated from this generator matrix is $\mathbb{C} = \{000, 101\}$

Example 3.1.7. *The linear code $\mathbb{C} = \{(g, 2+g, 3+g) : g \in \mathbb{R}^*\}$ is generated by $(0,2,3)$ as for any $g \in \mathbb{R}^*$*

$$g(0,2,3) = (g \otimes 0, g \otimes 2, g \otimes 3) = (g, g+2, g+3)$$

Thus, the matrix for this code is

$$\begin{bmatrix} 0 & 2 & 3 \end{bmatrix}$$

Example 3.1.8. *If we consider a matrix*

$$\begin{bmatrix} 0 & -\infty & -\infty & 2 \\ -\infty & 0 & -\infty & -\infty \\ -\infty & -\infty & 0 & -\infty \end{bmatrix}$$

For the code generated by this matrix consider

$$
\begin{aligned}
&[\mu\, \upsilon\, \omega] \begin{bmatrix} 0 & -\infty & -\infty & 2 \\ -\infty & 0 & -\infty & -\infty \\ -\infty & -\infty & 0 & -\infty \end{bmatrix} \\
&= [\mu \otimes 0 \oplus \upsilon \otimes -\infty \oplus \omega \otimes -\infty \quad \mu \otimes -\infty \oplus \upsilon \otimes 0 \oplus \omega \otimes -\infty \\
&\mu \otimes -\infty \oplus \upsilon \otimes -\infty \oplus \omega \otimes 0 \quad \mu \otimes 2 \oplus \upsilon \otimes -\infty \oplus \omega \otimes -\infty] \\
&= [\mu \quad \upsilon \quad \omega \quad \mu + 2]
\end{aligned}
$$

Thus,

$$\{(\mu \quad \upsilon \quad \omega \quad \mu + 2) \qquad \mu, \upsilon, \omega \in \mathbb{R}^{-}\}$$

is (4, 3) linear code generated by the given matrix

Remark 3 1 9 As basis for a subspace is not unique so we have more than one matrices for a code

3.2 Dual Code

In this section, we will define dual code of $\mathtt{C}$ over max plus and gives some examples of dual codes over Max-Plus algebra

Definition 3.2 1. *Let $\mathtt{C}$ be an (r,k)-code over $\boldsymbol{S}$ Then the* ***dual code*** *of $\mathtt{C}$ is defined to be*

$$\mathtt{C}^{\perp} = \{\, y \in \boldsymbol{S}^{r} \text{ such that } x \odot y = 0_{\oplus} \text{ for all } x \in \mathtt{C}\}$$

Remark 3 2 2

- A linear code $\mathtt{C}$ is self orthogonal over Max-Plus that is $\mathtt{C} \subset \mathtt{C}^{\perp}$
- A linear code $\mathtt{C}$ is self dual over Max-Plus if $\mathtt{C} = \mathtt{C}^{\perp}$

Example 3.2.3 *Let* $\mathbb{C} = \{100, 110\}$ *be a code over* $\mathbb{Z}_2$. *By checking the tropical product in*

$\mathbb{Z}_2^3 = \{000, 100, 010, 001, 110, 101, 011, 111\}$. *As,*

$$\mathbb{C}^{\perp} = \{y \in \mathbb{Z}_2^3 \text{ such that } x \odot y = 0 \text{ for all } x \in \mathbb{C}\}$$

Now,

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

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

$$[100] \odot [100] = [1 \otimes 1 \oplus 0 \otimes 0 \oplus 0 \otimes 0] = 1$$

$$[110] \odot [100] = [1 \otimes 1 \oplus 1 \otimes 0 \oplus 0 \otimes 0] = 1$$

$$[100] \odot [010] = [1 \otimes 0 \oplus 0 \otimes 1 \oplus 0 \otimes 0] = 0$$

$$[110] \odot [010] = [1 \otimes 0 \oplus 1 \otimes 1 \oplus 0 \otimes 0] = 1$$

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

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

$$[100] \odot [110] = [1 \otimes 1 \oplus 0 \otimes 1 \oplus 0 \otimes 0] = 1$$

$$[110] \odot [110] = [1 \otimes 1 \oplus 1 \otimes 1 \oplus 0 \otimes 0] = 1$$

$$[100] \odot [101] = [1 \otimes 1 \oplus 0 \otimes 0 \oplus 0 \otimes 1] = 1$$

$$[110] \odot [101] = [1 \otimes 1 \oplus 1 \otimes 0 \oplus 0 \otimes 1] = 1$$

$$[100] \odot [011] = [1 \otimes 0 \oplus 0 \otimes 1 \oplus 0 \otimes 1] = 0$$

$$[110] \odot [011] = [1 \otimes 0 \oplus 1 \otimes 1 \oplus 0 \otimes 1] = 1$$

$$[100] \odot [111] = [1 \otimes 1 \oplus 0 \otimes 1 \oplus 1 \otimes 1] = 1$$

$$[110] \odot [111] = [1 \otimes 1 \oplus 1 \otimes 1 \oplus 0 \otimes 1] = 1$$

Then $\mathbb{C}^{\perp} = \{000, 001\}$

Example 3.2.4. *Let* $\mathbb{C} = \{000, 110, 101, 011, 111\}$ *is a* $(3, 2)$*-code over* $\mathbb{Z}_2$. *By Checking the tropical product in*

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

$$\mathbb{C}^{\perp} = \{y \in (\boldsymbol{Z}_2)^3 \text{ such that } x \odot y = 0 \text{ for all } x \in \mathbb{C}\}$$

Now,

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

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

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

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

$$[110] \odot [100] = [1 \otimes 1 \oplus 1 \otimes 0 \oplus 0 \otimes 0] = 1$$

$$[011] \odot [100] = [0 \otimes 1 \oplus 1 \otimes 0 \oplus 0 \otimes 1] = 0$$

$$[101] \odot [100] = [1 \otimes 1 \oplus 0 \otimes 0 \oplus 1 \otimes 0] = 1$$

$$[111] \odot [100] = [1 \otimes 1 \oplus 1 \otimes 0 \oplus 1 \otimes 0] = 1$$

$$[110] \odot [010] = [1 \otimes 0 \oplus 1 \otimes 1 \oplus 0 \otimes 0] = 1$$

$$[011] \odot [010] = [0 \otimes 0 \oplus 1 \otimes 1 \oplus 1 \otimes 0] = 1$$

$$[101] \odot [010] = [1 \otimes 0 \oplus 0 \otimes 1 \oplus 1 \otimes 0] = 0$$

$$[111] \odot [010] = [1 \otimes 0 \oplus 1 \otimes 1 \oplus 1 \otimes 0] = 1$$

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

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

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

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

$$[110] \odot [110] = [1 \otimes 0 \oplus 1 \otimes 0 \oplus 0 \otimes 0] = 0$$

$$[011] \odot [110] = [0 \otimes 1 \oplus 1 \otimes 1 \oplus 1 \otimes 0] = 1$$

$$[101] \odot [110] = [1 \otimes 1 \oplus 0 \otimes 1 \oplus 1 \otimes 0] = 1$$

$$[111] \odot [110] = [1 \otimes 1 \oplus 1 \otimes 1 \oplus 1 \otimes 0] = 1$$

$$[110] \odot [101] = [1 \otimes 1 \oplus 1 \otimes 0 \oplus 0 \otimes 1] = 1$$

$$[011] \odot [101] = [0 \otimes 1 \oplus 1 \otimes 0 \oplus 1 \otimes 0] = 0$$

$$[101] \odot [101] = [1 \otimes 1 \oplus 0 \otimes 0 \oplus 1 \otimes 1] = 1$$

$$[111] \odot [101] = [1 \otimes 1 \oplus 1 \otimes 0 \oplus 1 \otimes 1] = 1$$

$$[110] \odot [011] = [1 \otimes 0 \oplus 1 \otimes 1 \oplus 0 \otimes 1] = 1$$

$$[011] \odot [011] = [0 \otimes 0 \oplus 1 \otimes 1 \oplus 1 \otimes 1] = 1$$

$$[101] \odot [011] = [1 \otimes 0 \oplus 0 \otimes 1 \oplus 1 \otimes 1] = 1$$

$$[111] \odot [011] = [1 \otimes 0 \oplus 1 \otimes 1 \oplus 1 \otimes 1] = 1$$

$$[110] \odot [111] = [1 \otimes 1 \oplus 1 \otimes 1 \oplus 0 \otimes 1] = 1$$

$$[011] \odot [111] = [0 \otimes 1 \oplus 1 \otimes 1 \oplus 1 \otimes 1] = 1$$

$$[101] \odot [111] = [1 \otimes 1 \oplus 0 \otimes 1 \oplus 1 \otimes 1] = 1$$

$$[111] \odot [111] = [1 \otimes 1 \oplus 1 \otimes 1 \oplus 1 \otimes 1] = 1$$

Then $\mathbb{C}^{\perp} = \{000\}$ *is a (3, 0)-code*

Example 3.2.5. *Consider the (4, 2) code*

$$\{(w, z, w+2, -\infty) \quad w, z \in \mathbb{R}^{*}\}$$

If $(a, b, c, d) \in \mathbb{C}^{\perp}$, *then*

$$(a, b, c, d) \odot (w, w, z+2, -\infty) = -\infty$$

$$\Rightarrow a \otimes w \oplus b \otimes z \oplus c \otimes (w+2) \oplus d \otimes -\infty = -\infty$$

That is

$$max\{a \otimes w, b \otimes z, c \otimes (w+2), -\infty\} = -\infty$$

Thus,

$$a \otimes w = b \otimes z = c \otimes (w + 2) = -\infty$$

We get that

$$a = b = c = -\infty$$

Hence $\mathbb{C}^{\perp} = \{(-\infty, -\infty, -\infty, d) \qquad d \in \mathbb{R}^{*}\}$ *which is a (4, 1) linear code*

Proposition 3.2.6. *For a code* $\mathbb{C}$ *the dual code* $\mathbb{C}^{\perp}$ *is linear*

Proof As $0_{\oplus} \odot c = 0_{\oplus}$ we get that $\mathbb{C}^{\perp}$ is non-empty If $w, z \in \mathbb{C}^{\perp}$, then $w \odot c = 0_{\oplus}$ and $z \odot c = 0_{\oplus}$ for every $c \in \mathbb{C}$ Thus

$$\begin{aligned}
&(\alpha w + \beta z) \odot c \\
&= \alpha w \odot c + \beta z \odot c \\
&= \alpha 0_{\oplus} + \beta 0_{\oplus} = 0_{\oplus}
\end{aligned}$$

□

Remark 3 2 7 If $w \in \mathbb{C} \bigcap \mathbb{C}^{\perp}$, then

$$w \odot w = 0_{\oplus} \Rightarrow w = 0_{\oplus}$$

that is

$$\mathbb{C} \bigcap \mathbb{C}^{\perp} = \{0_{\oplus}\}$$

However, from pervious examples it is clear that

$$\mathbb{C} + \mathbb{C}^{\perp} \neq S^{n}$$

Lemma 3.2 8. *Let* $\mathbb{C}$ *be an (n,k)-code with generator matrix and* $\mathcal{G}$ *be the matrix which is generator of* $\mathbb{C}$ *Then for every* $x \in S^{n}$ *it holds that* $x \in \mathbb{C}^{\perp}$ *if and only if* $x\mathcal{G}^{T} = 0 = \mathcal{G}x^{T}$

Proof Let $\mathcal{G}$ be any generator matrix Then here in particular $x\mathcal{G}^{T} = 0$ where $\mathcal{G}$ is row of generator matrix and hence $x\mathcal{G}^{T} = 0$ By taking transpose $\mathcal{G}x^{T} = 0$ □

Example 3.2.9. *Let* $\mathbb{C} = \{000, 001\}$ *be an* $(3,1)$*-code and* $\mathbb{C}^{\perp} = \{000, 100, 010, 110\}$ *be a dual code. Let* $\mathcal{G} = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}$ *be a generator matrix of* $(3,1)$*-code* $\mathbb{C}$.
At $x = [100]$

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

$$= [0 \otimes 1 \oplus 0 \otimes 0 \oplus 1 \otimes 0]$$

$$= max\{0, 0, 0\} = 0$$

At $x = [010]$

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

$$= [0 \otimes 0 \oplus 0 \otimes 1 \oplus 1 \otimes 0]$$

$$= max\{0, 0, 0\} = 0$$

At $x = [110]$

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

$$= [0 \otimes 1 \oplus 0 \otimes 1 \oplus 1 \otimes 0]$$

$$= max\{0, 0, 0\} = 0$$

Example 3.2.10. *For the code generated by matrix*

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

The dual code is $\{0000, 0010\}$

3.2.1 The Parity-Check Matrix

In this section we will define parity check matrix over Max-Plus Further we will give some examples of parity check matrix over Max-Plus

Definition 3 2.11. *A parity check matrix for* C *is an* $k \times n$ *matrix* $\mathcal{H}$ *such that* $c \in \mathcal{C}^{\perp}$ *if and only if* $c\mathcal{H}^T = 0$

Example 3.2.12. *Let* $\mathsf{C} = \{000, 001\}$ *is* $(3,1)$*-code Then the dual of* C *is* $\mathcal{C}^{\perp} = \{000, 100, 010, 110\}$

Parity check matrix is of an $k \times n$ *matrix that is* 2×3 *Hence we can take*

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

Example 3 2 13. *Consider the (4, 2) code*

$$\{(x\ y, x+2\ -\infty) \qquad x, y \in \mathbb{R}^*\}$$

The dual code is $\mathsf{C}^{\perp} = \{(-\infty\ -\infty, -\infty\ d) \qquad d \in \mathbb{R}^*\}$ *Thus the parity check matrices are of the form*

$$\mathcal{H} = \begin{bmatrix} -\infty & -\infty & -\infty & d \end{bmatrix}$$

Theorem 3 2.14 *Let* C *be a linear* (r, k)*-code over* $\boldsymbol{S}$ *and let* $\mathcal{H}$ *be a parity check matrix of* C *Then*

$$\mathsf{C} = \{x \in \boldsymbol{S}^n \qquad x\mathcal{H}^T = 0 = \mathcal{H}x^T\}$$

Proof We have seen that if $\mathcal{G}$ is matrix that generate C then the null space of $\mathcal{G}$ is C^T Now $\mathcal{H}$ is a generator matrix of C^T and hence the null space of $\mathcal{H}$ Hence $x \in \mathsf{C}$ if and only if $\mathcal{H} \otimes x^T = 0$ or equivalently $x \otimes \mathcal{H}^T = 0$ □

Example 3.2 15 *Let* $\mathsf{C} = \{000\ 001\}$ *be a linear* $(3\ 1)$*-code whose dual code is*

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

Let

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

be the generator matrix of dual code and is parity check matrix of linear code C

At $x = [001]$

$$x\mathcal{H}^{T} = [001]\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$$

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

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

Theorem 3.2.16. *Let* C *be an* (r,k)*-code. Let* $\mathcal{G}$ *be the matrix that generate code* C *and* $\mathcal{H}$ *is the parity check matrix of* C. *Then*

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

Proof. Let

$$\mathcal{G} = \begin{bmatrix} G_1 \\ G_2 \\ \\ G_k \end{bmatrix}$$

be the $k \times r$ matrix for C and

$$\mathcal{H} = \begin{bmatrix} H_1 \\ H_2 \\ \\ H_l \end{bmatrix}$$

be the $l \times r$ parity check matrix for C. Then the terms in $\mathcal{G}\mathcal{H}^{T}$ are of the form $G_i \odot H_j$. As $G_i \in \mathsf{C}$ and $H_j \in \mathsf{C}^{\perp}$, we get that

$$G_i \odot H_j = 0_{\oplus}$$

for all i and j Thus $\mathcal{G}\mathcal{H}^T$ is a zero matrix Hence $\mathcal{H}\mathcal{G}^T = (\mathcal{G}\mathcal{H}^T)^T = 0$ □

Example 3 2 17. *Let* $\mathbb{C} = \{0000, 0010\ 0001, 0011\}$ *be an* $(4, 2)$*-code whose generator matrix*

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

and dual code of $\mathbb{C}$ *is* $\mathbb{C}^{\perp} = \{000, 1000\ 0100, 1100\}$ *whose generator matrix is*

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

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

Remark 3 2 18

- If $\mathcal{G}$ is a $k \times r$ matrix of the code $\mathbb{C}$ then $\mathcal{H}$ is a generator matrix of $\mathbb{C}^{\perp}$ whose rows form a basis of $\mathbb{C}^{\perp}$
- Let $\mathbb{C}$ be an (r, k)-code, if $\mathbb{C}$ has a canonical generator matrix $\mathcal{G} = [I_k\ \ \mathcal{A}]$ then $\mathcal{H} = [\mathcal{A}^T\ \ I_{n-k}]$ is the canonical parity check matrix of $\mathbb{C}$ Conversely if $\mathcal{H} = [\mathcal{B}\ \ I_{n-k}]$ is a parity check matrix of $\mathbb{C}$ then $\mathcal{G} = [I_k\ \ \mathcal{B}^T]$ is a matrix which is generator of $\mathbb{C}$

Example 3.2.19 *Let* $\mathbb{C} = \{0000\ 0010\ 0001\ 0011\}$ *be a* $(4, 2)$ *linear code and* $\mathbb{C}^{\perp} = \{000, 1000, 0100, 1100\}$ *be its dual code Then*

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

is the parity check matrix, that is precisely a canonical generator matrix

$$
\begin{aligned}
\mathcal{H}^* &= [I_2 \quad B] \\
\mathcal{G}^* &= [B^\top \quad I_2] \\
&= \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}
\end{aligned}
$$

Where $\mathcal{G}^*$ is the generator matrix of code C

3.2.2 lth Order Reed Muller Code

The zeroth order Reed Muller code $\mathcal{R}(0,t)$ is defined to be the repetition code $\{0,1\}$ of length 2^t For any $l \geq 2$, the lth order Reed Muller code $\mathcal{R}(l\ t)$ is defined recursively by

1 $\mathcal{R}(l\ t) = \{Z_2^2 r$ if $t = l$

2 and $\mathcal{R}(l,t) = \{(x, x \oplus y)\ \ x \in \mathcal{R}(l\ t-1)\ y \in \mathcal{R}(l-1\ t-1)$ if $t > l$

Example 3.2 20 *To find $\mathcal{R}(2,3)$ code we need $\mathcal{R}(2,2)$and $\mathcal{R}(1,2)$*

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

y=0000	**y=0101**	**y=1010**	**y=1111**	**y=0011**	**y=0110**	**y=1011**
00000000	00000101	00001010	00001111	00000011	00000110	00001011
00010001	00010101	00011011	00011111	00010011	00010111	00011111
00100010	00100111	00101010	00101111	00100011	00100110	00101010
00110011	00110111	00111011	00111111	00110011	00110111	00111011
01000100	01000101	01001110	01001111	01000111	01000110	01001111
01010101	01010101	01011111	01011111	01010111	01010111	01011111
01100110	01100111	01101110	01101111	01100111	11001110	01101111
01110111	01110111	01111111	01111111	01110111	01110111	01111111
10001000	10001101	10001010	10001111	10001011	10001110	10001011
10011001	10011101	10011011	10011111	10011011	10011111	10011011
10101010	10101111	10101010	10101111	10101011	10101110	10101011
10111011	10111111	10111011	10111111	10111011	10111111	10111011
11001100	11001101	11001110	11001111	11001111	11001110	11001111
11011101	11011101	11011111	11011111	11011111	11011111	11011111
11101110	11101111	11101110	11101111	11101111	11101110	11101111
11111111	11111111	11111111	11111111	11111111	11111111	11111111

3.3 Ideals in Max-Plus algebra and related codes

Let S be a Max-Plus algebra, that is precisely a semiring. Then we have two types of substructures in S, the subsemiring and ideals. A non-empty subset A of S is subsemiring if $a_1 \oplus a_2$ and $a_1 \otimes a_2 \in A$ for all $a_1, a_2 \in A$. A becomes an ideal if the second condition is true for all $a_1 \in S$ and $a_2 \in A$.

If A is a subsemiring and $\mathsf{C}(A)$ is the set of all codes of length n over A. Then $\mathsf{C}(A)$ being a subset of S^n is a code over S. If $x = a_1 a_2 \ldots a_n$ and $y = b_1 b_2 \ldots b_n$

are codewords in $\mathsf{C}(A)$ Then

$$
\begin{aligned}
x + y &= a_1a_2 \cdots a_n + b_1b_2 \cdots b_n \\
&= (a_1 \oplus b_1)(a_2 \oplus b_2) \cdots (a_n \oplus b_n) \\
&= max\{a_1, b_1\}max\{a_2, b_2\} \cdots max\{a_n, b_n\} \in \mathsf{C}(A)
\end{aligned}
$$

because $max\{a_i, b_i\} \in A$

Now if, $\alpha \in S$ and $x = a_1a_2 \cdots a_n \in \mathsf{C}(A)$ Then

$$
\begin{aligned}
\alpha x &= \alpha(a_1a_2 \cdots a_n) \\
&= (\alpha \otimes a_1)(\alpha \otimes a_2) \cdots (\alpha \otimes a_n) \notin \mathsf{C}(A)
\end{aligned}
$$

because $\alpha \otimes a_i \notin A$ in general

However if A is an ideal then $\alpha \otimes a_i \in A$ and we get that $\alpha x \in \mathsf{C}(A)$

From the above discussion we have the following result

Proposition 3 3.1. *If A is an ideal in S Then $\mathsf{C}(A)$ is a linear code over S*

Now we will on backward direction that is is it possible that the set of codewords bits in a code provide us an ideal in S For that we have the following result

Proposition 3.3 2. *If C is a cyclic linear code over S then the set I_{C} of codewords bits is an ideal in S*

Proof Let us assume that C is a cyclic linear code as

$$0_S0_S \cdots 0_S \in \mathsf{C}$$

$$\Rightarrow 0_S \in I_{\mathsf{C}}$$

That is I_{C} is non-empty Let $x, y \in I_{\mathsf{C}}$ that is x and y are bits in some codeword $a = a_1a_2 \cdots x \cdots a_n$ and $b = b_1b_2 \cdots y \cdots b_n$ Now if x and y are at the same place in these codeword then by adding them we get that $x \oplus y$ a bit in $a + b$

If x and y are not at the same place, then to bring them at the same place we can apply cyclic shift on b Thus by adding a and b' we get $x \oplus y$ a bit in $a + b'$ Thus we get that $x \oplus y \in I_{\mathtt{C}}$

Now for $\alpha \in S$ and $a = a_1a_2 \quad x \quad a_n \in \mathtt{C}$

$$\alpha(a_1a_2 \quad x \quad a_n) = (\alpha \otimes a_1)(\alpha \otimes a_2) \quad (\alpha \otimes x) \quad (\alpha \otimes a_n) \in \mathtt{C}$$

We get that $\alpha \otimes x$ is a bit in αa Thus, $\alpha \otimes x \in I_{\mathtt{C}}$ Hence $I_{\mathtt{C}}$ is an ideal in S □

If $\mathcal{A}$ and $\mathcal{B}$ be any two ideals in S Then we know that their sum

$$\mathcal{A} + \mathcal{B} = \{a \oplus b \qquad a \in \mathcal{A}, b \in \mathcal{B}\}$$

is also an ideal

Proposition 3.3 3. *If $\mathcal{J}$ and $\mathcal{T}$ be any two ideals in S Then*

$$\mathtt{C}(\mathcal{J} + \mathcal{T}) = \mathtt{C}(\mathcal{J}) + \mathtt{C}(\mathcal{T})$$

Proof If $x \in \mathtt{C}(\mathcal{J} + \mathcal{T})$ Then

$$\begin{aligned} &x(j_1 \oplus t_1)(j_2 \oplus t_2) \quad (j_n \oplus t_n) \\ &= (j_1j_2 \quad j_n) + (t_1t_2 \quad t_n) \in \mathtt{C}(\mathcal{J}) + \mathtt{C}(\mathcal{T}) \end{aligned}$$

We get that

$$\mathtt{C}(\mathcal{J} + \mathcal{T}) \subseteq \mathtt{C}(\mathcal{J}) + \mathtt{C}(\mathcal{T})$$

Similarly,

$$\mathtt{C}(\mathcal{J}) + \mathtt{C}(\mathcal{T}) \subseteq \mathtt{C}(\mathcal{J} + \mathcal{T})$$

□

If $\mathcal{J}$ and $\mathcal{T}$ be any two ideals in S Then we know that their intersection and product are also an ideals with $\mathcal{J}\mathcal{T} \subseteq \mathcal{J} \bigcap \mathcal{T}$

Proposition 3.3.4. *If $\mathcal{J}$ and $\mathcal{T}$ be any two ideals in S. Then*

$$\mathsf{C}(\mathcal{J}\bigcap\mathcal{T}) = \mathsf{C}(\mathcal{J})\bigcap\mathsf{C}(\mathcal{T})$$

$$\mathsf{C}(\mathcal{J}\mathcal{T}) \subseteq \mathsf{C}(\mathcal{J}\bigcap\mathcal{T}) = \mathsf{C}(\mathcal{J})\bigcap\mathsf{C}(\mathcal{T})$$

Proposition 3.3.5. *If C and C' be any two cyclic linear codes over S. Then*

$$I_{\mathsf{C}+\mathsf{C}'} = I_{\mathsf{C}} + I_{\mathsf{C}'}$$

$$I_{\mathsf{C}\cap\mathsf{C}'} \subseteq I_{\mathsf{C}}\bigcap I_{\mathsf{C}'}$$

Proof. If $x \in I_{\mathsf{C}+\mathsf{C}'}$ then x is a bit in some codeword in $\mathsf{C}+\mathsf{C}'$ that is $x = a \oplus a'$ where a is a bit in some codeword in C and a' is a bit in some codeword in C'. In other words $a \in I_{\mathsf{C}}$ and $a' \in I_{\mathsf{C}'}$. Thus $x \in I_{\mathsf{C}} + I_{\mathsf{C}'}$. Similarly $I_{\mathsf{C}} + I_{\mathsf{C}'} \subseteq I_{\mathsf{C}+\mathsf{C}'}$.
If $x \in I_{\mathsf{C}\cap\mathsf{C}'}$, that is x is a bit in some codeword

$$a \in \mathsf{C}\bigcap\mathsf{C}'$$

$$\Rightarrow a \in \mathsf{C} \text{ and } a \in \mathsf{C}'$$

Thus $x \in I_{\mathsf{C}}\bigcap I_{\mathsf{C}'}$.
However, if $x \in I_{\mathsf{C}}\bigcap I_{\mathsf{C}'}$ then $x \in I_{\mathsf{C}}$ and $x \in I_{\mathsf{C}'}$ that is x is a bit in some codeword $a \in \mathsf{C}$ and codeword $b \in \mathsf{C}'$. It not necessary that $a, b \in \mathsf{C}\bigcap\mathsf{C}'$. Hence

$$I_{\mathsf{C}\cap\mathsf{C}'} \subseteq I_{\mathsf{C}}\bigcap I_{\mathsf{C}'}$$

□

Example 3.3.6. *Let $\mathsf{C} = \{000, 100\}$ and $\mathsf{C}' = \{000, 010\}$ be any two cyclic linear codes over S. If*

$$\mathsf{C}\bigcap\mathsf{C}' = \{000\}$$

Then $I_{\mathsf{C}\cap\mathsf{C}'} = \{0\}$. Now if $I_{\mathsf{C}} = \{0, 1\}$ and $I_{\mathsf{C}'} = \{0, 1\}$ then

$$I_{\mathsf{C}}\bigcap I_{\mathsf{C}'} = \{0, 1\}$$

Hence

$$I_{\mathsf{C}\cap\mathsf{C}} \subseteq I_{\mathsf{C}}\bigcap I_{\mathsf{C}'}$$

Bibliography

[1] G W Stewart, *Matrix Algorithm, Volume II Eigensystem*" SIAM Philadelphia 1998

[2] G H Cheng X X Luo and L Li, *The bounds of the eigenvalues for rank one modified of Hermitian matrix* Applied Mathematics Letters **25(6)** (2012) 1191-1196

[3] G H Golub and C F Loan, "*Matrix Computations, 3rd Edition*", The Johns Hopkins University Press, Baltimore MD 1996

[4] ZJ Bai X Huang YF SU, *Nonlinear rank-one modification of symmetric eigenvalues problem* (2010)

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

[2] E R Berlekamp, *Algebraic Coding Theory"*, World Scientific Publishing, 2011

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

[4] P Butkovi, *'Max-linear Systems Theory and Algorithms Springer Monographs in Mathematics"* Springer-Verlag, 2010

[5] K G Farlow, *Max-Plus Algebra, MS Thesis'* Virginia Polytechnic Institute and State University, USA, 2009

[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 van 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

[13] Y Yang and W Cai, *On self-dual constacyclic codes over finite field*, Des Codes Cryptogra 74 (2015) 355-364

Tropical Linear Algebra and Coding Theory

By

Gul Freen

198-FBAS/MSMA/F14

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