T.C.
İSTANBUL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MASTER OF SCIENCE

STRUCTURE THEOREM FOR WEIGHT ENUMERATORS OF SELF-DUAL CODES OVER $\mathbb{F}_3$, $\mathbb{F}_5$

Zekiye Pınar Cihan

Department of Mathematics

Matematik Programı

SUPERVISOR
Doç. Dr. Hatice Boylan

December, 2019

İSTANBUL

Doç. Dr. Hatice Boylan

This work was accepted on 21.01.2020 as a Master of Science in Department of Mathematics, Matematik Programı by the following Committee.

Examination Committee

Doç. Dr. Hatice Boylan (Supervisor)
İstanbul Üniversitesi
Fen Fakültesi

Doç. Dr. Şükrü Yalçınkaya
İstanbul Üniversitesi
Fen Fakültesi

Dr. Öğr. Üyesi Bilge Şipal
İstanbul Kültür Üniversitesi
Fen-Edebiyat Fakültesi

As required by the 9/2 and 22/2 articles of the Graduate Education Regulation which was published in the Official Gazette on 20.04.2016, this graduate thesis is reported as in accordance with criteria determined by the Institute of Graduate Sttudies in Science and Engineering by using the plagiarism software to which İstanbul University is a subscriber.

PREFACE

I would like to thank my supervisor Doç. Dr. Hatice BOYLAN for her support, help, and patience during this period. She has an important part in my life, I learned so many things about mathematic and still, I am learning that from her. So I always feel lucky to studying with her. I thank her so much for giving this wonderful subject as a project of the thesis to me as well. I would like to thank juries Doç. Dr. Şükrü YALÇINKAYA and Dr. Bilge ŞİPAL for their advice during my first presentation of this thesis.
I would like to thank somebody, who are important people for my life. First Prof. Dr. Yılmaz AKYILDIZ, I met with him in one kind of workshop for the math teachers of TUBITAK. He taught to look different perspective to mathematic to me, and he has always supported me for my graduate education of mathematics. So thank him so much for teaching many things and supports. Second Prof. Dr.Mustafa Türker ÖZKAN, he was my professor when I was an undergraduate student in the Department of Astronomy, and still he helps and supports me for whole my master's in Istanbul University, so I thank him for whole help and supports. Third my eye doctor Prof. Dr. Haluk KAZOKOĞLU, I met him when I was a child, then he has been a part of my family. So thank so much him for support, advice and, help.
I would like to thank my family for loves, supports, and helps. Especially, my parents confide in me, and so they have always supported me during this period; I love them. I thank my brother with his family so much for their supports.
As the last word, I need to apologize for certain typographic idiosyncrasies in this master thesis like double point separators in the numbering of theorems, double periods at the end of section references, variable names in upper case in section headings, references like "Table Table 2.2:", and some more. These unfortunate peculiarities are due to the incompatibilities of the class file ("şablon") `iufenbil.cls` required and provided by the university and the packages of the AMS for mathematical typesetting, whose usage is unavoidable for mathematical texts. They disappear as soon as this thesis is typeset with one of the class files provided by plain LaTeX or the AMS.

December, 2019 Zekiye Pınar Cihan

TABLE OF CONTENTS

Page Number

PREFACE ..... **iv**
TABLE OF CONTENTS ..... **vi**
LIST OF TABLES ..... **vii**
ÖZET ..... **viii**
SUMMARY ..... **ix**
1. PART I: INTRODUCTION **1**
2. PART II: GENERAL NOTION **4**
2.1. BASIC NOTIONS OF CODING THEORY 4
2.1.1. Finite Fields $\mathbb{F}_{25}$ and $\mathbb{F}_{49}$ 4
2.1.2. Basic Notions of a Code over a Finite Field 4
2.1.3. Hemming Weight of a Codeword 7
2.2. WEIGHT ENUMERATORS 10
2.3. DUAL AND SELF-DUAL CODES 15
3. PART III: MATERIAL AND METHODS **18**
3.1. SPECIAL CODES OVER $\mathbb{F}_3$ AND $\mathbb{F}_5$ 18
3.1.1. The codes t_4 and g_{12} 18
3.1.2. The Codes c_2, f_6 and e_{10} 19
3.1.3. Algebraic independence 21
3.2. WEIL REPRESENTATIONS OF THE QUADRATIC MODULES $\mathbb{F}_P$ 23
3.3. REPRESENTATION OF GROUPS 28
3.3.1. Quadratic Form 30
3.3.2. Weil Representations of $SL(2,\mathbb{F}_p)$ 31
3.3.3. Invariant Theory 34
3.4. SELF-DUAL CODES AND WEIL REPRESENTATIONS 35
3.4.1. Mac Williams' Identity 35
3.5. MOLIEN SERIES 40
3.5.1. Molien's theorem 40
3.5.2. The Molien series of the Weil representations for $p = 3,5$ 42

4. PART IV: RESULTS 47
4.1. THE MAIN THEOREMS 47
5. PART V: DISCUSSION 50
6. PART VI: CONCLUSION AND RECOMMENDATIONS 52
CURRICULUM VITAE 55

LIST OF TABLES

Page Number

Table 2.1: Finite Field $\mathbb{F}_{25}$ 5

Table 2.2: Finite Field $\mathbb{F}_{49}$ 6

ÖZET

YÜKSEK LİSANS TEZİ

$\mathbb{F}$_3 VE $\mathbb{F}$_5 ÜZERINDEKI SELF-DUAL KODLARIN AĞIRLIK ENUMERATÖRLERI İÇİN YAPISAL TEOREM

Zekiye Pınar Cihan

İstanbul Üniversitesi

Fen Bilimleri Enstitüsü

Matematik Anabilim Dalı

Danışman: Doç. Dr. Hatice Boylan

Asal cisim $\mathbb{F}_p$ üzerindeki kodlar için Lee weight enumerator tamamen uygun, kullanışlı ve ilginçtir. Bu daha çok, p-inci siklotomik cismin reel alt cismi üzerindeki Hilbert' in modüler formlar teorisi ile derinlemesine ilişkisi olması nedeniyledir.
Bu yüksek lisans tezinin amacı, $\mathbb{F}_3$ ve $\mathbb{F}_5$ üzerindeki self-dual kodların Lee weight enumeratorleri tarafından üretilmiş halkaları açıklayan iki teoremi yeniden ispatlamaktır. Bu ispatların şimdiye kadar bilinen ispatlardan farklı olması bu tezin ana fikridir. Örneğin $\mathbb{F}_5$ üzerindeki bu ispatı [Ebe02]'da, Hilbert' in modüler form teorisi kullanılarak kuadratik cisim $\mathbb{Q}(\sqrt{5})$ üzerinde yapılmıştır. Bu çalışmada bundan farklı olarak tamamen cebirsel bir temele dayanan $\mathrm{SL}(2,\mathbb{Z})$'in Weil temsillerinden yararlanarak Boylan ve Skoruppa' nın kendi *Coding Theory* [BS16] ders notlarında açıkladıkları şekilde ispatlanmıştır. Bu tezdeki açıklamalar $\mathbb{F}_3$ üzerindeki self-dual kodların Lee weight enumeratorleri tarafından üretilmş halkanın yapısal sonucunu [BS16] 'da verilen metot ve fikirler kullanılarak açıklanmıştır ve buna ek olarak da $\mathbb{F}_5$ üzerindeki self-dual kodların Lee weight enumeratörlerinin açıklaması da buradaki metotlardan yararlanılarak yeni bir ispat şeklinde yapılmıştır.

Aralık, 2019, $9+56$ sayfa.

Anahtar kelimeler: Kodlar, Weil temsilleri

SUMMARY

M.Sc. THESIS

STRUCTURE THEOREM FOR WEIGHT ENUMERATORS OF SELF-DUAL CODES OVER $\mathbb{F}\_3, \mathbb{F}\_5$

Zekiye Pınar Cihan

İstanbul University

Institute of Graduate Studies in Sciences

Department of Mathematics

Supervisor: Doç. Dr. Hatice Boylan

For codes over a prime field $\mathbb{F}_p$, the Lee weight enumerators of linear codes over $\mathbb{F}_p$ are known to be quite accessible, useful and interesting. This is partly due to the fact that they are intimately connected to the theory of Hilbert modular forms over the totally real subfield of the p-th cyclotomic field.
The aim of this master thesis is to reprove two theorems that describe explicitly the ring generated by the Lee weight enumerators of self-dual codes over $\mathbb{F}_3$ and $\mathbb{F}_5$, respectively. The main point of this project is that the proofs given in this thesis differ from the ones that can be found in the existing literature. For example, [Ebe02] proves the case of $\mathbb{F}_5$ using the theory of Hilbert modular forms over the quadratic field $\mathbb{Q}(\sqrt{5})$. In contrast to that approach the proofs in this thesis are purely algebraic based on the theory of Weil representations of $SL(2,\mathbb{Z})$ and follow ideas of Boylan and Skoruppa explained in their *Coding Theory* lecture notes [BS16]. This thesis explains in detail the methods and ideas used in [BS16] for deducing the structure of the ring generated by the Lee weight enumerators of self-dual codes over $\mathbb{F}_3$ and applies these methods to give a new proof for the explicit description of the Lee weight enumerators of self-dual codes over $\mathbb{F}_5$.

December, 2019, $9+56$ pages.

Keywords: Codes, Weil representations

1. PART I: INTRODUCTION

The classification of codes over a given finite field is currently, if not for ever, out of reach. In other words it is unknown how to describe the equivalence classes of such codes by a system of complete invariants whose codomain can be easily described. However, there are invariants, albeit not complete systems of such, whose codomains can be sometimes explicitly described: The weight enumerators of various kinds.

For codes over a prime field $\mathbb{F}_p$, the Lee weight enumerators of linear codes over $\mathbb{F}_p$ are known to be quite accessible, useful and interesting. This is partly due to the fact that they are intimately connected to the theory of Hilbert modular forms over the totally real subfield of the p-th cyclotomic field. Hirzebruch was the first to study this in connection with cusps of the Hilbert modular surface associated with the quadratic field $\mathbb{Q}(\sqrt{5})$ in 1985.

Our goal in this master thesis is to reprove two theorems that describe explicitly the ring generated by the Lee weight enumerators of self-dual codes over $\mathbb{F}_3$ and $\mathbb{F}_5$, respectively. Our proofs are purely algebraic and they are based on the theory of the Weil representations of $\mathrm{SL}(2,\mathbb{Z})$ and follow ideas of Boylan and Skoruppa explained in [BS16]. We explain in detail the methods and ideas used in [BS16] for deducing the structure of the ring generated by the Lee weight enumerators of self-dual codes over $\mathbb{F}_3$, and apply these methods to give a new proof for the explicit description of the Lee weight enumerators of self-dual codes over $\mathbb{F}_5$.

This master thesis has six parts and nine subsections. First part is the introduction.

Second part is the general notion which includes three subsections. In the first three subsections we prepare for the proofs of the cited theorems; in subsections one to three, some of the basics of the theory of linear codes over a prime field are included. In particular it is focused on the lee weight enumerators associated to a linear code. Other key notions mentioned are hamming weight, weight enumerator, complete weight enumerator, parity extension of code, the dual code, and self-dual codes.

Third part is the material and methods which includes three subsections. In [3.1.], we introduce five specific self-dual codes over $\mathbb{F}_3$ and $\mathbb{F}_5$ needed in two main theorems in section four. These are :

- Any maximal isotropic subgroup in the finite quadratic module $(\mathbb{F}_3^4, (x_1^2+x_2^2+x_3^2+x_4^2)/3)$, e.g., the tetra code t_4,
- The parity extension of the ternary Golay code $G_{3,11}$,
- Any maximal isotropic subgroup of the finite quadratic module $(\mathbb{F}_5^2, (x_1^2, x_2^2)/5)$, e.g., the code C_2,
- The code F_6,
- The code e_{10}.

The Lee weight enumerator of these codes are computed. It is shown that the Lee weight enumerators of the first three codes and of the last three codes are algebraically independent, respectively. So they generate rings R_3 and R_5 which are isomorphic to the ring of complex polynomials in two and three variables, respectively. The main theorems to be proved in this project can be stated in the form that the subrings of $\mathbb{C}[x_0, x_1]$ and $\mathbb{C}[x_0, x_1, x_2]$ generated by the Lee weight enumerators of self-dual codes over $\mathbb{F}_3$ and $\mathbb{F}_5$ coincide with R_3 and R_5, respectively.

Subsection 3.3.2. introduces the Weil representations associated to the finite quadratic modules $\underline{\mathbb{F}_p}(a) := (\mathbb{F}_p, \frac{ax^2}{p})$ $(a \in \mathbb{F}_p^+)$ for odd prime p. For a given p, this Weil representations define a $\mathrm{SL}(2,\mathbb{F}_p)$ module structure on the space of linear forms of the polynomial ring $\mathbb{C}[\{x_a\}_{a\in\mathbb{F}_p}]$. The Weil representation is naturally extended to the whole polynomial ring $\mathbb{C}[\{x_a\}_{a\in\mathbb{F}_p}]$, which becomes thus a graded $\mathrm{SL}(2,\mathbb{F}_p)$-module. The map $l : x_0 \mapsto x_0$ and $x_i \mapsto x_{p-i}$ $(1 \le i \le p)$ intertwines with the action of $\mathrm{SL}(2,\mathbb{F}_p)$, and hence the $+1$ and -1 eigenspaces of the involution l are invariant under $\mathrm{SL}(2,\mathbb{F}_p)$. The +1-eigenspace equals the space of all polynomials in the basic polynomials $y_0 = x_0$, and $y_i = x_i + x_{p-i}$ $(1 \le i \le \frac{p-1}{2})$, which are obviously algebraically independent. Hence, $\mathrm{SL}(2,\mathbb{Z}_p)$ acts on the polynomial ring in the $\frac{p+1}{2}$ variables $\mathbb{C}[y_0, \cdots, y_{\frac{p-1}{2}}]$.

In [3.4.] an important theorem is proven that a code over $\mathbb{F}_p$ (where p is odd prime) is a self-dual code if and only if its Lee weight enumerator is invariant under the action of $\mathrm{SL}(2,\mathbb{F}_p)$ on the polynomial ring $\mathbb{C}[y_0, \cdots, y_{\frac{p-1}{2}}]$ described in section three. This theorem can be viewed as a conceptual generalization of the classical Mac Williams' identity. As a consequence the subring L_p of $\mathbb{C}[y_0, \cdots, y_{\frac{p-1}{2}}]$ generated by the Lee weight enumerators of self-dual codes over $\mathbb{F}_p$ is contained in the ring $I_p := \mathbb{C}[y_0, \cdots, y_{\frac{p-1}{2}}]^{\mathrm{SL}(2,\mathbb{F}_p)}$ of invariants for

the Weil representations.

Subsection 3.5. consists of results. In [3.5.] the Molien series of the $\mathrm{SL}(2,\mathbb{F}_p)$-module $\mathbb{C}[y_0,\cdots,y_{\frac{p-1}{2}}]$ is calculated. For this one needs, for any g in $\mathrm{SL}(2,\mathbb{F}_p)$ an explicit formula for $\chi(g) = tr(g,\mathbb{C}[y_0,\cdots,y_{\frac{p-1}{2}}]_1)$, i.e., an explicit formula for the restriction of the Weil representations onto the space of linear forms.

Finally, in section four the proofs of the main theorems are given. Since $R_p \subseteq L_p \subseteq I_p$ (the first inclusion being obvious, the second one following from the result in section five) it suffices to prove for $p = 3,5$ that $\dim(R_p)_d = \dim(I_p)_d$ for all $d \geq 0$, where $(R)_d$ denotes the subspace of the homogeneous polynomials in the ring R. This follows easily from the fact that R_2 and R_3 are polynomial rings as shown in Subsection 3.1. and the explicit formulas for the Molien series obtained in Subsection 3.5.

In part five, we give the concluding remarks.

In part six, we review the study. We examine all parts, their contents and what can be done in future studies.

2. PART II: GENERAL NOTION

2.1. BASIC NOTIONS OF CODING THEORY

2.1.1. Finite Fields $\mathbb{F}_{25}$ and $\mathbb{F}_{49}$

Definition 2..1. If a field F has finite number of the elements, then it is called a finite field.

Theorem 2..2 ([Ser77, p. 3, Thm. 1])**.** *The characteristic of a finite field F is a prime number $p \neq 0$; if $r = [F, \mathbb{F}_p]$, the number of elements of F is $q = p^r$. All finite fields with $q = p^r$ elements are isomorphic to $\mathbb{F}_q$.*

Remark 2..3. If $n > 1$, the finite field F_{p^n} is isomorphic to $\mathbb{F}_p[x]/(g(x))$, where $g(x) \in \mathbb{F}_p[X]$ is an irreducible monic polynomial. Let $\theta = x + (g(x))$. Then $\{\theta^0, \theta^1, \cdots, \theta^{n-1}\}$ is a basis of $\mathbb{F}_{p^n}$ as vector space over $\mathbb{F}_p$.

Example 2..4 (Examples of F_{25} and F_{49})**.** 1. Firstly, we must find $g(x) \in \mathbb{F}_5[X]$, where $g(x)$ is an irreducible monic polynomial of degree 2. We can choose that $g(x) = x^2 - x + 2$. Setting $\alpha = x + (g(x))$, we have $\mathbb{F}_{25} = \mathbb{F}_5 \oplus \mathbb{F}_5 \cdot \alpha$. Moreover $\mathbb{F}_{25}^* = \langle \alpha \rangle$. Table **Table 2.1:** expresses the powers α^n in the $\mathbb{F}_5$ - basis $1, \alpha$.

2. Similarly, first we must find $h(x) \in \mathbb{F}_7[X]$, where $h(x)$ is an irreducible monic polynomial of degree 2. We can choose $h(x) = x^2 - x + 3$. Setting $\theta = x + (h(x))$, we have $\mathbb{F}_{49} = \mathbb{F}_7 \oplus \mathbb{F}_7 \cdot \theta$. Moreover $\mathbb{F}_{49}^* = \langle \theta \rangle$. Table **Table 2.2:** expresses the powers θ^n in the $\mathbb{F}_7$ - basis $1, \theta$.

2.1.2. Basic Notions of a Code over a Finite Field

Definition 2..5. Let C be any code of length n over a finite field $\mathbb{F}_q$. Then C is called linear code if and only if C is a subspace of $\mathbb{F}_q^n$.

Remark 2..6. Every linear combination of codewords is also codewords in the linear code C.

Example 2..7. If $C \subset \mathbb{F}_5^4$, the the following code is

$$C = \{0000, 1020, 2040, 3010, 4030\}.$$

Table 2.1: Finite Field $\mathbb{F}_{25}$

Power of α	Polynomials in $\mathbb{F}_{25}$
0	0
α^0	1
α^1	α
α^2	$\alpha+3$
α^3	$4\alpha+3$
α^4	$2\alpha+2$
α^5	$4\alpha+1$
α^6	2
α^7	$2\alpha+1$
α^8	$3\alpha+1$
α^{10}	$4\alpha+4$
α^{11}	$3\alpha+2$
α^{12}	4
α^{13}	4α
α^{14}	$4\alpha+2$
α^{15}	$\alpha+2$
α^{16}	$3\alpha+3$
α^{17}	$\alpha+4$
α^{18}	3
α^{19}	3α
α^{20}	$3\alpha+4$
α^{21}	$2\alpha+4$
α^{22}	$\alpha+1$
α^{23}	$2\alpha+3$

Let $v_1 = 1020$, $w_1 = 2040$, $v_2 = 3010$, $w_2 = 4030$. Then we have,

$$\begin{aligned} v_1 + w_1 &= 3010 \in C \\ v_1 + v_2 &= 4030 \in C \\ v_1 + w_2 &= 0000 \in C \\ w_1 + v_2 &= 0000 \in C \\ w_1 + w_2 &= 1020 \in C \\ v_2 + w_2 &= 2040 \in C. \end{aligned}$$

Moreover, $\mathbb{F}_5 \cdot c = C$. In fact, $C = \{a \cdot 1020 : a \in \mathbb{F}_5\}$. Hence, C is a subspace of $\mathbb{F}_5^4$ so it is a linear code of length 4 over $\mathbb{F}_5$.

Table 2.2: Finite Field $\mathbb{F}_{49}$

Power of β	Polynomials in $\mathbb{F}_{49}$	Power of θ	Polynomials in $\mathbb{F}_{49}$
0	0	θ^{24}	6
θ^0	1	θ^{25}	6θ
θ^1	θ	θ^{26}	$6\theta+3$
θ^2	$\theta+4$	θ^{27}	$2\theta+3$
θ^3	$5\theta+4$	θ^{28}	$5\theta+1$
θ^4	$2\theta+6$	θ^{29}	$6\theta+6$
θ^5	$\theta+1$	θ^{30}	$5\theta+3$
θ^6	$2\theta+4$	θ^{31}	$\theta+6$
θ^7	$6\theta+1$	θ^{32}	4
θ^8	3	θ^{33}	4θ
θ^9	3θ	θ^{34}	$4\theta+2$
θ^{10}	$3\theta+5$	θ^{35}	$6\theta+2$
θ^{11}	$\theta+5$	θ^{36}	$\theta+3$
θ^{12}	$6\theta+4$	θ^{37}	$4\theta+4$
θ^{13}	$3\theta+3$	θ^{38}	$\theta+2$
θ^{14}	$6\theta+5$	θ^{39}	$3\theta+4$
θ^{15}	$4\theta+3$	θ^{40}	5
θ^{16}	2	θ^{41}	5θ
θ^{17}	2θ	θ^{42}	$5\theta+6$
θ^{18}	$2\theta+1$	θ^{43}	$4\theta+6$
θ^{19}	$3\theta+1$	θ^{44}	$3\theta+2$
θ^{20}	$4\theta+5$	θ^{45}	$5\theta+5$
θ^{21}	$2\theta+2$	θ^{46}	$3\theta+6$
θ^{22}	$4\theta+1$	θ^{47}	$2\theta+5$
θ^{23}	$5\theta+2$		

,

Definition 2..8. An information rate of C is shown that $r(C)$ and it is defined by

$$r(C) := \frac{\log_q(|C|)}{\log_q(|\mathbb{F}_q^n|)} = \frac{\log_q(|C|)}{n}.$$

Definition 2..9. If the information rate of the linear code C be $\frac{k}{n}$. Then C is called a code of type2 $[n,k]_q$-code ($k = \dim C$).

Example 2..10. The information rate of the linear code C from the previous example is $R(C) = \frac{1}{4}$. Because, $|C| = 5$, then $\log_5(|C|) = \log_5 5 = 1$; $|\mathbb{F}_5^4| = 5^4$, then $\log_5 5^4 = 4$ hence $R(C) = \frac{1}{5}$. Thus, the linear code C of type is $[4,1]_5$-linear code.

2.1.3. Hemming Weight of a Codeword

Every distinct codeword in C should have different places, so the *Hamming distance* is very important for measuring in how many places the distinct words differ.

Definition 2..11. Let $t = \{t_1, \cdots, t_n\}$ and $r = \{r_1, \cdots, r_n\}$ be two words in $\mathbb{F}_q^n$. The Hamming distance is defined as the number of the different places between two words t, r, such that

$$h(t,r) := \#\{i : t_i \neq r_i\}.$$

For instance, $(cold)$ and $(corn)$ are two distinct words. The Hamming distance between $(cold)$ and $(corn)$ is

$$h(cold, corn) = 2.$$

Definition 2..12. Let C be a linear code. The minimal distance of C is defined as

$$d(C) := min\{h(m,n) | m \neq n, m, n \in C\}.$$

Definition 2..13. An $[n,k,d]$-code is a code C of length n, where $\dim C = k$ and $d(C) = d$.

Definition 2..14. Let C be a linear code of length n and $c = (c_1, c_2, \cdots, c_n)$ be a codeword of C. The Hamming weight of c, denoted by $h(c)$, is the number of nonzero places in C. i.e.,

$$h(c) := \#\{i : c_i \neq 0\}.$$

Example 2..15. Let $C = \{0000, 1001, 1000, 0001\}$ be a linear code over $\mathbb{F}_2^4$. Then the Hamming weights of the codewords in C :

$$h(1001) = 2,$$
$$h(1000) = 1,$$
$$h(0001) = 1.$$

Definition 2..16. Let C be a linear code of length n. A minimal distance $d(C)$ is the smallest

of the Hamming weights of the nonzero codewords of C. i.e.,

$$d(C) := \min\{h(c,0) : c \neq 0, c \in C\} = \min_{c\neq 0, c\in C} h(c).$$

Example 2..17. Consider the binary linear code $C = \{0000, 1000, 0100, 1100\}$. We have

$$h(1000) = 1,$$
$$h(0100) = 1,$$
$$h(1100) = 2.$$

Hence, $d(C) = 1$.

Definition 2..18. Let C be a $[n,k,d]$-code. An extended code is the parity extension code denoted by $\bar{C}$, of C is the code obtained by adding an extra parity bit to every codeword in C. Therefore $\bar{C}$ has codewords of length $n+1$. If C is binary and d is odd, then the extended code $\bar{C}$ is a $[n+1,k,d+1]$-code. (see [BS16, p. 13, Examples of Codes]).

Definition 2..19. If a linear code C of length n is invariant under $(c_0c_1\cdots c_{n-1}) \mapsto (c_{n-1}c_0\cdots c_{n-2})$, it is called a cyclic code.

Remark 2..20. There is a useful, more algebraic characterization of cyclic codes. For this we identify F^n with the ring (for any field F)

$$R_n := F[X]/(x^n - 1)$$

via the isomorphism of F-vector spaces

$$c_0c_1\cdots c_{n-1} \rightarrowtail [c_0 + c_1x + \cdots + c_{n-1}x^{n-1}]_{x^n-1},$$

where $[f]_{x^n-1}$ denotes the residue class $f + (x^n - 1)$. Note, for $n \geq 2$, R_n is not a field since $x^n - 1$ is not irreducible. In general, R_n is a ring. More important for us is that R_n is an $F[X]$-module via

$$(f, [g]_{x^n-1}) \rightarrowtail (f \cdot g)_{x^n-1}.(see[\text{BS16}, p.\ 39]).$$

Theorem 2..21 ([LX04, p.141, Thm. 7.3.1]). *Let $x^n - 1 = g(x).h(x)$ in $\mathbb{F}_q[X]$. If*

$$g(x) = g_0 + g_1 x + \cdots + g_{n-k}x^{n-k},$$
$$h(x) = h_0 + h_1 x + \cdots + h_k x^k,$$

then an $n \times k$ generator matrix G for the code C with the generator polynomial g is defined as

$$\mathbf{G} := \begin{pmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ x^3 g(x) \\ \vdots \\ x^{k-1} g(x) \end{pmatrix} = \begin{bmatrix} g_0 & 0 & \dots & 0 \\ g_1 & g_0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_{n-k} & g_{n-k-1} & \cdots & g_0 \\ 0 & g_{n-k} & \cdots & g_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & g_{n-k} \end{bmatrix}.$$

Corollary 2..22 ([LX04, p.144, Cor. 7.3.9]). *An $(n-k) \times n$ control matrix (or parity-check matrix) H for the code C with control polynomial h is defined as*

$$\mathbf{H} := \begin{bmatrix} 0 & \dots & 0 & 0 & h_k & \dots & h_0 \\ 0 & \dots & 0 & h_k & \dots & h_0 & 0 \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots & \vdots \\ h_k & \dots & h_0 & 0 & 0 & \dots & 0 \end{bmatrix}.$$

Example 2..23. The Golay code over $\mathbb{F}_3$ of length 11 is $[11,6,5]_3$. The generator polynomial is $g = x^5 + 2x^3 + x^2 + 2x + 2$, and the 6×11 generator matrix

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

$x^{11}-1=(x^5+2x^3+x^2+2x+2).(x^6+x^4+2x^3+2x^2+2x+1)$,therefore the control polynomial is $h=x^6+x^4+2x^3+2x^2+2x+1$, and the 5×11 control matrix

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

2.2. WEIGHT ENUMERATORS

The weight enumerators give information about weight and distance of codes, they are polynomials with the number of the weights as their coefficients.

Usual (Hamming) Weight enumerator:

Definition 2..24. Let C be a linear code of type $[n,k,d]$. A usual (or Hamming) weight

enumerator of the code C, is denoted by $w_C(x)$, is the polynomial

$$\begin{aligned} w_C(x) &:= \sum_{c \in C} x^{h(c)} \\ &= \sum_{j=0}^{n} B_j x^j \in \mathbb{Z}[X], \end{aligned} \tag{2.1}$$

where $j = h(c)$, and B_j is the number of the weight j of codewords. This is the homogeneous polynomial of degree equal to the length of the code.

Remark 2..25. The usual weight enumerator gives some information for especially the binary codes.

Example 2..26. We compute the usual weight enumerator for the $[7,4,3]_2$- Hamming code. It has $2^4 = 16$ codewords whose length 7 and minimum distance $d = 3$. i.e.,

0000000	1000110
0001101	1001011
0010111	1010001
0011010	1011100
0100011	1100101
0101110	1101000
0110100	1110010
0111001	1111111

Then we have

$$\begin{aligned} h(0000000) = 0, then \quad & B_0 = 1, \\ h(1111111) = 7, then \quad & B_1 = 1, \\ h(0001101) = h(0011010) &= h(0100011) = h(0110100) \\ &= h(1000110) = h(1010001) = h(1101000) = 3, then \quad B_2 = 7, \\ h(0010111) = h(0101110) &= h(0111001) = h(1001011) \\ &= h(1011100) = h(1100101) = h(1110010) = 4, then \quad B_3 = 7, \end{aligned}$$

where B_0, B_1, B_2, B_3 denote the number of the same Hamming weight of the codewords in the Hamming code.

Thus,the usual weight enumerator of the Hamming code over $\mathbb{F}_2$ is that

$$w_H = 1 + 7x^3 + 7x^4 + x^7.$$

Example 2..27. The binary extended Hamming code $\bar{H}$ is defined as $[8,4,4]_2$ - Hamming code. Only the codewords of odd weight become codewords of increased weight in the extended Hamming code, due to the addition of a parity bit. Therefore

$$w_{\bar{H}} = 1 + 14x^4 + x^8.$$

Complete Weight Enumerator: The complete weight enumerator is more general weight enumerator which gives more information about the linear code if the ground field has odd characteristic.

Definition 2..28. Let C be a $[n,k,d]$-code over $\mathbb{F}_p$. A complete weight enumerator of the linear code C is defined as

$$cw_C := \sum_{\substack{k_{a_1},k_{a_2},\cdots,k_{a_p}\geqslant 0 \\ k_{a_1}+k_{a_2}+\cdots+k_{a_p}=n}} A(k_{a_1},\cdots,k_{a_q}) x_{a_1}^{k_{a_1}} \ldots x_{a_p}^{k_{a_p}} \in \mathbb{Z}[\{x_a\}_{a\in\mathbb{F}_p}], \tag{2.2}$$

where index of the a_j is a fixed enumeration of $\mathbb{F}_p$, and $A(k_{a_1},\cdots,k_{a_p})$ is the number of the codewords in C which have k_{a_j} entries equal to a_j. i.e.,

$$A(k_0,\cdots,k_{p-1}) := Card\{c\in C : c \quad contains \quad exactly \quad k_0 - many \quad 0's, \cdots k_{p-1} - many \quad p-1's\}.$$

Note that

$$\sum_{a\in\mathbb{F}_q} k_a = n,$$

where k_a are non-negative integers.

Remark 2..29. If x_0 is replaced by 1 and all other x_a are replaced by x, then the complete weight enumerator equals to the usual (Hamming) weight enumerator w_C.

Proposition 2..30. *If $\mathbb{F}_p = \mathbb{F}_2$, then the complete weight enumerator cw_C implies that*

$$cw_C(x_0,x_1) = x_0^n w_C(x_1/x_0).$$

Proof.

$$\begin{aligned} cw_C(x_0,x_1) &= \sum_{\substack{k_0,k_1\geqslant 0\\ k_0+k_1=n}} A(k_0,k_1)x_0^{k_0}x_1^{k_1} \\ &= \sum_{\substack{k_0,k_1\geqslant 0\\ k_0+k_1=n}} A(k_0,k_1)x_0^{n-k_1}x_1^{k_1} \\ &= x^n \sum_{\substack{k_0,k_1\geqslant 0\\ k_0+k_1=n}} A(k_o,k_1)(x_1/x_0)^{k_1} \\ &= x^n.w_C(x_1/x_0). \end{aligned}$$

□

Example 2..31. The tetra code t_4 over $\mathbb{F}_3$ of length 4 is form $[4,2,3]_3$ - code, and the elements of Tetra code

$$\{0000,1110,0121,2220,0212,1201,2102,2011,1022\},$$

and the generator matrix is

$$\mathbf{t_4} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix}.$$

The homogeneous usual weight enumerator :

$$\begin{aligned} &h(1110) = h(0121) = h(2220) = h(0212) \\ &\quad = h(1201) = h(2102) = h(2102) = h(1022) = 3. \end{aligned}$$

Thus,there are 8 codewords of weight 3, and one codeword of weight 0. Hence,the usual weight enumerator of $\mathbf{t_4}$ is

$$w_C(x_0,x_1,x_1) = x_0^4 + 8x_0x_1^3. \tag{2.3}$$

The complete weight enumerator of the tetra code is

$$cw_C(x_0,x_1,x_2) = x_0^4 + x_0x_1^3 + x_0x_2^3 = x_0^4 + x_0(x_1+x_2)^3,$$

since the arithmetic in $\mathbb{F}_3[X]$, i.e., $(x_1+x_2)^3 = x_1^3+x_2^3 \mod 3$.

Lee Weight Enumerator: The Lee weight enumerator is important for codes with more than three variables. So that $p > 2$, where p is odd prime.

Definition 2..32. Suppose $p = 2t+1$ (where t is the non-negative integer) is an odd prime number. Let C be the linear code over $\mathbb{F}_p$. Then the Lee weight enumerator is defined as

$$lw_C(x_0,x_1,\ldots,x_t) := \sum_{c\in C} x_0^{l_0(c)}\cdots x_t^{l_t(c)},$$

where $l_0(c)$ is the number of the 0's in the codeword c, and $l_j(c), 1 \le j \le t$, is the number of $\mp j$ in the codeword c.

Example 2..33. Some codes over $\mathbb{F}_p$:

- Let C_1 be any linear code over $\mathbb{F}_3$. Then C_1 is a polynomial in 2 variables, since $3 = 2t+1$ implies $t = 1$. If we replace x_1 by x_2, we can write the complete weight enumerator. The Lee weight enumerator is the same with the usual weight enumerator for the code C_1. i.e.,$lw_{C_1}(x_0,x_1) = w_{C_1}(x_0,x_1)$.

- Let C_2 be any linear code over $\mathbb{F}_5$. Then the Lee weight enumerator of C_2 is a polynomial in 3 variables, since $5 = 2t+1$ implies $t = 2$. The Lee weight enumerator is for C_2 : $l_0(v) = p$ is the consisting o's, $l_1(v) = r$ is consisting ±1's and $l_2(v) = s$ is consisting ±2's in code C_2 for $v \in C_2$. Then,

  $$lw_{C_2}(x_0,x_1,x_2) = \sum_{v\in C_2} x_0^p x_1^r x_2^s,$$

  and the usual weight enumerator,

  $$w_{C_2}(x_0,x_1) = lw_{C_2}(x_0,x_1,x_1).$$

- Let C_3 be any linear code over $\mathbb{F}_7$. Then the Lee weight enumerator of C_3 is a polynomial in 4 variables, since $7 = 2t+1$ implies $t = 3$. The Lee weight enumerator is for C_3 : $l_0(v) = a$ is the consisting 0's, $l_1(v) = b$ is consisting ±1's, $l_2(v) = c$ is consisting

± 2's and $l_3(v) = d$ is consisting ± 3's in the code C_3 for $v \in C_3$. Then,

$$lw_{C_3}(x_0, x_1, x_2, x_3) = \sum_{v \in C_3} x_0^a x_1^b x_2^c x_3^d,$$

and the usual weight enumerator of $\mathscr{C}_3$,

$$lw_{C_3}(x_0, x_1, x_1, x_1) = w_{C_3}(x_0, x_1).$$

2.3. DUAL AND SELF-DUAL CODES

In coding theory, one of the important constructions about codes is also the dual of a given code.

Definition 2..34. Let W be a vector space over the field K, and let T be a subset of W. The *annihilator* T^0 *is the set of linear functional* g *on* W *such that* $g(\gamma) = 0$*, for all* $\gamma \in T$.T^0 *is a subspace of the dual space* W^* *of* W.

Theorem 2..35 ([HK71, p.101, Thm. 16])**.** *Let* V *be a finite dimensional vector space over the field* F*,* W *be a subspace of* V*, and* W^0 *be annihilator of* W*. Then*

$$\dim W + \dim W^0 = \dim V.$$

Proof. We follow [HK71, p. 101-102]. Let $\{\alpha_1, \cdots, \alpha_k\}$ be a basis for k-dimensional vector space W. Take vectors $\alpha_{k+1}, \cdots, \alpha_n$ in n-dimensional vector space V such that $\{\alpha_1, \cdots, \alpha_n\}$ is a basis for V. Let $\{f_1, \cdots, f_n\}$ be a basis for the dual space V^*.
The claim is that $\{f_{k+1}, \cdots, f_n\}$ is the basis for the annihilator W^0. Now, we know that

$$f_i(\alpha_j) = \delta_{ij},$$

and $\delta_{ij} = 0$, if $i \geq k+1$, and $j \leq k$, since $f_i(\alpha) = 0$ for $i \geq k+1$ whenever α is a linear combination of $\alpha_1, \cdots, \alpha_k$. The linear functionals $f_{k+1}, \cdots, f_n$ are linearly independent. Then suppose f in V^*, now

$$f = \sum_{i=1}^{n} f(\alpha_i) f_i = 0,$$

for $i \leq k$. Thus f in W^0, and then

$$f = \sum_{i=k+1}^{n} f(\alpha_i) f_i = 0.$$

Hence, if V is n-dimensional vector space and W is k-dimensional subspace of V, then $\dim W^0 = n-k$. □

Definition 2..36. Let F be a finite field. Let $y, z \in F^n$. An inner product $(y|z)$ is defined as the dot product $y.z$ on the vector space F^n for a fixed basis. Therefore if $y = (y_1, \cdots, y_n)$ and $z = (z_1, \cdots, z_n)$ with respect to the fixed basis then,

$$(y|z) := yz = y_1 z_1 + \cdots + y_n z_n.$$

Remark 2..37. Any inner product $(y|z)$ is non-degenerate since, for a dot product with respect to any basis $y.z = 0$ for all $y \in F^n$ implies that $z = 0$.

Definition 2..38. Let C be any code (not necessarily linear code). Let F be a finite field. A dual code of C, is denoted by $C^\perp$, is defined by

$$C^\perp := \{w \in F^n : w.v = 0 \quad \text{for all} \quad v \in C\}. \tag{2.4}$$

Remark 2..39. Every dual code is also a linear code over the finite field F, as can bee seen by 2.4. If $\dim c = k$, then $\dim C^\perp = n-k$.

Example 2..40. The Golay code over the finite field $\mathbb{F}_3$ is type $[11,6]_3$-code. Then,the dual Golay code $G^\perp$ is type $[11,5]_3$-code.

Proposition 2..41 ([BS16, p. 59])**.** *Let C be a linear code of length n over $\mathbb{F}_q$. Then*

$$\dim C + \dim C^\perp = n.$$

Proof. Let $\{c_1, c_2, \cdots, c_k\}$ be a basis for the linear code C. Take some vectors $c_{k+1}, \cdots, c_n$ in F^n such that $\{c_1, \cdots, c_k, c_{k+1}, \cdots, c_n\}$ is a basis for F^n. Let $\{f_{k+1}, \cdots, f_n\}$ be the dual basis for C^0, as defined in 2..35. Then from the definition 2..38

$$f = \sum_{i=1}^{n} f(c_i) f_i = 0, \quad for \quad f \in C^\perp.$$

Similarly, for $i \leq k$, and $f \in C^0$.

$$f = \sum_{j=k+1}^{n} f(c_j) f_j = 0.$$

Thus,the dual code $C^\perp$ is a annihilator of C so it is the null space of the $k \times n$ generator matrix of G, such that

$$u \in C^\perp,$$

$$x.G.v = 0, \quad \text{for} \quad v \in \mathbb{F}^n \quad \text{and } G \text{ is generator-matrix of } C,$$

$$Gx^t = 0.$$

Hence, $\dim C^\perp = n - k$. □

Definition 2..42. Let C be a linear code of length n. If the dual code of C is the same code with C, i.e. $C^\perp = C$, then the dual code $C^\perp$ is called self-dual code. If $C^\perp \subseteq C$, then the dual code $C^\perp$ is called self-orthogonal code.

Definition 2..43. Let C be an $[n,k]_q$-code. A generator matrix G of C is a $k \times n$ matrix, such that all rows of G form a basis for C. If the generator matrix of the form $(I_k|X)$, then a generator matrix is called to be in standard form, where I_k the $k \times k$ identity matrix, and X is a $k \times n-k$ matrix.

Definition 2..44. Let C be an $[n,k]_q$-code. A control matrix H of C is a generator matrix for the dual code $C^\perp$. Then it is a $(n-k) \times n$ matrix.

Remark 2..45. In particular, given a $k \times n$ matrix G, then G is generator matrix of C if and only if the rows of G are linearly independent and $GH^t = 0$.(See e.g. [LX04, p. 53, Remark 4.5.5])

Theorem 2..46. *If $G = [I_k|X]$ is the generator matrix in standard form for the $[n,k]$-code C, then $H = [-X^t|I_{n-k}]$ is the control matrix for C.*

3. PART III: MATERIAL AND METHODS

3.1. SPECIAL CODES OVER $\mathbb{F}_3$ AND $\mathbb{F}_5$

The five codes described in this section play a very significant role in the two main theorems.

3.1.1. The codes t_4 and g_{12}

The *tetra code* t_4 is a $[4,2,3]_3$-code, which is a maximal isotropic subgroup in the finite quadratic module $(\mathbb{F}_3^4, (x_1^2+x_2^2+x_3^2+x_4^2)/3))$. Its generator matrix is

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix} \tag{3.1}$$

That is a self-dual code as one sees from the generator matrix: The scalar product of each row with itself is 0 and the scalar product of the first and second row is 0 too. The weight enumerators of t_4 are as follows [NRS06, p. 67] (In fact, [NRS06] gives only the usual and the complete weight enumerators. For the Lee weight enumerator we use that $lw_{t_4}(x_0,x_1) = cw_{t_4}(x_0,x_1,x_1) = x_0^4 + x_0(x_1+x_1)^3$.)

- The usual weigh enumerator: $w_{t_4}(x_0,x_1) = x_0^4 + 8x_0x_1^3$.
- The complete weight enumerator: $cw_{t_4}(x_0,x_1,x_2) = x_0^4 + x_0(x_1+x_2)^3$.
- The Lee weight enumerator:

$$lw_{t_4}(x_0,x_1) = x_0^4 + 8x_0x_1^3. \tag{3.2}$$

Note that $lw_{C_1}(x_0,x_1) = w_{C_1}(x_0,x_1)$.

The *parity extension* g_{12} *of the ternary Golay code* is a $[12,6,6]_3$-code [Ebe02, p. 145]. The

generator matrix of the extended Golay code is [Ebe02, p. 145]

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}. \tag{3.3}$$

This code is a self-dual code [Ebe02, p. 145]. The weight enumerators of g_{12} are as follows [NRS06, p. 67]

- The usual weight enumerator:

$$w_{\bar{g}}(x_0,x_1) = x_0^{12} + 264x_0^6x_1^6 + 440x_0^3x_1^9 + 24x_1^{12}.$$

- The complete weight enumerator:

$$\begin{aligned} &cw_{\bar{g}}(x_0,x_1,x_2) \\ &\quad = x_0^{12} + x_1^{12} + x_2^{12} + 22(x_0^6x_1^6 + x_0^6x_2^6 + x_1^6x_2^6) + 220(x_0^6x_1^3x_2^3 + x_0^3x_1^6x_2^3 + x_0^3x_1^3x_2^6). \end{aligned}$$

- The Lee weight enumerator:

$$lw_{\bar{g}}(x_0,x_1) = w_{\bar{g}}(x_0,x_1). \tag{3.4}$$

3.1.2. The Codes c_2, f_6 and e_{10}

The *code* c_2 is a maximal isotropic subgroup in the finite quadratic module $(\mathbb{F}_5^2, (x_1^2+x_2^2)/5)$. It is defined as

$$c_2 = \{00, 12, 24, 31, 43\} \subset \mathbb{F}_5^2. \tag{3.5}$$

That is a self-dual code over $\mathbb{F}_5$ [MS77, ch.5.§6 p. 145]. Its generator matrix is

$$\begin{bmatrix} 1 & 2 \end{bmatrix}. \tag{3.6}$$

That is from [LPS82, p. 182]. The weight enumerators of c_2 are as follows [MS77, ch.5.§6 p. 145]

- The usual weight enumerator : $w_{c_2}(x_0,x_1) = x_0^2 + 4x_1^2$,

- The complete weight enumerator :

$$cw_{c_2}(x_0,x_1,x_2,x_3,x_4) = x_0^2 + x_1x_2 + x_4x_2 + x_1x_3 + x_4x_3,$$

- The Lee weight enumerator:

$$lw_{c_2}(x_0,x_1,x_2) = x_0^2 + 4x_1x_2. \tag{3.7}$$

The *code* f_6 is a $[6,3,4]$-code over $\mathbb{F}_5$. The code f_6 is a self-dual code and its generator matrix is

$$\begin{pmatrix} 1 & -1 & 2 & 2 & 0 & 0 \\ 0 & 0 & 1 & -1 & 2 & 2 \\ 2 & 2 & 0 & 0 & 1 & -1 \end{pmatrix}, \tag{3.8}$$

(See e.g. [LPS82, p. 183]) The Lee weight enumerator of f_6 is as follows [LPS82, p. 183]

$$lw_{f_6}(x_0,x_1,x_2) = x_0^6 + 12x_0(x_1^5 + x_2^5) + 60x_0^2x_1^2x_2^2 + 40x_1^3x_2^3. \tag{3.9}$$

The *code* e_{10} is a $[10,4,4]$-code in $\mathbb{F}_5^{10}$. The code e_{10} is a self-dual code over $\mathbb{F}_5$. Its generator matrix is

$$\begin{pmatrix} 1 & 2 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 & 2 \end{pmatrix}. \tag{3.10}$$

(See e.g. [LPS82, p. 183]) The Lee weight enumerator of e_{10} is as follows [LPS82, p.187, Table II](In fact, [LPS82] gives the Lee weight enumerator as $\alpha^5 - 20\alpha^2\beta - 4\gamma$. So we calculated the Lee weight enumerator via that formula.)

$$\begin{aligned} &lw_{e_{10}}(x_0,x_1,x_2) \\ &= x^{10} + 36x^5y^5 - 4y^{10} + 120x^3y^6z + 360xy^7z^2 + 480x^4y^3z^3 + 1260x^2y^4z^4 + 36x^5z^5 \\ &\qquad + 360y^5z^5 + 120x^3yz^6 + 360xy^2z^7 - 4z^{10}. \quad (3.11) \end{aligned}$$

3.1.3. Algebraic independence

For the main theorems that we shall prove in this thesis we need the following proposition.

Proposition 3..1. *The Lee weight enumerators of the codes t_4 and g_{12} (defined in 3.1.1.) and the Lee weight enumerators of the codes c_2, f_6 and e_{10} (defined in 3.1.2.) are algebraically independent.*

Proof. We use the following criterion: Given polynomials $f_1,\ldots,f_n$ in n variables $x_1,\ldots,x_n$ are algebraically independent if and only if $\det\left(\frac{\partial f_i}{\partial x_j}\right)_{1\le i,j\le n} \neq 0$ (see [MS77, p. 610]).

We apply this to lw_{t_4} and $lw_{g_{12}}$. Let $f_1 := lw_{t_4}$ and $f_2 := lw_{g_{12}}$. Now, we calculate the Jacobi matrix J and then calculate the $\det(J)$ for these Lee weight enumerators.

$$J = \begin{pmatrix} \frac{\partial f_1}{\partial x_0} & \frac{\partial f_1}{\partial x_1} \\ \frac{\partial f_2}{\partial x_0} & \frac{\partial f_2}{\partial x_1} \end{pmatrix} = \begin{pmatrix} 4x_0^3 + 8x_1^3 & 24x_0x_1^2 \\ 12x_0^{11} + 1584x_0^5x_1^6 + 1320x_0^2x_1^9 & 1584x_0^6x_1^5 + 3960x_0^3x_1^8 + 288x_1^{11} \end{pmatrix},$$

$$\det(J) = -288x_0^{12}x_1^2 + 6336x_0^9x_1^5 - 9504x_0^6x_1^8 + 1152x_0^3x_1^{11} + 2304x_1^{14}.$$

The determinant is nonzero and hence lw_{t_4} and $lw_{g_{12}}$ are algebraically independent.

Next we apply the Jacobian criterion to the Lee weight enumerators $f_1 := lw_{c_2}$, $f_2 := lw_{f_6}$ and $f_3 := lw_{e_{10}}$ (which were given in the previous section). Let J be their Jacobi matrix. It suffice to show that $\det(J(1,1,2)) \neq 0$ (since this implies $\det(J) \neq 0$). We have

$$J(x_0,x_1,x_2)=\begin{pmatrix}\frac{\partial f_1}{\partial x_0} & \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2}\\ \frac{\partial f_2}{\partial x_0} & \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2}\\ \frac{\partial f_3}{\partial x_0} & \frac{\partial f_3}{\partial x_1} & \frac{\partial f_3}{\partial x_2}\end{pmatrix},$$

and hence

$$J(1,1,2)=\begin{pmatrix}2 & 8 & 4\\ 882 & 1500 & 1680\\ 132910 & 261260 & 243160\end{pmatrix},$$

so that

$$\begin{aligned}&\det(J(1,1,2))=\\ &2(364740000-438916800)-8(214467120-223288800)\\ &\qquad\qquad +4(230431320-199365000)=46485120\neq 0.\end{aligned}$$

Thus, the Lee weight enumerators lw_{c_2}, lw_{f_6} and $lw_{e_{10}}$ are algebraically independent. □

Corollary 3..2. *Let R_3 denote the subring of $\mathbb{C}[x_0,x_1]$ generated by lw_{t_4} and $lw_{g_{12}}$, and let R_5 denote the subring of $\mathbb{C}[x_0,x_1,x_2]$ generated by lw_{c_2}, lw_{f_6} and $lw_{e_{10}}$. Then one has*

$$\begin{aligned}\dim R_3 &:= \sum_{n\geq 0}\dim(R_3)_n x^n = \frac{1}{(1-x^4)(1-x^{12})},\\ \dim R_5 &:= \sum_{n\geq 0}\dim(R_5)_n x^n = \frac{1}{(1-x^2)(1-x^6)(1-x^{10})}.\end{aligned}$$

Here $(R_3)_n$ and $(R_5)_n$ denote the subspaces of homogeneous polynomials of degree n, respectively.

Proof. For any given positive integers $a_1,\ldots,a_r$, one has

$$\begin{aligned}F_{a_1,\ldots,a_r} &:= \sum_{n\geq 0}\#\{(x_1,\ldots,x_r)\in\mathbb{Z}_{\geq 0} : a_1x_1+\cdots+a_rx_r=n\}x^n\\ &= \sum_{x_1,\ldots,x_r\geq 0} x^{a_1x_1+\cdots+a_rx_r} = \frac{1}{(1-x^{a_1})\cdots(1-x^{a_r})}.\end{aligned}$$

From the preceding proposition we know that one can take as basis for $(R_3)_n$ the polynomials $lw_{t_4}^a lw_{g_{12}}^b$ where (a,b) runs through all pairs of non-negative integers such that $4a+12b=n$. Therefore $\dim R_3 = F_{4,12}$, which proves the first identity.

Similarly, a basis for $(R_5)_n$ is given by the polynomials $lw_{c_2}^a lw_{f_6}^b lw_{e_{10}}^c$, where a,b,c are non-negative integers such that $2a+6b+10c=n$. It follows $\dim R_5 = F_{2,6,10}$, which is the second identity. □

3.2. WEIL REPRESENTATIONS OF THE QUADRATIC MODULES $\mathbb{F}_P$

Definition 3..3. Let G be a group, and X is a set. A group (left) action on the set G is the mapping $\varphi : G \times X \mapsto X, (h,y) \mapsto hy$, which holds the following two properties :

1. e is the identity : $e(y) = y$ for $y \in X$,
2. for every t_1, t_2 in G, $(t_1 t_2)(y) = t_1(t_2 y)$.

Theorem 3..4 ([Con08])**.** *Let G act on X. If $x \in X$, $g \in G$, and $y = gx$, then $x = g^{-1}y$. If $x \neq x'$, then $g.x \neq g.x'$.*

Proof. We follow [Con08] If $y = gx$ for $g \in G$ and $x \in X$, then we get

$$g^{-1}.y = g^{-1}.(gx) = (g^{-1}g).x = ex = x.$$

Now, we prove the second part of the theorem via contradiction: Suppose $gx = gx'$. Then we get

$$g^{-1}.(gx) = g^{-1}.(gx') \implies (g^{-1}g).x = (g^{-1}g).x' \implies x = x'.$$

It shows that $x \neq x' \implies gx \neq gx'$. □

Definition 3..5. If for an action $\varphi : G \times X \mapsto X$, $h \in G$, $\forall y \in X$ $hy = y$ implies that $h = e$ then the action is called faithful.

Definition 3..6. A group of matrices $SL(2,\mathbb{R})$ is defined by

$$SL(2,\mathbb{R}) := \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | ad - bc = 1; a,b,c,d \in \mathbb{R} \}.$$

$SL(2,\mathbb{R})$ acts on $\tilde{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ in the following way :
If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL(2,\mathbb{R})$, and $z \in \tilde{\mathbb{C}}$, then an action is defined by

$$g.z := \frac{az+b}{cz+d}.$$

If $z = x+iy$, and we put z in the formula gz, then we have that with some basic calculation :

$$Im(gz) = \frac{Im(z)}{|cz+d|^2}.$$

This shows that H is constant under the action of $SL(2,\mathbb{R})$. Note that the element

$$-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

of $SL(2,\mathbb{R})$ acts trivially on H (see [Ser77, p. 77]).

Definition 3..7. A projective special linear group $PSL(2,\mathbb{R})$ is defined by $PSL(2,\mathbb{R}) := SL(2,\mathbb{R})/\{+I\}$ which acts faithfully on H (see [Ser77, p. 77]).

Definition 3..8. The group $G = SL(2,\mathbb{Z})/\{\pm 1\}$ is called the modular group; it is image of $SL(2,\mathbb{Z})$ in $PSL(2,\mathbb{R})$ (see [Ser77, p. 77]).

Proposition 3..9 ([FHhP03, p. 147])**.** *The action of the modular group*

$$G = SL(2,F) = \{ \begin{pmatrix} k & l \\ m & n \end{pmatrix} | kn - lm = 1; k,l,m,n \in F \}$$

on $F \times F$ is faithful action, where F is a finite field $\mathbb{F}_p$.

Proof. Let $h \in H$ and suppose $h.t = t$ for all $t \in \mathbb{F}^2$. Choosing $t = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $t = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ yields h.

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

whence $h = 1$. □

Theorem 3..10 ([Con10]). *The group $H = SL(2,\mathbb{Z})$ is generated by the operators S and T*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Remark 3..11. $S^2 = -I$, and then S has 4 matrices such that

$$S = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \}.$$

$$T^r = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}, \text{where} \quad r \in \mathbb{Z}.$$

$$ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, (ST)^3 = -I, \quad \text{then} \quad (ST)^6 = I.$$

Proof. We follow [Con10].

Pick any arbitrary element $\gamma = \begin{pmatrix} k & l \\ m & n \end{pmatrix}$ in $SL(2,\mathbb{Z})$. Then it follows :

$$S\gamma = \begin{pmatrix} -m & -n \\ k & l \end{pmatrix}, \quad T^r\gamma = \begin{pmatrix} k+rm & l+rn \\ m & n \end{pmatrix} (for \quad r \in \mathbb{Z}). \tag{3.12}$$

Suppose $m \neq 0$. If $|k| \geq |m|$, then m divides k. i.e., $k = m.p + s$ with $0 \leq s < |m|$. By the equation 3.12, $T^{-p}\gamma$ has upper left entry $k - mp = s$, which is smaller in absolute value than the lower left entry m in $T^{-p}\gamma$. Then, applying S with multiplication of $T^{-p}\gamma$ on the left, such that

$$ST^{-p}\gamma = \begin{pmatrix} -m & -n \\ s & l-pn \end{pmatrix}.$$

Consequently, multiplication of γ on the left by enough copies of S and powers of T gives a matrix in H with left lower entry 0. It has the form $\begin{pmatrix} \pm 1 & j \\ 0 & \pm 1 \end{pmatrix}$ for some $j \in \mathbb{Z}$. This matrix is T^j or T^{-j}, so there is some $h \in H$ such that $h\gamma = \pm T^r$ $(r \in \mathbb{Z})$. Thus, we have $\gamma = h^{-1}T^r$ in

H, since $T^r \in H, \quad S^2 = -I$. So, theorem is obvious. □

Theorem 3..12 ([Con10]). *The group $G = SL(2,\mathbb{F}_p)$ is generated by*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \mathbb{F}_p. \tag{3.13}$$

Proof. This follows from the preceding theorem and the fact that the natural reduction modulo p defines a homomorphism of groups $SL(2,\mathbb{Z}) \to SL(2,\mathbb{F}_p)$. □

Remark 3..13. Let U be a transpose matrix of the operator matrix T, i.e., $U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and the operator matrix $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ generate to the operator $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, such that $S = T^{-1}UT^{-1}$.

Example 3..14. Let $A = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$ in $G = SL(2,\mathbb{F}_7)$.A is expressed by the linear operators S and T.

Since $5 = 3.2 + (-1)$, then we have

$$T^{-2}\mathscr{A} = \begin{pmatrix} -1 & -1 \\ 3 & 2 \end{pmatrix}.$$

Now, we want to switch the roles of -1 and 3. Then left multiplication of S

$$ST^{-2}\mathscr{A} = \begin{pmatrix} -3 & -2 \\ -1 & -1 \end{pmatrix}.$$

Since $-3 = (-1).(3) + 0$, and then

$$T^{-3}ST^{-2}\mathscr{A} = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Thus, we have

$$ST^{-3}ST^{-2}A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad = T.$$

Hence, $A = T^2ST^3ST$, where $S^{-1} = S$.

Definition 3..15. Let G be a group and G acts on a set X. For, $\theta \in X$, its orbit is

$$Orb_\theta := \{h\theta | h \in G\}, \tag{3.14}$$

and its stabilizer is

$$Stab_\theta := \{h \in G | h.\theta = \theta\}. \tag{3.15}$$

Theorem 3..16. *Assume that G is finite group and X is the finite set. Then, for $\theta \in X$ $|G| := |Orb_\theta|.|Stab_\theta|$.*

Example 3..17. Let $G = SL(2,\mathbb{F}_p)$, and the group G acts on the set $\gamma = \mathbb{F}_p \times \mathbb{F}_p = \{\binom{x}{y} | x,y \in \mathbb{F}_p\}$. Then $|\gamma| = p^2$. Firstly, we should calculate $|Orb_\gamma|$ and $|Stab_\gamma|$. Let $h = \{\binom{m\ r}{s\ t} | mt - rs = 1, m,r,s,t \in \mathbb{F}_p\} \in G$.

$$\begin{pmatrix} m & r \\ s & t \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} mx+ry \\ sx+ty \end{pmatrix} \in Orb_\gamma \subset \gamma \tag{3.16}$$

We know that $mt - tr = 1$ so the equation 3.16 shouldn't be $\binom{0}{0}$. Thus, $|Orb_\gamma| = p^2 - 1 = (p-1)(p+1)$. Now, we calculate the order of $Stab_\gamma$ so the equation 3.16 must be equal to γ due to the definition 3..15. Then, we have

$$\left.\begin{aligned} px+ry = x \\ sx+ty = y \end{aligned}\right\} \quad \text{that implies} \quad ry = x(t-1) \quad \text{then} \quad t = 1, r = 0. \tag{3.17}$$

Thus, $Stab_\gamma = \{\binom{1\ 0}{s\ 1} | s \in \mathbb{F}_p\}$. Thus, $|Stab_\gamma| = p$. Hence, from the theorem 3..16, we have

$$|G| = p(p^2-1) = (p-1)p(p+1). \tag{3.18}$$

Example 3..18. Since the example 3..17

1. $|SL(2,\mathbb{F}_3)| = 3.(3-1)(3+1)3.2.4 = 24$
2. $|SL(2,\mathbb{F}_5)| = 5.(5-1)(5+1) = 120$
3. $|SL(2,\mathbb{F}_7)| = 7.(7-1)(7+1) = 336$

3.3. REPRESENTATION OF GROUPS

Definition 3..19. Let G be a finite group, and let V be an n-dimensional finite vector space over the complex field $\mathbb{C}$. A representation of G is a homomorphism from G in to $GL(V)$. i.e.

$$\rho : G \mapsto GL(V), \rho(g)(v) := \rho_g v \quad (g \in G, v \in V).$$

Here, $GL(V)$ is the general linear group of V.

Definition 3..20. If the representation $\rho(h)$ is unitary for each $h \in G$, then we call it an unitary representation. i.e.,$(\rho(h)w_1, \rho(h)w_2) = (w_1, w_2)$ for all $w_1, w_2 \in W$, where W is a finite dimensional complex Hilbert space with inner product $(,)$. So, the group G acts on W unitarily.

Definition 3..21. Let G be a finite group. A G-module is a vector space V together with an operation from $G \times V$ to V of G on V such that for each $g \in G$, $v \in V$, the map $v \mapsto gv$ is linear.

Remark 3..22. Let W be a $G-module$. A subspace U of W is called G-invariant subspace of W or G-submodule, if $hU \subseteq U, h \in G$.

Definition 3..23. The representation $\rho : G \mapsto GL(W), \rho(h)w = hw$ or G-module W is called irreducible if there is no proper non-zero G-invariant subspace of W.

Theorem 3..24 ([FW91, p. 6])**.** *If W is a subrepresentation of a representation V of a finite group G, then there is a complementary invariant subspace W' of V, so that $V = W \bigoplus W'$.*

Proof. We follow [FW91, p. 6]. Let W be a G-submodule of V. Take a complement of W and denote it by U. Then, $V = W \oplus U$. Define the projection $\pi_0 : V \mapsto W, \quad (w,u) \mapsto u$. Now, define $\pi : V \mapsto W$ by

$$\pi := \frac{1}{|G|} \sum_{g \in G} g(\pi_0 g^{-1}).$$

Then, we have

$$\pi(v) = \frac{1}{|G|} \sum_{g \in G} g(\pi_0 g^{-1}(v)).$$

We claim that $\pi(v)$ is also projection, i.e., $\pi^2(v) = \pi(v)$. We can easily show that

$$\pi^2(v) = \pi(\pi(v)) = \pi(\frac{1}{|G|}\sum_{g\in G} g(\pi_0 g^{-1})(v)) \text{which implies}$$
$$\pi^2(v) = \frac{1}{|G|^2}\sum_{g\in G}\sum_{g\in G} g(\pi_0(\pi_0(g_{-1}v)))$$
$$= \frac{1}{|G|}.|G|\pi(v) = \pi(v),$$

since cancellation rule. Thus $\pi(v)$ is a projection, and then $W = \pi(v)$. Now, we should show that $ker\pi$ is a $G-invariant$ subspace of V. Let $a,b \in ker\pi$. Then,

$$\pi(a) = \pi(b) = 0,$$

since π is a projection and then $\pi(a), \pi(b)$ in $ker\pi$.

$$\pi(a+b) = \pi(a) + \pi(b) = 0+0 = 0,$$

due to the homomorphism rule and so $\pi(a+b) \in ker\pi$. For $g \in G$, $\pi(gb) = \pi(0) = 0 \quad (b \in ker\pi)$ so $\pi(gb)$ in $ker\pi$. Thus, $ker\pi$ is a G-invariant subspace of V. Lastly, we must show that $ker\pi \cap W = \{0\}$: For any $v \in V$, we have $v = (1-\pi)(v) + \pi(v)$. Indeed,

$$\pi(1-\pi)(v) = (\pi - \pi^2)(v) = \pi(v) - \pi(v=0),$$
$$\text{then} \quad 1-\pi \in ker\pi \quad \text{and} \quad \pi(v) \in W.$$

If $v \in ker\pi \cap W$, then $\pi(v) = 0$ and for some $v' \in V, \quad v = \pi(v')$. So, $0 = \pi(v) = \pi^2(v) = \pi(v') = v$. Thus, $ker\pi \cap W = \{0\}$. Hence, $V = ker\pi \oplus W$, that means the complement $U = ker\pi$ of W. Therefore, W is a G - invariant submodule of V. □

Definition 3..25. Let $\rho_1 : G \mapsto GL(W_1)$ and $\rho_2 : G \mapsto GL(W_2)$ be two representations of a group G. A direct sum representation $\rho : G \mapsto GL(W_1 \oplus W_2)$ is defined as

$$\rho(k) := (\rho_1 \oplus \rho_2)(k) = \begin{pmatrix} \rho_1(k) & 0 \\ 0 & \rho_2(k) \end{pmatrix}, \quad \text{for all } k \in G. \tag{3.19}$$

3.3.1. Quadratic Form

Definition 3..26. Let V be a module. The map $(x,y) \mapsto x.y$ is a symetric bilinear form on V, called the scalar product associated with Q. One has $Q(x) = x.x$. This establishes a bijective correspondence between quadratic forms and symetric bilinear forms.

Definition 3..27. Let (W,Q) be quadratic form over $\mathbb{F}_p$. If $\theta.\omega = 0, \theta, \omega \in W$, then θ, ω are called orthogonal of W.

Definition 3..28. Let the polynomial ring $R = \mathbb{C}[\{x_a\}_{a\in\mathbb{F}_p}]$, and let the finite group $G = SL(2,\mathbb{F}_p)$ (for p odd prime). A finite quadratic module is a pair of $\underline{\mathbb{F}_p^n} = (\mathbb{F}_p^n, Q)$ consisting of a G-module $\mathbb{F}_p^n$, and non-degenerate quadratic form Q on $\mathbb{F}_p^n$, i.e. where $Q : \mathbb{F}_p^n \mapsto \mathbb{Q}/\mathbb{Z}$ is a map which satisfies the following properties :

- For all $a \in R$ and $x \in \mathbb{F}_p^n$ one has $Q(ax) := a^2 Q(x)$.

- The bilinear form corresponding to Q, is the map $B : \mathbb{F}_p^n \times \mathbb{F}_p^n \mapsto \mathbb{Q}/\mathbb{Z}$ defined as $B(x,y) := Q(x+y) - Q(x) - Q(y)$.

- $B(x,\mathbb{F}_p^n) = \{0\}$, if and only if $x = 0$. Then B is called non-degenerate.

For all odd prime p.

Definition 3..29. Let U_i $(1 \leq i \leq m)$ be subspaces of the vector space W. If every pair of U_i is orthogonal, then the orthogonal direct sum of U_i equals to W, i.e.

$$W = U_1 \hat{\oplus} \cdots \hat{\oplus} U_m.$$

Definition 3..30. An element x of a quadratic module (V,Q) is called isotropic if $Q(x) = 0$. A subspace U of V is called isotropic if all its elements are isotropic. Such that

$$U \quad isotropic \leftrightarrow U \subset U^0 \leftrightarrow Q|U = o$$

(see [Ser77]).

Definition 3..31. An $SL(2,\mathbb{F}_p)$-submodule U of $\underline{\mathbb{F}_p^n} = (\mathbb{F}_p^n, Q)$ is called isotropic if Q vanishes on U, i.e., $Q|U = 0$.

Example 3..32. We have two examples:

- The self-dual tetra code t_4 over $\mathbb{F}_3$ is a maximal isotropic subgroup in the finite quadratic module $\underline{\mathbb{F}_3^4} = (\mathbb{F}_3^4, (x_1^2 + x_2^2 + x_3^2 + x_4^2)/3)$.
- The self-dual code c_2 over $\mathbb{F}_5$ is a maximal isotropic subgroup in the finite quadratic module $\underline{\mathbb{F}_5^2} = (\mathbb{F}_5^2, (x_1^2 + x_2^2)/5)$.

Definition 3..33. A quadratic module having a basis formed of two isotropic elements x, y such that $x.y \neq 0$ is called hyperbolic plane (see [Ser73, p. 29]).

Example 3..34. If $k.t = 1$, the quadratic form is the matrix form such that $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} k \\ t \end{pmatrix}$; $\det(Q) = -1$. So it is non degenerate.

Definition 3..35. A basis $(e_1, \cdots, e_m)$ of quadratic module (W, Q) is called orthogonal if its elements are pairwise orthogonal,i.e. $W = ke_1 \hat{\oplus} + \cdots + \hat{\oplus} ke_m$. The matrix of Q with respect to this basis is a diagonal matrix :

$$\begin{pmatrix} k_1 & 0 & \dots & 0 \\ 0 & k_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & k_m \end{pmatrix}.$$

If $x = \sum x_i e_i$, then we have the quadratic form $Q(x) = k_1 x_1^2 + \cdots + k_m x_m^2$.

3.3.2. Weil Representations of $SL(2,\mathbb{F}_p)$

Fix an odd prime $p \neq 2$. For the following we fix a nontrivial character of the additive group of the field $\mathbb{F}_p$. One can take for χ for example the map

$$e_p : a \mapsto e^{2\pi i x/p},$$

where x is any preimage under the unique nontrivial ring homomorphism $\mathbb{Z} \to \mathbb{F}_p$. We shall also need

$$\sigma(\mathbb{F}_p) := \frac{1}{\sqrt{p}} \sum_{a \in \mathbb{F}_p} \chi\left(\frac{-a^2}{2}\right). \tag{3.20}$$

The usual formulas for Gauss sums yield for $\chi = e_p$ the following.

Proposition 3..36 ([Wei03, p. 1166])**.** *For $\chi = e_p$, one has*

$$\sigma(\mathbb{F}_p) = \left(\tfrac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4, \\ i & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

Remark 3..37. The action of $\mathrm{SL}(2,\mathbb{F}_p)$ on the space H of linear forms in $\mathbb{C}[\{x_a\}_{a\in\mathbb{F}_p}]$:

$$\begin{aligned} Tx_a &:= \psi(a)x_a = \chi(a^2/2)x_a, \\ Sx_a &:= \frac{\sigma(\mathbb{F}_p)}{\sqrt{(p)}} \sum_{b\in\mathbb{F}_p} \chi(-ab)x_b, \end{aligned}$$

where $\psi(a)^2 = \chi(a^2)$ then $\psi(a) = \psi(a^2/2)$.

Theorem 3..38 ([BS16, p. 56])**.** *For any odd prime p, the formulas*

$$\rho(A)\,x_u = \begin{cases} \left(\frac{c}{p}\right)\frac{\sigma(\mathbb{F}_p)}{\sqrt{p}} \sum_{v\in\mathbb{F}_p} \chi\left(\frac{av^2-2uv+du^2}{2c}\right) x_v & \text{if } c \neq 0, \\ \left(\frac{d}{p}\right)\chi\left(\frac{bd}{2}u^2\right)\, x_{du} & \text{if } c = 0, \end{cases} \qquad \left(A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}(2,\mathbb{F}_p)\right)$$

define a representation $\rho : \mathrm{SL}(2,\mathbb{F}_p) \to \mathrm{GL}(\mathbb{C}[H])$. Here H denotes the space of homogenuous linear polynomials in $\mathbb{C}[\{x_a\}_{a\in\mathbb{F}_p}]$.

Remark 3..39. The *Weil representations* ρ is naturally extended to the whole polynomial ring $R = \mathbb{C}[\{x_a\}_{a\in\mathbb{F}_p}]$, which becomes thus a graded $SL(2,\mathbb{F}_p)$-module.

The map $l : x_a \mapsto x_{-a}$, $(a \in \mathbb{F}_p)$ obviously intertwines with the action of $\mathrm{SL}(2,\mathbb{F}_p)$ on H, and hence the $+1$ and -1 eigenspaces H^+ and H^- of l are invariant under $\mathrm{SL}(2,\mathbb{F}_p)$ and define representations $\rho^\pm : \mathrm{SL}(2,\mathbb{F}_p) \to \mathrm{GL}(H^\pm)$.

We are interested in the representation ρ^+. A basis for H^+ is given by $y_a := \frac{1}{2}(x_a + x_{-a})$

$(0 \leq a \leq \frac{p-1}{2})$[1]). From the last theorem we therefore obtain the following.

Theorem 3..40 ([BS16, p. 65, Thm. 14.2])**.** *For any prime $p \neq 2$, the group $\mathrm{SL}(2,\mathbb{F}_p)$ acts on the space of linear forms in $\mathbb{C}[y_0, y_1, \cdots, y_{\frac{p-1}{2}}]$ via*

$$\rho^+\left(\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]\right) y_h = \begin{cases} (\frac{c}{p})\frac{\sigma(\mathbb{F}_p)}{\sqrt{p}} \sum_{0 \leq j \leq \frac{p-1}{2}} \delta_j \chi(\frac{aj^2-2hj+dh^2}{2c}) y_j & if \quad c \neq 0 \\ (\frac{d}{p})\chi(\frac{bd}{2}h^2)\, y_{dh} & if \quad c = 0 \end{cases}$$

Here $\delta_j = 2$ for $j \neq 0$ and $\delta_0 = 1$.

Proof. From Theorem 3..38 we have for $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ with $c \neq 0$

$$\begin{aligned} \rho^+(A)y_h &= \rho(A)\tfrac{1}{2}(x_h + x_{-h}) = \rho(A)\tfrac{1}{2}(x_h) + \rho(A)\tfrac{1}{2}(x_{-h}) \\ &= \left(\frac{c}{p}\right)\frac{\sigma(\mathbb{F}_p)}{\sqrt{p}} \sum_{v \in \mathbb{F}_p} \frac{1}{2}\chi(\frac{av^2-2hv+dh^2}{2c})\, x_v \\ &+ \left(\frac{c}{p}\right)\frac{\sigma(\mathbb{F}_p)}{\sqrt{p}} \sum_{v \in \mathbb{F}_p} \frac{1}{2}\chi(\frac{av^2+2vh+dh^2}{2c})\, x_v \\ &= (\frac{c}{p})\frac{\sigma(\mathbb{F}_p)}{\sqrt{p}} \sum_{v \in \mathbb{F}_p} \sum_{\mathbb{F}_p} (\chi(\frac{av^2-2hv+dh^2}{2c}) + \chi(\frac{av^2+2vh+dh^2}{2c}))(x_h + x_{-h}), \end{aligned}$$

since homomorphism. Thus we have for $c \neq 0$

$$\rho^+(A)y_h = (\frac{c}{p})\frac{\sigma(\mathbb{F}_p)}{\sqrt{p}} \sum_{j=0}^{\frac{p-1}{2}} \delta_j \chi(\frac{aj^2-2hj+dh^2}{2c}) x_j, \text{for} \quad \delta_0 = 1, \delta_j = 2 (j \neq o).$$

If $c = 0$, the formula

$$\begin{aligned} \rho^+(A)y_h &= \rho(A)\frac{1}{2}(x_h + x_{-h}) = \rho(A)\frac{1}{2}x_h + \rho(A)\frac{1}{2}x_{-h} \\ &= \frac{1}{2}(\frac{d}{p})\chi(\frac{bd}{2c}h^2)x_{dh} + \frac{1}{2}(\frac{d}{p})\chi(\frac{bd}{2c}h^2)x_{-dh} \\ &= (\frac{d}{p})\chi(\frac{bd}{2c}h^2)(x_{dh} + x_{-dh}), \end{aligned}$$

since homomorphism. Thus we have

$$\rho^+(A)y_h = (\frac{d}{p})\chi(\frac{bd}{2c}h^2)y_{dh}.$$

[1] For convenience we sometimes identify elements of $\mathbb{F}_p$ with their preimages $0 \leq j < p$ under the nontrivial homomorphism $\mathbb{Z} \to \mathbb{F}_p$. It should be always clear form the context whether a is an integer or an element of $\mathbb{F}_p$.

□

As before we continue the action of $\mathrm{SL}(2,\mathbb{F}_p)$ on the linear forms in the y_a to the polynomial ring in the variables y_a by

$$(A,f) \mapsto f(A.y_0,\cdots,A.y_{\frac{p-1}{2}}),$$

where we used $A.y_a$ for $\rho^+(A)y_a$.

3.3.3. Invariant Theory

Definition 3..41. An invariant of $\mathscr{G}$ is a polynomial $f(x)$, which is unchanged by every linear transformation in $\mathscr{G}$. In other word, the polynomial $f(x)$ is invariant of $\mathscr{G}$ if

$$A_\alpha o f(x) := f(A_\alpha.x) = f(x) \quad \text{for} \quad \alpha = 1,2,\cdots,g.$$

Definition 3..42 ([BS16, p. 67])**.** Let G be a finite group acting on the space of linear forms in the ring $R = \mathbb{C}[x_1,\cdots,x_n]$ of polynomials in n variables with complex coefficients F. This action on R by setting $(g\cdot F)(x_1,x_2,\cdots,x_n) = F(gx_1,\cdots,gx_n)$. If $g\cdot F = F$ for all $g \in G$. Then the subring R^G of the polynomials F is called invariant under G, it is denoted R^G, is defined as

$$R^G := \sum_{d\geq 0} R_d^G,$$

where R_d is the space of homogeneous polynomials of degree d.

Remark 3..43. An action of $G_{\mathbb{F}_p,\psi}$ on H by setting for A in $G_{\mathbb{F}_p,\psi}$ and a polynomial f defines that

$$(A.f)(\{x_a\}) := f(A.x_a\}). \tag{3.21}$$

3.4. SELF-DUAL CODES AND WEIL REPRESENTATIONS

3.4.1. Mac Williams' Identity

Mac Williams' identity theorem is playing important role in Coding theory, which implies that a weight enumerator of the dual code $C^{\perp}$ is determined by the given weight enumerator of the code C. It was discovered by Jessie C. Macwilliams, and it expresses the usual weight enumerator of a dual code in terms of the enumerator of the given code.

Theorem 3..44 ([BS16, p. 55, Thm. 12.1]). *For any linear code C over $\mathbb{F}_p$ of length n, one has*

$$Slw_C := \frac{\sigma(\mathbb{F}_p)^n|C|}{\sqrt{p^n}} lw_{C^{\perp}}. \tag{3.22}$$

Proof. One has

$$\begin{aligned} Slw_C &= lw_C(\{Sx_u : u \in \mathbb{F}_p\}) \\ &= lw_C(\{\frac{\sigma(\mathbb{F}_p)}{\sqrt{p}} \sum_{v\in\mathbb{F}_p} \chi(-uv)x_v\}_{u\in\mathbb{F}_p}) \\ &= (\frac{\sigma(\mathbb{F}_p)}{\sqrt{p}})^n \sum_{c\in C} \sum_{w\in\mathbb{F}_p} \chi(-c.w)x_{w_1}x_{w_2}\cdots x_{w_n} \end{aligned}$$

If $\chi(-c.w) = \chi(0) = 1$, then we have

$$\begin{aligned} Slw_C &= (\frac{\sigma(\mathbb{F}_p)}{\sqrt{p}})^n \sum_{c\in C} 1 \sum_{w=w_1\cdots w_n\in\mathbb{F}_p} x_{w_1}\cdots x_{w_n} \\ &= (\frac{\sigma(\mathbb{F}_p)}{\sqrt{p}})^n |C| lw_{C^{\perp}} \end{aligned}$$

by the definition of the Lee weight enumerator. Since the dual code $C^{\perp}$ is the subspace of the words $w = w_1w_2\cdots w_n$ in $\mathbb{F}_p^n$ such that $c\cdot w = \sum_{i=1}^n c_iw_i = o$ for $c \in C$. □

Remark 3..45. The previous theorem is given for the complete weight enumerator in [BS16, p. 55, Thm. 12.1].

Theorem 3..46 ((Mac Williams'Identity)[BS16, p. 55, Thm. 12.2]). *For any code of length n over a finite field $\mathbb{F}_p$, one has*

$$w_{C^{\perp}} := |C|^{-1} w_C(\frac{1-x}{1+(p-1)x})(1+(p-1)x)^n. \tag{3.23}$$

Proof. We follow [BS16, p. 55].

Set $x_0 = 1$ and $x_b = x \quad (b \in \mathbb{F}_q)$, then the sum

$$\sum_{b\in\mathbb{F}_q} \chi(-ab)x_b = \begin{cases} 1-x, & if \quad a \neq 0, \\ 1+(p-1)x, & if \quad a = 0 \end{cases}$$

Since the Proposition **??**. The homogeneous Hamming (usual) weight enumerator is that

$$w_C(x_o, x_1) = \sum_{c\in C} x_0^{n-h(c)} x_1^{h(c)}.$$

If x_0 replace by $1+(p-1)x$, and x_1 replace by $1-x$ then the usual weight enumerate formula is that

$$w_C(x) = \sum_{c\in C} (1+(p-1)x)^{n-h(c)}(1-x)^{h(c)}.$$

Now, if we put it in the equation Slw_c 3.22, then we have

$$Slw_c(x_0//1, x_b//x(b \in \mathbb{F}_{\frac{p-1}{2}})) = \frac{\sigma(\mathbb{F})^n}{\sqrt{p^n}} \sum_{c\in C} (1+(1-p)x)^{n-h(c)}(1-x)^{h(c)}.$$

From the theorem 3..44 therefore

$$\frac{\sigma(F)^n}{\sqrt{p^n}}|C|.lw_{C^\perp} = \frac{\sigma(F)^n}{\sqrt{p^n}} lw_C(1+(p-1)x, 1-x)$$
$$\text{which implies} \quad lw_{C^\perp} = |C|^{-1} lw_C(1+(p-1)x, 1-x),$$

where lw_C is a homogeneous Lee weight enumerator. Hence, for the usual weight enumerator w_C Mac Williams' theorem

$$w_{C^\perp} = |C|^{-1} w_C(\frac{1-x}{1+(p-1)x})(1+(p-1)x)^n,$$

due to the Proposition 2..30. □

Example 3..47. If $\mathbb{F}_p = \mathbb{F}_2$, then $w_{C^\perp}$ is

$$w_{C^\perp}(x_0, x_1) = \frac{1}{\sqrt{p}} W_C(x_0 + (1-p)x_1, x_0 - x_1). \tag{3.24}$$

Since $|C|.|C^{\perp}| = |\mathbb{F}_p^n| = q^n$ from the proposition 2..41 and from the Definition 2..42 $|C| = |C^{\perp}|$, thus we have $p^{n/2}.p^{n/2} = p^n$, that means $|C|^{-1} = 1/p^{n/2}$.

Remark 3..48. Let $w(x_0,x_1)$ be a weight enumerator of the self-dual code $C^{\perp}$ over $\mathbb{F}_p$, such that

$$w(x_0,x_1) = \frac{1}{\sqrt{p}} w(x_0+(p-1)x_1, x_0-x_1). \tag{3.25}$$

The problem is to find all polynomials $w(x_0,x_1)$. We solves that kind of problems via invariant theory, which means $w(x_0,x_1)$ is unchanged, or invariant under the linear transformation

$$T : replace \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \quad by \quad C \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}, \tag{3.26}$$

where

$$C = \frac{1}{\sqrt{p}} \begin{pmatrix} 1 & p-1 \\ 1 & -1 \end{pmatrix}, \quad C^2 = I.$$

So, $w(x,y)$ must be invariant under the group G consisting of the two matrices I, and A, which means that the order of the group G is 2. i.e. $|G| = 2$.
From the Equation 3.25, the weight enumerator of the self-dual code of C is :

$$\begin{aligned} w_{C^{\perp}}(x_0,x_1) &= w_C(\frac{x_0+x_1}{\sqrt{2}}, \frac{x_0-x_1}{\sqrt{2}}) \\ &= \frac{1}{\sqrt{2}} w_C((x_0,x_1) \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}), \quad \text{for} \quad \mathbb{F}_q = \mathbb{F}_2. \end{aligned}$$

Example 3..49. For binary Golay code and Hamming code, we find the weight enumerators of their dual codes.

1. For $[23,11,7]_2$-Golay code:

$$\begin{aligned} w_{G_{23}^{\perp}} &= 2^{-12} w_{G_{23}}(\frac{1-x}{1+x})(1+x)^{23} \\ &= 253x^{16} + 1288x^{12} + 506x^8 + 1. \end{aligned}$$

2. For $[7,4,3]_2$-Hamming code: First the weight enumerator of Hamming code:

$$w_{H_7} = 1+7x^3+7x^4+x^7, \quad \text{and for the self-dual of the Hemming code}$$
$$w_{H_7^\perp} = 2^{-4} w_{H_7}(\frac{1-x}{1+x})(1+x)^7 = 7x^4+1.$$

Theorem 3..50 ([BS16, p. 64, Thm. 14.1]). *For a linear code C of length n over the field $\mathbb{F}_p$ the following statements are equivalent :*

1. *The code C is self-dual,*
2. *The Lee weight enumerator lw_C satisfies $g.lw_C = lw_C$ for all $g \in G_{\mathbb{F}_p,\psi}$.*

Remark 3..51. The subring of polynomials in $R := \mathbb{C}[\{x_a\}_{a\in\mathbb{F}_p}]$ generated by the complete weight enumerators of self-dual codes is therefore equal to the subring $R^{\{SL(2,\mathbb{F}_p)\}}$ of the polynomials invariant under $SL(2,\mathbb{F}_p)$.

Proof of Theorem 3..50. We follow the proof in [BS16, p. 64]. If C is self dual code, i.e. $C = C^\perp$. Then theorem 3..44 implies

$$Slw_C = \frac{\sigma(\mathbb{F}_p)^n.|C|}{\sqrt{p^n}} lw_{C^\perp}. \tag{3.27}$$

But $\dim C = \dim C^\perp = n/2$ as follows from Proposition 2..41 and hence $|C| = p^{n/2}$. Moreover,

$$\begin{aligned}\sigma(\mathbb{F}_p)^n &= \frac{1}{\sqrt{|\mathbb{F}_p|^n}} \sum_{w=w_1,\cdots,w_n\in\mathbb{F}_p^n} \prod_{i=1}^n \psi(w_i)^{-1} \\ &= \frac{1}{\sqrt{p^n}} \sum_{w=w_1,\cdots,w_n\in C^\perp/C} \prod_{i=1}^n \chi(-w_i)\end{aligned}$$

If n is even and $\mathbb{F}_p^n$ contains a self-dual code then we have

$$\sigma(\mathbb{F}_p)^n = \frac{1}{\sqrt{p^n}}|C^\perp| = \frac{1}{\sqrt{p^n}} p^{n/2} = 1,$$

since $c\cdot c = 0$ for c in self-dual code $C^\perp$. Hence,

$$Slw_C = \frac{1\cdot|C|}{\sqrt{p^n}} lw_C = lw_C,$$

since C is self-dual or doubly even code.

Immediately from the definition of lw_C one finds that the application of T multiplies each term in

$$lw_C = \sum_{c=c_1\cdots c_n \in C} x_{c_1}\cdots x_{c_n} \in \mathbb{C}[y_0, y_1, \cdots, y_{\frac{p-1}{2}}],$$

where $y_0 = x_0$, and $y_i = x_i + x_{p-i}$ $(1 \leq i \leq \frac{p-1}{2})$, by $\psi(c_1)\cdots\psi(c_n)$. From this it follows that

$$Tlw_C = \prod_{i=1}^{n} \psi(c_i) \cdot lw_C = \prod_{i=1}^{n} \chi(c_i.c_i/2) lw_C,$$

which implies $Tlw_C = lw_C$, where for all $c = c_1c_2\cdots c_n$ in C, $c.c = 0$ since $C = C^{\perp}$ and so $\psi(c) = \chi(c.c/2) = \chi(0) = 1$. But $\psi(c_1)\psi(c_2)\cdots(c_n) = \chi(c\cdot c/2)$ for $p \neq 2$. For $p = 2$ we have

$$\psi(c_1)\psi(c_2)\cdots\psi(c_n) = \chi(c_1.c_1/2)\cdots\chi(c_n.c_n/2) = i^k,$$

where $k = h(c)$ which reduces again to 1 if C is doubly even. Since $\chi(0) = 1$, and $\chi(1) = e^{\frac{\pi\cdot i}{2}} = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2} = i$. If the code C is doubly even code for $p = 2$, then $i^k = 1$ if and only if $4|h(c)$. Thus, $Tcw_C = cw_c$ for doubly-even code C and self-dual code C are both. Vice versa, $Tlw_C = lw_C$ implies $c.c = 0$ for all codewords c and $p = 2$, even more $4|h(c)$. It follows by a standard argument that $C \subseteq C^{\perp}$. But $lw_C = Slw_C = \frac{\sigma(\mathbb{F}_1)^n|C|}{\sqrt{p^n}} lw_{C^{\perp}}$ implies $|C| = \frac{\sigma(\mathbb{F}_p)^n|C|}{\sqrt{p^n}}|C^{\perp}|$ (as follows on setting all variables in the preceding identity equal to 1), and hence $\dim C^{\perp} = \dim C = n/2$, which implies $C = C^{\perp}$ by the Proposition 2..41. □

Corollary 3..52. *The length of a self-dual code over $\mathbb{F}_p$ is even. If $p \equiv -1 \bmod 4$ the length is divisible by* 4.

Proof. If C is a self-dual code of length n, then $\dim C = \dim C^{\perp}$. But by Proposition 2..41 one has $n = \dim C + \dim C^{\perp}$. It follows that n is even.

Let w denote the Lee weight enumerator of C. By the preceding theorem and the equation (3.27) we have $\sigma(\mathbb{F}_p)^n = 1$. But for $p \equiv -1 \bmod 4$ and $\chi = e_p$ we have $\sigma(\mathbb{F}_p) = \pm i$ (see Proposition 3..36). It follows $1 = (\pm i)^n$, whence $4 \mid n$. □

3.5. MOLIEN SERIES

3.5.1. Molien's theorem

The theorem of the Molien series is the important to find the number of the linearly independent homogeneous invariants of the self-dual codes. We want to describe $R^{SL(2,\mathbb{F}_p)}$ by generators and relations via Molien series.

Definition 3..53. The Molien series M associated to the $G-module$ ring $R=\mathbb{C}[x_1,\cdots,x_n]$ is defined as

$$M := \dim R = \sum_{d\geq 0} \dim R_d t^n,$$

where R_d is the space of homogeneous polynomials of degree d.

Remark 3..54. The representation $\rho : G\times F \mapsto GL(R)$ is defined by $\rho(g).F = gF$, for all $g\in G$ (F is a set of polynomial functions).

Theorem 3..55 ([BS16, p. 67])**.** *One has*

$$M = \dim R = \sum_{d=0}^{\infty} R_d t^d$$

be the generating function for this sequence, then

$$M = \dim R = \frac{1}{|G|}\sum_{g\in G}\frac{1}{det(I-\rho(g)t)},$$

where $\rho(g)$ in $GL(R_1)$ defined by $\rho(g)F = g\cdot F$.

Proof. We follow the proof in [BS16, p.67, Thm 14.4.] Let G be a finite group acting on a finite dimensional vector space $V\cong\mathbb{C}^n$ via $\rho : G\mapsto GL(V)$. Let $x_1,\cdots,x_n$ be basis in the dual space V^* of V. Then the polynomial functions on V are the polynomial ring $R = \mathbb{C}[V] = \mathbb{C}[x_1,\cdots,x_n]$. Now G acts on R via $\rho : G\mapsto GL(R_d)$, where R_d is the space of the homogeneous polynomials of degree d. Let $\rho_d(g)$ denote the element of $GL(R_d)$ defined by $\rho(g)Fg\cdot F$. Let P_d denote the projection of R onto R_d defined by

$$P_d := \frac{1}{|G|}\sum_{g\in G}\rho_d(g).$$

The endomorphism P_d of R_d has image in R_d^G and equals to the identity on R_d. Hence the dimension of the subspace R_d^G is that

$$\dim R_d^G = \frac{1}{|G|}\sum_{g\in G} tr(\rho_d(g)).$$

The claimed identity follows now from

$$\sum_{d\leq 0} tr(\rho_d(g))t^d = \frac{1}{\det(1-\rho(g)t)},$$

which is valid for every g in G. □

Example 3..56. Consider the matrix group

$$S = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\} \subset GL(2,\mathbb{C}).$$

So $|S| = 4$. The Molien's series is calculated as :

$$det(I - S_1 t) = det(\begin{pmatrix} 1-t & 0 \\ 0 & 1-t \end{pmatrix}) = (1-t)^2,$$

$$det(I - S_2 t) = (\begin{pmatrix} 1+t & 0 \\ 0 & 1-t \end{pmatrix}) = 1-t^2,$$

$$det(I - S_3 t) = det(\begin{pmatrix} 1-t & 0 \\ 0 & 1+t \end{pmatrix}) = 1-t^2,$$

$$det(I - S_4 t) = det(\begin{pmatrix} 1+t & 0 \\ 0 & 1+t \end{pmatrix}) = (1+t)^2.$$

Thus, we have

$$\begin{aligned} M &= \frac{1}{4}(\frac{1}{(1-t)^2} + \frac{1}{(1-t^2)} + \frac{1}{(1-t^2)} + \frac{1}{(1+t)^2}) \\ &= \frac{1}{4}(\frac{4}{(1-t^2)(1-t^2)}) = \frac{1}{(1-t^2)^2} = 1 + 2t^2 + 3t^4 + ... \end{aligned}$$

Hence, there are two independent invariants of degree 2. Now, we calculate the $\rho(f)$, where

$f \in \mathbb{C}[x,y]$:

$$\rho(f) = \frac{1}{4}\{f(x,y)+f(-x,y)+f(x,-y)+f(-x,-y)\}.\text{Then, we have}$$
$$\rho(x^2) = \frac{1}{4}\{x^2+x^2+x^2+x^2\} = x^2,$$
$$\rho(y^2) = \frac{1}{4}\{y^2+y^2+y^2+y^2\} = y^2.$$

Thus, $\alpha = x^2, \beta = y^2$ in $\mathbb{C}[x,y]$ and they are algebraically independent. Hence, $\mathbb{C}^S = \mathbb{C}[\alpha,\beta]$.

3.5.2. The Molien series of the Weil representations for $p = 3,5$

Theorem 3..40 describes an action of $\mathrm{SL}(2,\mathbb{F}_p)$ on the space of linear homogeneous polynomial in $S_p := \mathbb{C}[x_0, x_1, \ldots x_{\frac{p-1}{2}}]$, which extends naturally to an action on the whole polynomial ring S_p. We know that every Lee weight enumerator of a self-dual code is contained in the ring of $\mathrm{SL}(2,\mathbb{F}_p)$-invariants in S_p. Moreover, by Corollary 3..52 any such Lee weight enumerator is homogeneous of even degree. In other words it is an invariant under the action of $\mu_2 = \{\pm 1\}$ on S_p given by $(s, f(x)) \mapsto f(-x)$ (where we use $x = x_0, x_1, \ldots x_{\frac{p-1}{2}}$). If $p \equiv -1 \bmod 4$ then the degree of any given Lee weight enumerator of a self-dual code is even more divisible by 4. Accordingly, any such Lee weight enumerator is invariant under the action of $\mu_4 = \{\pm 1, \pm i\}$ defined as before. Therefore we are interested in the invariants in S_p with respect to the action of $G_p := \mathrm{SL}(2,\mathbb{F}_p) \times \mu_2$ if $p \equiv +1 \bmod 4$,and $G_p := \mathrm{SL}(2,\mathbb{F}_p) \times \mu_4$ if $p \equiv -1 \bmod 4$.

For the following theorem recall that $\dim S_p^{G_p}$ denotes the subring of polynomials F in R_p which satisfy $g \cdot F = F$ for all $g \in G_p$, and that we use $\dim S_p^{G_p} = \sum_{n \geq 0} \dim(S_p)_n x^n$.

Theorem 3..57. *One has*

$$\dim \mathbb{C}[x_0,x_1]^{\mathrm{SL}(2,\mathbb{F}_3)\times\mu_4} = \frac{1}{(1-x^4)(1-x^{12})}$$
$$\dim \mathbb{C}[x_0,x_1,x_2]^{\mathrm{SL}(2,\mathbb{F}_5)\times\mu_2} = \frac{1}{(1-x^2)(1-x^6)(1-x^{10})}$$

Proof. We consider the case $p = 3$. From Proposition 3..40 we have for $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, $c \neq 0$,

$$\begin{aligned}(\rho^+(A)x_0, \rho^+(A)x_1) &= (x_0, x_1)(\frac{c}{3})\frac{\sigma(\mathbb{F}_3)}{\sqrt{3}}\left[\begin{smallmatrix} 1 & 2\chi(\frac{a}{2c}) \\ \chi(\frac{d}{2c}) & 2\chi(\frac{a+d-2}{2c}) \end{smallmatrix}\right] \\ &= (x_0, x_1)(\frac{c}{3})\frac{i}{\sqrt{3}}\left[\begin{smallmatrix} 1 & 2\chi(\frac{a}{2c}) \\ \chi(\frac{d}{2c}) & 2\chi(\frac{a+d-2}{2c}) \end{smallmatrix}\right],\end{aligned}$$

where $\sigma(\mathbb{F}_3) = \frac{1}{\sqrt{3}}\sum_{a\in\mathbb{F}_3}\chi(-a^2/2) = i$. The invariants in S_3 with respect to the action $G_3 := \mathrm{SL}(2,\mathbb{F}_3) \times \mu_4$ defined on the space of linear forms S_1 by $(g,F) = \rho^+(g)F$ with ρ^+ denoting the unique extension of $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \mapsto S$ and $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] \mapsto T$. Moreover, if we take $A = S = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ for the case $c \neq 0$, then $(\rho^+(A)x_0, \rho^+(A)x_1)$ implies that :

$$\alpha := \frac{i}{\sqrt{3}}\left[\begin{smallmatrix} 1 & 2 \\ 1 & -1 \end{smallmatrix}\right].$$

It follows

$$\begin{aligned}\det(I - \rho^+(A)x) &= \det(\left[\begin{smallmatrix} 1-(\frac{c}{3})\frac{i}{\sqrt{3}}x & -(\frac{c}{3})\frac{i}{\sqrt{3}}2\chi(\frac{a}{2c})x \\ -(\frac{c}{3})\frac{i}{\sqrt{3}}\chi(\frac{d}{2c})x & 1-(\frac{c}{3})\frac{i}{\sqrt{3}}2\chi(\frac{a+d-c}{2c})x \end{smallmatrix}\right]) \\ &= (1-(\frac{c}{3})\frac{i}{\sqrt{3}}x)(1-(\frac{c}{3})\frac{i}{\sqrt{3}}2\chi(\frac{a+d-2}{2c}x) + \frac{2}{3}\chi(\frac{d}{2c})\chi(\frac{a}{2c})x^2.\end{aligned}$$

Now, we compute $(\rho^+(A)x_0, \rho^+(A)x_1)$ for $c = 0$.

$$(\rho^+(A)x_0, \rho^+(A)x_1) = (x_0, x_1)\left[\begin{smallmatrix} (\frac{d}{3})\chi(0) & 0 \\ 0 & (\frac{d}{3})\chi(\frac{bd}{2}1^2) \end{smallmatrix}\right].$$

If we take $A = T = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ for case $c = 0$, then $(\rho^+(A)x_0, \rho^+(A)x_1$ implies that :

$$\beta := \left[\begin{smallmatrix} 1 & 0 \\ 0 & \zeta \end{smallmatrix}\right],$$

where $\zeta = e^{\frac{2\pi i}{3}}$. It follows

$$\begin{aligned}\det(I - \rho^+(A)x) &= \det(1 - \left[\begin{smallmatrix} (\frac{d}{3})x & 0 \\ 0 & (\frac{d}{3})\chi(\frac{bd}{2}) \end{smallmatrix}\right]) \\ &= (1-(\frac{d}{3})x)(1-(\frac{d}{3})\chi(\frac{bd}{2})x),\end{aligned}$$

where a, b, c, d in $\mathbb{F}_3$. Thus we have

$$G_3 = \mathrm{SL}(2,\mathbb{F}_3) \times \mu_4 := \langle \frac{i}{\sqrt{3}}\left[\begin{smallmatrix} 1 & 2 \\ 1 & -1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & \zeta \end{smallmatrix}\right]\rangle, \quad |G_3| = 24.$$

Now, we find $\dim \mathbb{C}[x_0,x_1]^{\mathrm{SL}(2,\mathbb{F}_3)\times\mu_4}$ via the Molien series formula. i.e.,

$$\dim \mathbb{C}[x_0,x_1]^{\mathrm{SL}(2,\mathbb{F}_3)\times\mu_4} = \frac{1}{24}\sum_{A\in \mathrm{SL}(2,\mathbb{F}_3)} \frac{1}{\det(I-\rho^+(A)x)}.$$

Thus from the Molien series we have

$$M = \dim \mathbb{C}[x_0,x_1]^{\mathrm{SL}(2,\mathbb{F}_3)\times\mu_4} = \frac{1}{(1-x^4)(1-x^{12})}.$$

Now, we consider the case $p=5$, which is used the similar way with case $p=3$. From the Proposition 3..40 we have for $A=\left[\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right], c\neq 0$. Before, we shall compute the $\sigma(\mathbb{F}_5)$. From the Equation 3.20 we have

$$\begin{aligned}\sigma(\mathbb{F}_5) &= \frac{1}{\sqrt{5}}\sum_{a\in\mathbb{F}_5}\chi(\frac{-a^2}{2}) \\ &= \frac{1}{\sqrt{5}}(1+2\zeta^2+2\zeta^4), \text{where} \quad \zeta = e^{2\pi i/5}.\end{aligned}$$

It follows

$$\begin{aligned}&(\rho^+(A)x_0,\rho^+(A)x_1,\rho^+(A)x_2) = \\ &((\frac{c}{5})\frac{\sigma(\mathbb{F}_5)}{\sqrt{5}}(x_0+2\chi(\frac{a}{2c}x_1+2\chi(\frac{2a}{c})x_2), \\ &(\frac{c}{5})\frac{\sigma(\mathbb{F}_5)}{\sqrt{5}}(\chi(\frac{d}{2c})x_0+2\chi(\frac{a+d-2}{2c})x_1+2\chi(\frac{4a+d-4}{2c})x_2), \\ &\qquad (\frac{c}{5})\frac{\sigma(\mathbb{F}_5)}{\sqrt{5}}(\chi(\frac{d}{c})x_0+2\chi(\frac{a+4d-4}{2c})x_1+2\chi(\frac{4a+4d-8}{2c})x_2)).\end{aligned}$$

Now, we compute the $(\rho^+(A)x_0,\rho^+(A)x_1,\rho^+(A)x_2)$ for case $c=0$ from Proposition 3..40.

$$\begin{aligned}(\rho^+(A)x_0,\rho^+(A)x_1,\rho^+(A)x_2) = ((\frac{d}{5})\chi(0)x_0, \\ (\frac{d}{5})\chi(\frac{bd}{2})(x_1), \\ (\frac{d}{5})\chi(2bd)(x_2),\end{aligned}$$

where a,b,c,d in $\mathbb{F}_5$ ($ad-bd=1$). The invariants in S_5 with respect to the action $G_5 := \mathrm{SL}(2,\mathbb{F}_5)\times\mu_2$ defined on the space of linear forms S_1 by $(g,F)=\rho^+(g)F$ with ρ^+ denoting the unique extension of $\left[\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right]\mapsto S$ and $\left[\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right]\mapsto T$. Moreover, if we take $A=S=\left[\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right]$ for

the case $c \neq 0$, then $(\rho^+(A)x_0, \rho^+(A)x_1, \rho^+(A)x_2$ implies that :

$$\alpha' := \frac{1}{5}\begin{pmatrix} 1 & 2 & 2 \\ 1 & \zeta+\zeta^4 & \zeta^2+\zeta^3 \\ 1 & \zeta^2+\zeta^3 & \zeta+\zeta^4 \end{pmatrix}.$$

Now, if we take $A = T = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ for case $c = 0$, then $(\rho^+(A)x_0, \rho^+(A)x_1, \rho^+(A)x_2)$ implies that :

$$\beta' := \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta & 0 \\ 0 & 0 & \zeta^4 \end{pmatrix},$$

where $\zeta = e^{\frac{2\pi i}{5}}$. Hence, we have

$$\begin{aligned} G_5 &= \mathrm{SL}(2,\mathbb{F}_5) \times \mu_2 = \langle \alpha', \beta' \rangle \\ &= \langle \frac{1}{5}\begin{pmatrix} 1 & 2 & 2 \\ 1 & \zeta+\zeta^4 & \zeta^2+\zeta^3 \\ 1 & \zeta^2+\zeta^3 & \zeta+\zeta^4 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta & 0 \\ 0 & 0 & \zeta^4 \end{pmatrix} \rangle, |G_5| = 120, \end{aligned}$$

where $\zeta = e^{\frac{2\pi i}{5}}$. It follows (for the case $c \neq 0$)

$$\det(1-\rho^+(A)x) = \det(I - (\frac{c}{5})\frac{\sigma(\mathbb{F}_5)}{\sqrt{5}}\begin{bmatrix} 1x & 2\chi(\frac{a}{2c})x & 2\chi(\frac{2a}{c})x \\ \chi(\frac{d}{2c})x & 2\chi(\frac{a+d-2}{2c})x & 2\chi(\frac{4a-d-4}{2c})x \\ \chi(\frac{d}{c})x & 2\chi(\frac{a+4d-4}{2c})x & 2\chi(\frac{4a+4d-8}{2c})x \end{bmatrix}),$$

and the case for $c = 0$

$$\det(1-\rho^+(A)x) = \det(I - (\frac{d}{5})\begin{bmatrix} 1x & 0 & 0 \\ 0 & \chi(\frac{bd}{2})x & 0 \\ 0 & 0 & \chi(2bd)x \end{bmatrix})$$

Now, we find $\dim \mathbb{C}[x_0,x_1,x_2]^{\mathrm{SL}(2,\mathbb{F}_5)\times\mu_2}$ via the Molien series formula. i.e.,

$$\begin{aligned}\dim \mathbb{C}[x_0,x_1,x_2]^{\mathrm{SL}(2,\mathbb{F}_5)\times\mu_2} &= \frac{1}{120}\sum_{A\in \mathrm{SL}(2,\mathbb{F}_5)} \frac{1}{\det(I-\rho^+(A)x)} \\ &= \frac{1}{(1-x^2)(1-x^6)(1-x^{10})}.\end{aligned}$$

□

4. PART IV: RESULTS

4.1. THE MAIN THEOREMS

In this last but not least section we state and prove the main theorems of this thesis. As explained in the introduction the two theorems of this section are well-known, however, we give here a new proof based purely on invariant theory following ideas of [BS16].

Theorem 4..1 (Broué, Enguehard [BS16, p. 65, Thm. 14.3])**.** *Every Lee weight enumerator of a ternary self-dual code can be written as a polynomial in the Lee weight enumerators of the two codes t_4 and g_{12} described in Section 3.1.1.. Such a writing can be done in only one way.*

Remark 4..2. Note that the Lee weight enumerators of codes over $\mathbb{F}_3$ are identical with the standard weight enumerators. So the prefix "Lee" can be omitted in the above theorem. We keep using it only for showing the consistency with the case of self-dual codes over $\mathbb{F}_5$ described below.

Proof of Theorem 4..1. Let A be the subring of $R = \mathbb{C}[x_0, x_1]$ generated by the Lee weight enumerators of t_4 and g_{12}, let B be the subring of R generated by the Lee weight enumerators of the self-dual codes over $\mathbb{F}_3$, and, finally, let C be the subring of all polynomials in R that are invariant under the action of the group $G := \mathrm{SL}(2, \mathbb{F}_3) \times \mu_4$ as introduced in Section 3.5.2.. We have

$$A \subseteq B \subseteq C.$$

Indeed, the first identity is obvious, whereas the second one follows from (the remark after) Theorem 3..50 and the fact that the length of a self-dual code over $\mathbb{F}_3$ is divisible by 4 (see Corollary 3..52). We need to show that $A = C$. This implies $A = B$, that is that every Lee weight enumerator of a self-dual code C over $\mathbb{F}_3$ is a polynomial in the Lee weight enumerators of t_4 and g_{12}. Since the Lee weight enumerators of the latter two codes are algebraically independent by Corollary 3..2 the representation of a Lee weight enumerator of a self-dual code over $\mathbb{F}_3$ as polynomial in lw_{t_4} and $lw_{g_{12}}$ is unique.

To show that $A = C$ it suffices to show for any non-negative integer n, that $\dim A_n = \dim C_n$ since we have already $A \subseteq C$, whence $A_n \subseteq C_n$. In other words we have to show that $\sum_{n\geq 0} A_n x^n = \sum_{n\geq 0} C_n x^n$. But the left hand side was computed in Corollary 3..2, and the right hand side in Theorem 3..57 which shows that we indeed have the equality. This proves the theorem. □

Theorem 4..3 (Gleason and Pierce; Sloane [Ebe02, p. 165, Cor. 5.5])**.** *Every Lee weight enumerator of a self-dual code over $\mathbb{F}_5$ can be written as a polynomial in the Klein invariants A, B, C.*

A proof of this theorem, using Hilbert modular forms and results of Klein on the symmetry group of the icosahedron, can also be found in [Ebe02, §5.6].

Theorem 4..4. *Every Lee weight enumerator of a self-dual code over $\mathbb{F}_5$ can be written as a polynomial in the weight enumerators of the three codes c_2, f_6 and e_{10} introduced in Section 3.1.2.. Such a writing can be done in only one way.*

Proof of Theorem 4..4. The proof follows the same strategy as the proof of the preceding theorem. For the reader who does wish to read it again, we repeat it here, with $p = 5$. Let A be the subring of $R = \mathbb{C}[x_0, x_1, x_2]$ generated by the Lee weight enumerators of c_2, f_6 and e_{10}, let B be the subring of R generated by the Lee weight enumerators of the self-dual codes over $\mathbb{F}_5$, and, finally, let C be the subring of all polynomials in R that are invariant under the action of the group $G := \mathrm{SL}(2, \mathbb{F}_5) \times \mu_2$ as introduced in Section 3.5.2.. We have

$$A \subseteq B \subseteq C.$$

Indeed, the first identity is obvious, whereas the second one follows from (the remark after) Theorem 3..50 and the fact that the length of a self-dual code over $\mathbb{F}_5$ is even (see Corollary 3..52). We need to show that $A = C$. This implies $A = B$, that is that every Lee weight enumerator of a self-dual code C over $\mathbb{F}_5$ is a polynomial in the Lee weight enumerators of c_2, f_6 and e_{10}. Since the Lee weight enumerators of the latter three codes are algebraically independent by Corollary 3..2 the representation of a Lee weight enumerator of a self-dual code over $\mathbb{F}_5$ as polynomial in lw_{c_2}, lw_{f_6} and $lw_{e_{10}}$ is unique.

To show that $A = C$ it suffices to show for any non-negative integer n, that $\dim A_n = \dim C_n$ since we have already $A \subseteq C$, whence $A_n \subseteq C_n$. In other words we have to show that

$\sum_{n\geq 0} A_n x^n = \sum_{n\geq 0} C_n x^n$. But the left hand side was computed in Corollary 3..2, and the right hand side in Theorem 3..57 which shows that we indeed have the equality. This proves the theorem. □

5. PART V: DISCUSSION

In this thesis, we studied on the self-dual codes over the prime fields $\mathbb{F}_3$ and $\mathbb{F}_5$, and the structure theorems for their Lee weight enumerators and also associated the Lee weight enumerators of those self-dual codes with the Weil representations of $\mathrm{SL}(2,\mathbb{Z})$.

The weight enumerators give us significant knowledge about Hamming weight, Hamming distance of the linear codes over the prime field $\mathbb{F}_p$. There are three weight enumerators in this area : Usual weight enumerator, complete weight enumerator and Lee weight enumerator. The Lee weight enumerator is much more useful for the linear codes over $\mathbb{F}_p$ (for $p \neq 2$) which are polynomial in the complex polynomial ring $\mathbb{C}[y_0,\cdots,y_{\frac{p-1}{2}}]$.

Earlier work about these structure theorems for the Lee weight enumerators of the self-dual codes over $\mathbb{F}_3$ and $\mathbb{F}_5$ was proven via geometrical methods. Instead of the Lee weight enumerators of the three codes over $\mathbb{F}_5$ one can also take the so-called Klein invariants, two of which are, however not weight enumerators of codes. These are interesting because of their connection to the icosahedron (see e.g. [Ebe02, §5.6]). In the literature the Klein invariants are, in fact, used instead of the above Lee weight enumerators.

We proved these two structure theorems for the Lee weight enumerators of the self-dual codes over $\mathbb{F}_3$ and $\mathbb{F}_5$ via purely algebraic methods. For this, first we explained two self-dual codes over $\mathbb{F}_3$ and three self dual codes over $\mathbb{F}_5$ in [3.1.]. Then, we showed that the Lee weight enumerators of these self dual codes are algebraically independent so they generate rings R_3 and R_5 which are isomorphic to the complex polynomials rings $\mathbb{C}[x_0,x_1]$ and $\mathbb{C}[x_0,x_1,x_2]$, respectively in [3.1.3.]. After that, we associated the Weil representations with the finite quadratic modules $\underline{\mathbb{F}_p}$, $p \neq 2$, this Weil representations defined a $\mathrm{SL}(2,\mathbb{F}_p)$-module structure on the space of linear forms of the complex polynomial ring $\mathbb{C}[\{x_a\}_{a\in\mathbb{F}_p}]$ in [3.3.2.], and then we proved that a code over $\mathbb{F}_p$ is a self-dual code if and only if its Lee weight enumerator is invariant under the action $\mathrm{SL}(2,\mathbb{F}_p)$ on the complex polynomial ring $\mathbb{C}[y_0,\cdot,y_{\frac{p-1}{2}}]$ in Theorem 3..50 in [3.3.2.]. Then we calculated the Molien series of the Weil representations for $p = 3,5$ in [5]. Finally, we found that $\dim\mathbb{C}[x_0,x_1]^{\mathrm{SL}(2,\mathbb{F}_3)\times\mu_4} = \frac{1}{(1-x^4)(1-x^{12})}$ and $\dim\mathbb{C}[x_0,x_1,x_2]^{\mathrm{SL}(2,\mathbb{F}_5)\times\mu_2} = \frac{1}{(1-x^2)(1-x^6)(1-x^{10})}$ via Molien series in Theorem 3..57.

The interesting results constitute the two main theorems in [4.1.].

6. PART VI: CONCLUSION AND RECOMMENDATIONS

In this thesis we reproved two structure theorems that describe explicitly the ring generated by the Lee weight enumerators of self-dual codes over $\mathbb{F}_3$ and $\mathbb{F}_5$. Our approach of the proofs were purely algebraic based on the theory of Weil representations of $\mathrm{SL}(2,\mathbb{F}_p)$ and follows ideas of Boylan and Skoruppa explained in [BS16].

For future work, one can use the methods in this thesis to reprove structure theorem which describes explicitly the Lee weight enumerators of self-dual codes over $\mathbb{F}_7$.

REFERENCES

[BS16]. Hatice Boylan and Nils-Peter Skoruppa. Coding theory lecture notes, 2016.

[Con08]. Keith Conrad. Group action, expository text. University of Connecticut, uconn.edu, Math Dept. UConn, 341 Mansfield Road Unit 1009,Storrs, CT 06269-1009, 2008.

[Con10]. Keith Conrad. Sl(2,z). University of Connecticut, uconn.edu, Math Dept. UConn, 341 Mansfield Road Unit 1009,Storrs, CT 06269-1009, 2010. Expository Text.

[Ebe02]. Wolfgang Ebeling. *Lattices and codes*. Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn, Braunschweig, revised edition, 2002. A course partially based on lectures by F. Hirzebruch.

[FHhP03]. Marc Fossorier, Tom Hø holdt, and Alain Poli, editors. *Applied algebra, algebraic algorithms and error-correcting codes*, volume 2643 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, 2003.

[FW91]. Harris J. Fulton W. *Representation Theory*. A First Course. Springer- Verlag, 1991.

[HK71]. K. Hoffman and R Kunze. *Linear Algebra, Second Edition*. Prentice-Hall, Inc., 1971.

[LPS82]. J. S. Leon, V. Pless, and N. J. A. Sloane. Self-dual codes over GF(5). *J. Combin. Theory Ser. A*, 32(2):178–194, 1982.

[LX04]. San Ling and Chaoping Xing. *Coding Theory, a first course*. Cambridge, 2004.

[MS77]. F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. II*. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. North-Holland Mathematical Library, Vol. 16.

[NRS06]. Gabriele Nebe, Eric M. Rains, and Neil J. A. Sloane. *Self-dual codes and invariant theory*, volume 17 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2006.

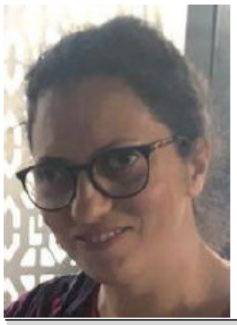
[Ser73]. J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[Ser77]. Jean-Pierre Serre. *Linear representations of finite groups*. Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[Wei03]. Eric W. Weisstein. *CRC concise encyclopedia of mathematics.* Number 1944431 in Second edition. Chapman & Hall/CRC, Boca Raton, FL, 2003.

CURRICULUM VITAE

Personal Details	
Name	Zekiye Pınar Cihan
Place of Birth	Hatay
Date of Birth	25.02.1976
Nationality	[X] T.C. [ ] Other:
Phone	0542 785 54 72
Email	pinaryamuk@gmail.com



Education B.Sc.	
University	Istanbul Üniversitesi
Faculty	Fen Fakültesi
Department	Astronomy and Space Science
Graduation Year	1998