Weight Enumerators and Gray Maps of Linear Codes over Rings

Thesis by

Bahattin Yildiz

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

2006

(Defended May 10, 2006)

To my family

Acknowledgements

I want to thank first and foremost my advisor Prof. Richard M Wilson who patiently guided me through the evolution of this thesis. The experience I got by working alongside him will always be a valuable component of my future career.

I also want to thank the rest of my committee of Prof. Wales, Prof. Ramakrishnan and Prof. McEliece for their valuable evaluation and time. I want to thank the math department of Caltech for supporting me for the duration of my studies.

I want to thank my college professor Serguei Stepanov from Bilkent University for evoking interest in coding theory in me. I also want to thank my high school math teacher and mentor Recep Yucesan who had a substantial share in showing me the beauty and the elegance of mathematics and hence guiding me towards becoming a mathematician.

Abstract

The main focus in this thesis is linear codes over rings. In the first part, we look at linear codes over Galois rings, $GR(p^\ell, m)$, and using the homogeneous weight, we improve upon Wilson's results about the prime power that divides the coefficients of the homogeneous weight enumerators of these codes. We also prove that our results are best possible. Our results about homogeneous weight enumerators of linear codes over $GR(p^\ell, m)$ generalize the results that we have for the Lee weight enumerators of linear codes over $\mathbb{Z}_4$.

We also consider other weight enumerators, in particular the complete weight enumerators of linear codes and we obtain MacWilliams-like identities for these weight enumerators considering different rings. These MacWilliams-like identities lead to MacWilliams identities for the Hamming weight enumerators of linear codes over rings. We also give a counter-example to show that we cannot have MacWilliams-like identities for the Euclidean weight enumerators of linear codes over $\mathbb{Z}_4$.

We also look at Gray maps from $\mathbb{Z}_{p^k}$ to $\mathbb{Z}_p^{p^{k-1}}$. We first give an application of the distance-preserving map from $\mathbb{Z}_9$ to $\mathbb{Z}_3^3$ to obtain good ternary codes, and then we give an inductive algebraic construction of a distance-preserving Gray map from $(\mathbb{Z}_{p^k}, \text{homogeneous distance})$ to $(\mathbb{Z}_p^{p^{k-1}}, \text{hamming distance})$ as well as a combinatorial construction. By using the Gray maps, we obtain some results about the weight enumerators of linear codes over the ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ with $u^2 = 0$.

In the last part of this work, we consider the permutation invariance of binary codes and the connection with linearity over certain rings. Among the rings considered, we have $\mathbb{F}_2 + u\mathbb{F}_2,\ u^2 = 0$; $\mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{2^k-1}\mathbb{F}_2,\ u^{2^k} = 0$; $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2,\ u^2 = v^2 = 0$. In this context we consider the Reed-Muller codes and answer questions about permutation invariance of Reed-Muller codes under certain permutation groups and the linearity of

Reed-Muller codes over these aforementioned rings.

Contents

Chapter 1

Introduction

In the early history of Coding Theory, codes were usually taken over finite fields, in particular over the field of elements modulo 2, which led to the binary codes. In the last decade or so, a growing interest has been shown in linear codes over rings and the so-called Gray maps that mapped these codes into codes over finite fields. In a ground-breaking work, Sloane, Calderbank et al. showed in 1994 that the Kerdock Codes, the Preparata Codes, and Delsarte-Goethals Codes can be obtained by taking the Gray images of linear codes over $\mathbb{Z}_4$. The work that I present in this thesis was partially inspired by their work that led me to consider linear codes over the ring $\mathbb{Z}_4$ with the Lee weight.

A linear code over a ring R of length n is an R-submodule of R^n. The most common rings that were used in this work and in other works about this subject are the ring of integers modulo a prime power, i.e., $\mathbb{Z}_{p^\ell}$ where p is a prime number and more generally the Galois ring extensions of these rings, which we will denote by $GR(p^\ell, m)$. This will denote the Galois ring extension of $\mathbb{Z}_{p^\ell}$ of degree m. Here, ℓ and m are integers. $GR(p^\ell, m)$ will briefly be defined as the quotient $\mathbb{Z}_{p^\ell}[x]/(\phi(x))$ where $\phi(x)$ is a basic irreducible polynomial of degree m over the ring $\mathbb{Z}_{p^\ell}$. We will give a more detailed description of the elements of the Galois ring $GR(p^\ell, m)$ in Chapter 2 with the help of a set that we will define as the *Teichmuller set*, but for now we will only give some of the basic properties of the Galois Ring. $GR(p^\ell, m)$ is a finite chain ideal ring with a unique maximal ideal that is given by $(p) = pGR(p^\ell, m)$ and the quotient field is

$$\frac{GR(p^\ell, m)}{pGR(p^\ell, m)} \simeq \mathbb{F}_{p^m}. \tag{1.1}$$

All ideals of $GR(p^\ell, m)$ can be ordered as

$$\{0\} = p^\ell GR(p^\ell, m) \subset p^{\ell-1} GR(p^\ell, m) \subset \cdots \subset pGR(p^\ell, m) \subset GR(p^\ell, m).$$

A linear code is permutationally equivalent to another code if one can be obtained from the other by a permutation of the coordinates. Because of the finite chain ideal structure of the Galois rings, we can see that any linear code C over $GR(p^\ell, m)$ is equivalent to a code with a generating matrix

$$G = \begin{bmatrix} I_{k_1} & A_1 & . & . & . & A_\ell \\ 0 & pI_{k_2} & pB_1 & . & . & pB_{\ell-1} \\ 0 & 0 & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & . & 0 & p^{\ell-1}I_{k_\ell} & p^{\ell-1}C \end{bmatrix}$$

where $A_i, B_j, \ldots, C$ are all matrices over $GR(p^\ell, m)$. This means that C can be obtained as a linear combination of the rows of G over the Galois ring $GR(p^\ell, m)$. Such a linear code is said to be of *type*

$$(p^{\ell m})^{k_1} (p^{(\ell-1)m})^{k_2} \ldots (p^m)^{k_\ell}$$

and in this case we will have

$$|C| = p^{m\left(\ell k_1 + (\ell-1)k_2 + \cdots + k_\ell\right)}.$$

Another type of rings that will come up in the latter parts of this thesis is the ring of the form $\mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{2^k-1}\mathbb{F}_2$ with $u^{2^k} = 0$. In other words this ring is the same as $\mathbb{F}_2[X]/(x^{2^k})$. Note that this ring is also a finite chain ideal ring. We will also consider another type of rings of the form $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ with $u^2 = v^2 = 0, uv = vu$. Note that this ring is not a finite chain ideal ring, i.e., all its ideals cannot be written in the form of an inclusion chain.

A weight w is a function from the ring to the set of non-negative integers. This function is then extended to the code by letting the weight of a codeword be the sum of the weights of all the coordinates, i.e., if $\overline{c} = (c_1, c_2, \ldots, c_n) \in C$, then we let $w(\overline{c}) = w(c_1)+w(c_2)+\cdots+w(c_n)$. The most common weight used in coding theory is the Hamming weight, which assigns 0 to the zero coordinate and 1 to the rest. We will denote it by w_{H} and so we have $w_{\mathrm{H}}(0) = 0$ and $w_{\mathrm{H}}(x) = 1$, for all $x \neq 0$. A special weight that has been considered in the works of the aforementioned authors and also in my earlier works is the Lee weight on $\mathbb{Z}_4$, which we will denote by w_{L}, and is defined as

$$w_{\mathrm{L}}(x) := \begin{cases} 0 & \text{if } x = 0 \\ 2 & \text{if } x = 2 \\ 1 & \text{otherwise.} \end{cases}$$

A generalization of this weight to the Galois rings is the so-called *homogeneous weight*, which we will denote by w_{hom} and is defined as

$$w_{\mathrm{hom}}(x) := \begin{cases} 0 & \text{if } x = 0 \\ p^{m(\ell-1)} & \text{if } 0 \neq x \in p^{\ell-1}GR(p^\ell, m) \\ (p^m - 1)p^{(\ell-2)m} & \text{otherwise.} \end{cases}$$

Suppose that w is a weight function over a ring R, and C is a linear code over R of length n. Then the w-weight enumerator of C is the polynomial

$$P_C(z) = \sum_{\overline{c} \in C} z^{w(\overline{c})}. \tag{1.2}$$

In some parts of the thesis we will be interested in the *complete weight enumerator* of C. To define that, suppose that $R = \{r_1, r_2, \ldots, r_k\}$ is the whole ring. Then the complete weight enumerator of C is denoted by $\mathrm{cwe}_C(X_1, X_2, \ldots, X_k)$ and is defined as

$$\mathrm{cwe}_C(X_1, X_2, \ldots, X_k) = \sum_{\overline{c} \in C} \prod_{i=1}^{k} X_i^{n_{r_i}(\overline{c})} \tag{1.3}$$

where $n_{r_i}(\overline{c})$ is the number of coordinates in $\overline{c}$ that are equal to r_i. Note that the complete

weight enumerator is a homogeneous polynomial of total degree n in $k = |R|$ variables.

A *Gray map* over $\mathbb{Z}_{p^\ell}$ is a map from $\mathbb{Z}_{p^\ell}^n$ to $\mathbb{F}_p^{np^{\ell-1}}$ that is distance preserving where we take the homogeneous weight in $\mathbb{Z}_{p^\ell}^n$ and the Hamming weight in $\mathbb{F}_p^{np^{\ell-1}}$. This definition is extended to the Galois rings as well.

For a binary code C of length n, a permutation $\tau \in S_n$ acts on a codeword $\overline{c} = (c_1, c_2, \ldots, c_n)$ as

$$\tau(\overline{c}) = (c_{\tau(1)}, c_{\tau(2)}, \ldots, c_{\tau(n)}).$$

We say that a code C is *invariant* under a permutation τ if $\tau(\overline{c}) \in C$ for all $\overline{c} \in C$. For a permutation subgroup $H < S_n$, we say that C is invariant under the permutation group H if C is invariant under τ for all $\tau \in H$.

1.1 History

The main work that forms a basis of inspiration and a basic tool for the work done in Chapter 2 about the weights of codes modulo prime powers was done by Wilson in 2003 in [1]. His main theorem in this work was about the weights modulo p^e of linear codes and contains the following:

Theorem 1.1. (Wilson, [1]) *Let G be a group of order p^s, p prime, let $\mathbf{C}$ be a subgroup of $G^n = G \times \cdots \times G$, and let $\mathbf{A}$ be a coset of $\mathbf{C}$ in G^n. Suppose $|\mathbf{A}| = |\mathbf{C}| = p^k$. Let μ be a mapping from G into integers and define for $\overline{a} = (a_1, \ldots, a_n) \in G^n$, $\mu(\overline{a}) = \sum_{i=1}^n \mu(a_i)$. If $k > s((m(p-1)+1)p^{e-1} - 1)$, then for any integer t, the number N of solutions $\overline{a} \in \mathbf{A}$ to the equation $\mu(\overline{a}) \equiv t \pmod{p^e}$ is divisible by p^m.*

He also proved the following theorem in the same work that forms a basis in proving that my results in Chapter 2 are best possible:

Theorem 1.2. (Wilson, [1]) *Let c be an integer with $c \equiv 1 \pmod{p}$ where p is a prime. Then*

$$(cx-1)^{(m(p-1)+1)p^{e-1}-1} \equiv (-p)^{m-1} \sum_{j=0}^{p^e-1} x^j \pmod{p^m, x^{p^e}-1}$$

for all positive integers m.

Noting that the coefficients of $f(x)^k$ are linear combinations of the coefficients of $f(x)^{k-1}$, where $f(x)$ is a polynomial with integer coefficients, we get the following corollary to Theorem 1.2, which will be useful in our calculations:

Corollary 1.3. *Suppose p is a prime and c is an integer with $c \equiv 1 \pmod{p}$. If*

$$(cx-1)^k \equiv A_0 + A_1 x + \dots A_{p^e-1} x^{p^e-1} \pmod{x^{p^e}-1},$$

then

$$\min\left\{ \nu_p(A_j) \middle| j = 0, \dots, p^e - 1 \right\} = \left\lfloor \frac{k - p^{e-1}}{(p-1)p^{e-1}} \right\rfloor$$

where $\nu_p(A_j)$ is the p-adic valuation of A_j, namely, the highest power of p that divides A_j.

While Wilson worked over general group codes with a generic weight function, Vera Pless obtained the following result about the Hamming weight distributions of binary codes modulo 4 in [3]:

Theorem 1.4. (Pless, [3]) *Let C be a binary $[n,k]$-code with odd weight vectors. Let a,b,c,d denote the number of codewords in C that have weights congruent to $0,2,3,1$ respectively. If $a=b=c=d=2^{k-2}$, then $C \cap C^\perp$ is singly-even. $\frac{k-2}{2} \le s \le k-2$. In all other cases $C \cap C^\perp$ is doubly-even and we have the following possibilities where $\frac{k-2}{2} \le s \le k-2$:*
1) *$a = b = 2^{k-2}$, $c = 2^{k-2} \pm 2^s$, $d = 2^{k-2} \mp 2^s$. If $s = k-2$, $C \cap C^\perp$ consists of all the doubly even vectors in C.*
2) *$a = 2^{k-2} \pm 2^s$, in case of the minus sign we take $s \le k-3$. $b = 2^{k-2} \mp 2^s$, and the following three cases:*

(i) $c = b$, $a = d$

(ii) $c = a, b = d$

(iii) $c = d = 2^{k-2}$

We obtain the following immediate corollary to Theorem 1.4, which is more in context of what will be done in Chapter 2:

Corollary 1.5. *Suppose C is a k-dimensional binary linear code of length n and suppose $N_C(i,4)$ denotes the number of codewords in C that have their Hamming weights congruent*

to i modulo 4. Then

$$N_C(i,4) \equiv 0 \pmod{2^q}, \qquad i = 0,1,2,3$$

where

$$q = \left\lfloor \frac{k-2}{2} \right\rfloor.$$

Jurian Simonis, in his work ([4]) in 1994, obtained similar results to those of Pless about binary codes with Hamming weights.

In their ground-breaking work that was published as [2] in 1994, Hammons, Sloane et al. introduced the notions of complete weight enumerators, symmetric weight enumerators, and Lee and Hamming weight enumerators for linear codes over $\mathbb{Z}_4$. Suppose that C is a linear code over the ring $\mathbb{Z}_4$ and let $C^{\perp}$ be the dual of C with respect to the Euclidean inner product modulo 4. Then

$$\mathrm{cwe}_C(W,X,Y,Z) = \sum_{a \in C} W^{n_0(a)} X^{n_1(a)} Y^{n_2(a)} Z^{n_3(a)} \tag{1.4}$$

where $n_j(a)$ is the number of coordinates in a that are congruent to j modulo 4. They defined the *symmetrized weight enumerator* of C, $\mathrm{swe}_C(W,X,Y)$, as

$$\mathrm{swe}_C(W,X,Y) = \mathrm{cwe}_C(W,X,Y,X). \tag{1.5}$$

They defined the *Lee weight enumerator* of C as

$$\mathrm{Lee}_C(W,X) = \sum_{a \in C} W^{2n - w_L(a)} X^{w_L(a)} = \mathrm{swe}_C(W^2, WX, X^2) \tag{1.6}$$

and similarly, the *Hamming weight enumerator* was defined as

$$\mathrm{Ham}_C(W,X) = \mathrm{swe}_C(W,X,X). \tag{1.7}$$

Then the following analogous MacWilliams identities were obtained:

$$\mathrm{cwe}_{C^\perp}(W,X,Y,Z) =$$
$$\frac{1}{|C|}\mathrm{cwe}_C(W+X+Y+Z, W+iX-Y-iZ, W-X+Y-Z, W-iX-Y+iZ), \quad (1.8)$$

$$\mathrm{swe}_{C^\perp}(W,X,Y) = \frac{1}{|C|}\mathrm{swe}_C(W+2X+Y, W-Y, W-2X+Y), \quad (1.9)$$

$$\mathrm{Lee}_{C^\perp}(W,X) = \frac{1}{|C|}\mathrm{Lee}_C(W+X, W-X), \quad (1.10)$$

$$\mathrm{Ham}_{C^\perp}(W,X) = \frac{1}{|C|}\mathrm{Ham}_C(W+3X, W-X). \quad (1.11)$$

Delsarte considered the problem of MacWilliams identities for the Hamming weight enumerators of abelian group codes in 1973 in his work [5]. Suppose C is a group code over G with $|G| = q$. Suppose

$$\mathrm{H}_C(W,X) = \sum_{\overline{c}\in C} W^{n-h(\overline{c})}X^{h(\overline{c})}$$

is the Hamming weight enumerator of C and suppose C^* is the dual of C with respect to the inner product defined on G by using characters on G. Then we have the MacWilliams identity for the Hamming weight enumerators of C and C^* as follows:

$$\mathrm{H}_{C^*}(W,X) = \frac{1}{|C|}\mathrm{H}_C\big(W+(q-1)X, W-X\big). \quad (1.12)$$

Considering the Gray map from $\mathbb{Z}_4$ to $\mathbb{F}_2^2$ that preserves the Lee distance on $\mathbb{Z}_4$-codes, Hammons et al. in their work [2] in 1994 proved the following theorem that inspired some of the work done in Chapter 5 of this thesis:

Theorem 1.6. *The rth order binary Reed-Muller code $RM(r,m)$ of length $n = 2^m$, $m \geq 1$, is the Gray image of a linear code over $\mathbb{Z}_4$ for $r = 0, 1, 2, m-1$ and m.*

They also conjectured that the Reed-Muller codes $RM(r,m)$ with $3 \leq r \leq m-2$ cannot be obtained as the Gray images of linear codes over $\mathbb{Z}_4$ and they proved the conjecture in the particular case for $r = m-2$ when $m \geq 5$. They linked $\mathbb{Z}_4$-linearity with invariance under certain permutations, which formed the inspiration for the work in Chapter 5.

1.2 Methods and Summary of the Main Results

In Chapter 2, our main focus will be on homogeneous weights modulo p^e of linear codes over the Galois ring $GR(p^\ell, m)$. I basically will prove that the number of codewords in a linear code over $GR(p^\ell, m)$ that have homogeneous weights in a particular congruence class modulo p^e is divisible by a high power of p. This result will in a sense be similar to Wilson's result in [1] and in fact my main tool will be Theorem 1.1. But the difference in my result will be that the power of p that divides $N_C(i, p^e)$'s will be higher than those obtained by Theorem 1.1. In fact, using Theorem 1.2 as a tool, I will prove that the results that I obtained are best possible. I will first talk about my earlier results, which are mainly about the Lee weights of the linear codes over $\mathbb{Z}_4$. The first result that I obtained was the following:

Theorem 1.7. *Let* $\mathbf{C}$ *be a* k*-dimensional linear code over* $\mathbb{Z}_4$*, or equivalently let* C *be a linear code over* $\mathbb{Z}_4$ *of type* $(4)^k$*. Denote by* $N_{\mathbf{C}}(i, 4)$ *the number of codewords in* $\mathbf{C}$ *that have Lee Weights congruent to* i *modulo* 4*. Then*

$$N_{\mathbf{C}}(i, 4) \equiv 0 \pmod{2^{k-1}}$$

for $i = 0, 1, 2, 3$*.*

Then, with a method similar to the proof of Theorem 1.1, I was able to obtain the following result:

Theorem 1.8. *Suppose* $\mathbf{C}$ *is a* k*-dimensional linear* $\mathbb{Z}_4$*-code. If we denote by* $N_C(j, 2^e)$ *the number of codewords in* $\mathbf{C}$*, that have Lee weights congruent to* j *modulo* 2^e*, then we have*

$$N_{\mathbf{C}}(j, 2^e) \equiv 0 \pmod{2^{\lfloor \frac{k-2^{e-2}}{2^{e-2}} \rfloor}}, \qquad j = 0, 1, \ldots, 2^e - 1.$$

I then extended the result to linear codes over $\mathbb{Z}_4$ of the general type $(4)^{k_1}(2)^{k_2}$ by using a method that involved looking at the cosets of the *even subcode* of the code C. The following result was obtained:

Theorem 1.9. *Suppose* $\mathbf{C}$ *is a linear code over* $\mathbb{Z}_4$ *of type* $(4)^{k_1}(2)^{k_2}$*. If we denote by*

$N_C(j, 2^e)$ the number of codewords in $\mathbf{C}$*, that have Lee weights congruent to j modulo 2^e, then we have*

$$N_{\mathbf{C}}(j, 2^e) \equiv 0 \pmod{2^q}, \qquad j = 0, 1, \ldots, 2^e - 1$$

where $q = 2k_1 + k_2 - 1$ if $e = 1$ and

$$q = \max\left\{0, \left\lfloor \frac{k_1 + k_2 - 2^{e-2}}{2^{e-2}} \right\rfloor\right\}$$

for $e \geq 2$.

Here, $\lfloor . \rfloor$ is the floor function, i.e., $\lfloor x \rfloor$ is the greatest integer less than or equal to x. I also proved, by looking at the trivial block code over $\mathbb{Z}_4$, namely $(\mathbb{Z}_4)^{k_1}(2\mathbb{Z}_4)^{k_2}$ as an example and, using Theorem 1.2, that the results in the previous theorems are best possible.

The coset method used in the proof of Theorem 1.9 proved to be useful in extending the result to more general rings with a proper extension of the Lee weight defined. Some of the rings that were used were $\mathbb{Z}_{2^m}$, $\mathbb{Z}_{p^m}$, and finally the Galois ring $GR(p^\ell, m)$. Consequently the following result was obtained that generalizes all the theorems 1.7–1.9:

Theorem 1.10. *Suppose C is a linear code over $GR(p^\ell, m)$ of type*

$$(p^{\ell m})^{k_1}(p^{(\ell-1)m})^{k_2} \ldots (p^m)^{k_\ell},$$

then we have

$$N_C^{\hom}(j, p^e) \equiv 0 \pmod{p^q}, \qquad j = 0, 1, \ldots, p^e - 1$$

where

$$q = \max\left\{0, \left\lfloor \frac{k_1 + k_2 + \cdots + k_\ell - p^{e-(\ell-1)m-1}}{(p-1)p^{e-(\ell-1)m-1}} \right\rfloor\right\}$$

and $e \geq (\ell - 1)m + 1$.

Here $N_C^{\hom}(j, p^e)$ denotes the number of codewords in C that have homogeneous weights (as defined at the beginning of this chapter) congruent to j modulo p^e. Of course, due to the nature of the homogeneous weight, we don't need to bother about $N_C(j, p^e)$ when $e \leq (\ell - 2)m$, but there remains the case when $(\ell - 2)m + 1 \leq e \leq (\ell - 1)m$, which is not

covered by Theorem 1.10, and for that, we have the following theorem, which is proved by looking at the particular coset structure:

Theorem 1.11. *With C being the same as in Theorem 1.10, we have*

$$N_C^{\hom}(j, p^e) \equiv 0 \pmod{p^x}$$

where

$$x = m(k_1 + k_2 + \cdots + k_{\ell-1} + k_\ell) + \left\lfloor \frac{k_1 + k_2 + \cdots + k_{\ell-1} - p^{e-(\ell-2)m-1}}{(p-1)p^{e-(\ell-2)m-1}} \right\rfloor$$

for all $(\ell-2)m + 1 \leq e \leq (\ell-1)m$.

In this case also, we prove that the result in Theorem 1.10 is best possible by looking at the trivial block code over $GR(p^\ell, m)$ of type

$$(p^{\ell m})^{k_1}(p^{(\ell-1)m})^{k_2} \ldots (p^m)^{k_\ell}$$

and again using Theorem 1.2.

We also extend the result of Theorem 1.10 to a slightly more general weight than the homogeneous weight in a way that generalizes the Hamming weight as well. We will introduce the weight and the subsequent result at the end of Chapter 2, together with an analogous result for the Hamming weight. We will also comment on different possible ways of generalizing the Lee weight to higher rings.

We will obtain similar results for different kinds of rings that we will introduce in Chapter 4, and so those results will be stated and proved in that chapter.

In Chapter 3, we will talk about the MacWilliams identities for linear codes over rings. First, inspired by the MacWilliams identities for the complete, symmetrized, Hamming and Lee weight enumerators of linear $\mathbb{Z}_4$-codes that Sloane, Calderbank, et al. came up with in [2] in the form of equations 1.8–1.11, I wanted to settle down the question of whether a MacWilliams-like identity exists between the *Euclidean* weight enumerators of the dual codes over $\mathbb{Z}_4$. I want to recall that the Euclidean weight w_{E} on $\mathbb{Z}_4$ is given by $w_{\mathrm{E}}(0) = 0$,

$w_{\mathrm{E}}(2) = 2^2 = 4$, $w_{\mathrm{E}}(1) = w_{\mathrm{E}}(3) = 1$. After numerous attempts at trying to come up with a similar equation to those in (1.8)–(1.11), I finally came up with a counter example that prompted the following little result:

Theorem 1.12. *There exist linear codes over $\mathbb{Z}_4$ whose Euclidean weight enumerators are the same, but the Euclidean weight enumerators of the duals are not the same. Hence there cannot be a MacWilliams-like identity for the Euclidean weight enumerators of dual codes over $\mathbb{Z}_4$.*

The counter example itself and the weight enumerators are very big, and we make special use of (1.9) to calculate the weight enumerators of the duals. This will all be given in Chapter 3.

After this failed attempt at finding a MacWilliams-like identity for the Euclidean weight enumerators of linear $\mathbb{Z}_4$-codes and seeing how useful MacWilliams identities for the complete weight enumerators can be, I decided to look for MacWilliams identities for the complete weight enumerators of linear codes over rings. In [5], Delsarte looked at abelian group codes and found MacWilliams identities for the Hamming weight enumerators of these codes. Using some of his material together with the techniques from [6], I proved the following theorem for group codes:

Theorem 1.13. *Suppose that $G = \{g_1, \ldots, g_q\}$ is an abelian group of order q and suppose it is of the form*

$$G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \mathbb{Z}_{m_r}$$

where

$$m_i = p_1^{e_{i1}} p_2^{e_{i2}} \ldots p_k^{e_{ik}}$$

for primes $p_1 > p_2 > \cdots > p_k$ and for non-negative integers $e_{1j} \geq e_{2j} \geq \cdots \geq e_{rj}$, $j = 1, 2, \ldots, k$. Suppose ξ is a primitive $m_1 = (p_1^{e_{11}} p_2^{e_{21}} \ldots p_k^{e_{k1}})^{th}$ root of unity over complex numbers. Suppose that C is a group code of length n over G, and suppose C^* is the dual of C with respect to an appropriately defined inner product. Then we have

$$\mathrm{cwe}_{C^*}(W_1, W_2, \ldots, W_q) = \frac{1}{|C|} \mathrm{cwe}_C\Big(\sum_{i=1}^{q} \xi^{g_1 * g_i} W_i, \sum_{i=1}^{q} \xi^{g_2 * g_i} W_i, \ldots, \sum_{i=1}^{q} \xi^{g_q * g_i} W_i\Big)$$

where

$$g_i * h_i = g_i(1)h_i(1) + \frac{m_1}{m_2}g_i(2)h_i(2) + \cdots + \frac{m_1}{m_r}g_i(r)h_i(r).$$

This turns out to be a generic formula for the MacWilliams identities for the complete weight enumerators of the group codes. From here, it is very easy to prove Delsarte's theorem about the Hamming weight enumerators of group codes. Now, when it comes to linear codes over rings, there is something to be careful about. *While every linear code over a ring can be viewed as an abelian group code, not every group code can be viewed as a linear code over a ring.* So, while the dual with respect to the above inner product of every group code is an abelian group code, we can't use the same inner product for linear codes over rings, because the dual of a linear code over a ring with respect to this inner product might not be linear over that ring.

For the rest of Chapter 3, I introduced new inner products for different rings, and using Theorem 1.13 as a base, I obtained some numerical MacWilliams identities for linear codes over rings, and in particular for some of them I introduced the notion of symmetrized weight enumerators as well and found MacWilliams identities for the symmetrized weight enumerators of these codes. I will state some of the results as corollaries to Theorem 1.13:

Corollary 1.14. *Suppose C is a linear $\mathbb{Z}_m$-code of length n and suppose $C^\perp$ is its dual with respect to the Euclidean inner product modulo m. Then, $C^\perp$ is also a linear code over $\mathbb{Z}_m$. Suppose, moreover, that ξ is a primitive m^{th} root of unity over the complex numbers. Then if*

$$\mathrm{cwe}_C(W_0, W_1, \ldots, W_{m-1}) = \sum_{\bar{c}} \prod_{i=0}^{m-1} W_i^{n_i(\bar{c})}$$

is the complete weight enumerator of C, we have

$$\mathrm{cwe}_{C^\perp}(W_0, W_1, \ldots, W_{m-1}) = \frac{1}{|C|}\mathrm{cwe}_C\Big(\sum_{i=0}^{m-1} W_i, \sum_{i=0}^{m-1} \xi^i W_i, \ldots, \sum_{i=0}^{m-1} \xi^{(m-1)i} W_i\Big).$$

A substantial result that I obtained was for linear codes over the Galois ring $GR(p^\ell, m)$. I had to introduce an inner product so that the dual of linear codes over the Galois rings would be linear as well. To this extent, I introduced the following inner product:

Suppose

$$\overline{x} = (x_1, x_2, \ldots, x_n),\ \ \overline{y} = (y_1, y_2, \ldots, y_n) \in GR(p^e, m)^n$$

are two vectors, then we define a symmetric function $< ., . >$ from $GR(p^\ell, m)^n \times GR(p^\ell, m)^n$ to $\mathbb{Z}_{p^\ell}$ by letting

$$< \overline{x}, \overline{y} >= \mathrm{Tr}(x_1 y_1 + x_2 y_2 + \cdots + x_n y_n) \tag{1.13}$$

where $x_i y_i$ is the ordinary product in $GR(p^\ell, m)$.

Here, Tr is the trace function over the Galois rings, which is a $\mathbb{Z}_{p^\ell}$-linear function and more information will be given on this and Galois rings in Chapter 2. Then, I was able to conclude the following by Theorem 1.13 as well as a lemma that I will introduce in Chapter 3:

Theorem 1.15. *Suppose that $GR(p^\ell, m) = \{u_0, u_1, \ldots, u_{p^{\ell m}-1}\}$ is the Galois ring extension of $\mathbb{Z}_{p^\ell}$, and suppose C is a linear code over $GR(p^\ell, m)$ of length n and suppose that C^* is the dual of C with respect to the inner product defined above. Then C^* is also a linear code over $GR(p^\ell, m)$ of length n and moreover we have*

$$\mathrm{cwe}_{C^*}(W_0, W_1, \ldots, W_{p^{\ell m}-1}) =$$
$$\frac{1}{|C|}\mathrm{cwe}_C\Big(\sum_{i=0}^{p^{\ell m}-1} \alpha^{\mathrm{Tr}(u_0 u_i)} W_i,\ \sum_{i=0}^{p^{\ell m}-1} \alpha^{\mathrm{Tr}(u_1 u_i)} W_i, \ldots,\ \sum_{i=0}^{p^{\ell m}-1} \alpha^{\mathrm{Tr}(u_{p^{\ell m}-1} u_i)} W_i\Big).$$

A similar result was obtained for the symmetrized weight enumerators of linear codes over Galois rings inspired by the homogeneous weight. The corresponding result for the Hamming weight enumerators was unchanged.

Similar results, together with new inner products, were introduced for the rings $\mathbb{F}_{p^m}$, and $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ where $u^2 = 0$. They will all be mentioned appropriately in Chapter 3.

In Chapter 4, I focus mainly on Gray maps. Starting with the Gray map from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$ that was introduced in [2], I first extended the Gray map to a distance preserving Gray map from $\mathbb{Z}_9$ to $\mathbb{Z}_3^3$ where we take the homogeneous distance in $\mathbb{Z}_9$ and the Hamming distance in $\mathbb{Z}_3^3$. Using the Weil bound that I took from [7] that gives a bound on the exponential sums, and the $\mathbb{Z}_9$-ary linear trace codes, similar to the one Carlet used in [8], I was able

to come up with some ternary codes with high minimum distances, comparable to the ones that Harada and Gulliver obtained in [9]. In particular I obtained as an example a ternary code with parameters $[243, 3^{10}, \geq 126]$.

I then ventured to generalize the Gray map to $\mathbb{Z}_{p^k}$, and I got the following inductive construction of the Gray map. I proved that it is distance-preserving. I obtained this Gray map independently of the Gray maps obtained by Ling in [10]. In what follows, G_k denotes the Gray map from $\mathbb{Z}_{p^k}$ to $\mathbb{Z}_p^{p^{k-1}}$.

Definition 1.16. We first let

$$G_k(0) = \Big(G_{k-1}(0), G_{k-1}(0), \ldots, G_{k-1}(0) \Big), \tag{1.14}$$

and define

$$G_k(j \cdot p^{k-1}) = \Big(G_{k-1}(j \cdot p^{k-2}), \ldots, G_{k-1}(j \cdot p^{k-2}) \Big). \tag{1.15}$$

Now, for $0 \leq m, j \leq p-1$ and for $1 \leq i \leq p^{k-2} - 1$, we define

$$G_k((mp+j)p^{k-2} + i) = \Big(G_{k-1}\big(\gamma(mjp^{k-2} + i)\big), G_{k-1}\big(\gamma((m+1)jp^{k-2} + i)\big), \ldots, G_{k-1}\big(\gamma((m+p-1)jp^{k-2} + i)\big) \Big). \tag{1.16}$$

where $\gamma(.)$ is the map that takes a number to its residue modulo p^{k-1}. Finally for $j \cdot p^{k-1} + np^{k-2}$ for some $0 \leq j \leq p-1$ and $1 \leq n \leq p-1$, then we define

$$G_k(j \cdot p^{k-1} + np^{k-2}) = \Big(G_{k-1}\big(\gamma((j + n \cdot 0)p^{k-2})\big), G_{k-1}\big(\gamma((j + n \cdot 1)p^{k-2})\big), \ldots, G_{k-1}\big(\gamma((j + n(p-1))p^{k-2})\big) \Big). \tag{1.17}$$

This is the inductive step with $G_1 : \mathbb{Z}_p \to \mathbb{Z}_p$ being the identity map.

I then proved that the map thus defined is indeed distance-preserving:

Theorem 1.17. *The map G_k defined above in Definition 1.16, is distance-preserving from*

$(\mathbb{Z}_{p^k}^n, \text{homogeneous distance})$ *to* $(\mathbb{Z}_p^{p^{k-1}n}, \text{Hamming distance})$.

Seeing as how there are different ways of defining the Gray map algebraically, which give rise to equivalent maps, I then considered the Gray map from a purely combinatorial perspective. As a result I was able to obtain the Gray map by using Affine geometries. The information on Affine geometries together with the relevant lemmas with their proofs are all going to appear in Chapter 4. I refer the reader to Chapter 4 for further information. I will just give the combinatorial construction that I came up with here:

Suppose that $\Gamma_0, \Gamma_1, \ldots, \Gamma_{p^{k-1}-1}$ are the parallel classes of the hyperplanes of $AG_k(p)$ (the Affine Geometry of order k over $\mathbb{F}_p$) that don't contain any of the lines $L_0, L_1, \ldots, L_{p^{k-1}-1}$ in the parallel class $\bar{L}$. So, each hyperplane in these parallel classes is formed by taking one element from each column of

$$\bar{L} = \left\{ \begin{pmatrix} 0 \\ 1 \\ \vdots \\ p-1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ p-1 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ p-1 \end{pmatrix} \right\}, \tag{1.18}$$

which is just a labelling of the lines. Suppose, without loss of generality that we have labelled (1.18) in such a way that there exists a hyperplane corresponding to the labelling of $(0, 0, \ldots, 0)$ and that it is in Γ_0. From now on, when we say the vector that corresponds to a hyperplane, we will mean the $\{0, 1, \ldots, p-1\}$-vector of length p^{k-1} that comes from the labelling of the elements of the hyperplane. So, now, we are finally ready to describe the Gray map $G_k : \mathbb{Z}_{p^k} \to (\mathbb{Z}_p)^{p^{k-1}}$.

We map $0, p^{k-1}, \ldots, (p-1)p^{k-1}$ to the vectors of the hyperplanes in Γ_0 bijectively, with the convention that we map 0 to $(0, 0, \ldots, 0)$. For $1 \leq j \leq p^{k-1}-1$, we map $j, p^{k-1}+j, \ldots, (p-1)p^{k-1}+j$ to the vectors of the hyperplanes of Γ_j bijectively. Note that this is indeed a map from $\mathbb{Z}_{p^k}$ to $(\mathbb{Z}_p)^{p^{k-1}}$. We prove the main result in the following theorem:

Theorem 1.18. *The map G_k defined as above is indeed a distance-preserving map from $\mathbb{Z}_{p^k}$ with the homogeneous weight to $(\mathbb{Z}_p)^{p^{k-1}}$ with the Hamming weight.*

As an application of the Gray maps, I looked at the rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ that

were introduced in [13] and [11], respectively. In particular there are several Gray maps defined from $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ where the target field could be $\mathbb{F}_{2^m}$ or $\mathbb{F}_2$ or the ring $\mathbb{F}_2 + u\mathbb{F}_2$. I proved in particular that the Gray map defined from $(\mathbb{F}_{2^m} + u\mathbb{F}_{2^m})^n$ to $(\mathbb{F}_2 + u\mathbb{F}_2)^{mn}$ is an $\mathbb{F}_2 + u\mathbb{F}_2$-linear map and in particular it maps a linear code over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ of type $(2^{2m})^{k_1}(2^m)^{k_2}$ to a linear code over $\mathbb{F}_2 + u\mathbb{F}_2$ of type $(4)^{mk_1}(2)^{mk_2}$, and moreover this map is weight preserving where we take the extended Lee weight in $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$, which is defined in section 4.4 and the Lee weight in $\mathbb{F}_2 + u\mathbb{F}_2$.

I was then interested in the weight distributions of linear codes over these rings in the same context as the work that I did in Chapter 2. With the *Lee weight* defined in $\mathbb{F}_2 + u\mathbb{F}_2$ to be $w_{\mathrm{L}}(0) = 0, w_{\mathrm{L}}(1) = w_{\mathrm{L}}(1+u) = 1, w_{\mathrm{L}}(u) = 2$, I was able to prove the following result with the same methods as in Chapter 2:

Theorem 1.19. *Suppose C is a linear code of type $(4)^{k_1}(2)^{k_2}$ over $\mathbb{F}_2 + u\mathbb{F}_2$. If $N_C^{\mathrm{L}}(j, 2^e)$ denotes the number of codewords in C that have Lee weights congruent to j modulo 2^e, then*

$$N_C^{\mathrm{L}}(j, 2^e) \equiv 0 \pmod{2^q}, \qquad j = 0, 1, \ldots, 2^e - 1$$

where

$$q = \left\lfloor \frac{k_1 + k_2 - 2^{e-2}}{2^{e-2}} \right\rfloor$$

for all $e \geq 2$. Moreover,

$$N_C^{\mathrm{L}}(j, 2) \equiv 0 \pmod{2^{2k_1+k_2-1}}, \qquad j = 0, 1.$$

I was also able to prove that this result is best possible. With an analogous definition of the Lee weight for the ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ taken from [11] and with the tools that I obtained from the Gray maps, I was able to extend Theorem 1.19 to the ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$, which gives us a result different than those obtained in Chapter 2. I was also able to prove that these results are best possible.

The last part of my research that is summarized in Chapter 5 focuses on binary codes that are invariant under certain permutations and how this relates to being the Gray images

of some linear codes over some certain rings. The work in this chapter was partly inspired by a conjecture in [2] in which the authors conjectured that the Reed-Muller codes $RM(r,m)$ are not $\mathbb{Z}_4$-linear for $3 \leq r \leq m-2$. With [11], [12], [13], I was first introduced to linear codes over rings of the form $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$. Since binary codes are the Gray images of linear codes over these rings if and only if they are invariant under the *swap map*, which essentially is the permutation group $\mathbb{Z}_2$, I considered different permutation groups that in turn led me to different rings. Some of the results I got in this context are given below. The proofs of these theorems together with the descriptions of the particular Gray maps involved are going to be given in Chapter 5:

Theorem 1.20. *Suppose C is a binary linear code of length $4n$. Then C is the Gray image of a linear code over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ of length n if and only if C is K_4-invariant.*

Here, K_4 denotes the Klein-4 group.

Theorem 1.21. *Suppose C is a binary linear code of length $4n$. Then C is the Gray image of a linear code over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ of length n if and only if C is $\mathbb{Z}_4$-invariant.*

An interesting application of these theorems was to show the linearity of the Reed-Muller codes $RM(r,m)$ over these rings. I was able to prove this both by directly finding the pre-images of the Reed-Muller codes in these rings and also by proving their invariance under the permutation groups mentioned:

Theorem 1.22. *The Reed-Muller code $RM(r,m)$ is K_4-invariant for all $0 \leq r \leq m$ or equivalently the Reed-Muller code is the image under the Gray map of a linear code over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ of length 2^{m-2}.*

Theorem 1.23. *The Reed-Muller code $RM(r,m)$ is $\mathbb{Z}_4$-invariant or equivalently is the Gray image of a linear code over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$.*

The pre-images of the Reed-Muller codes in the rings $\mathbb{F}_2+u\mathbb{F}_2$, $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2+u^3\mathbb{F}_2$ and $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ are found in section 5.4. For example, if we define by $FRM(r,m-1)$, for $r = 0,1,2,\ldots,m$, the linear code over $\mathbb{F}_2 + u\mathbb{F}_2$ that is generated by $RM(r-1,m-1)$ and $uRM(r,m-1)$, with the conventions that $RM(-1,m-1) = RM(m,m-1) = 0$,

and if $\phi : (\mathbb{F}_2 + u\mathbb{F}_2)^n \to \mathbb{F}_2^{2n}$ is the Gray map, then $\phi(FRM(r, m-1)) = RM(r, m)$ for $r = 0, 1, 2, \ldots, m$.

In section 5.5 I considered the extension $\mathbb{Z}_{2^k}$ of the permutation groups $\mathbb{Z}_2$ and $\mathbb{Z}_4$ and tried to determine if the Reed-Muller codes are invariant under this permutation group. It turned out that in general we won't have this invariance. The main theorem I proved was the following:

Theorem 1.24. *Suppose $3 \leq k \leq m$ is an integer, then $RM(r, m)$ is invariant under the permutation group $\mathbb{Z}_{2^k}$ if and only if $r = 0, r = m$ or $r = m - 1$.*

I also wanted to consider the ring $\mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{2^k-1}\mathbb{F}_2$ with a weight function defined so that we could define a Gray map that would relate to $\mathbb{Z}_{2^k}$-invariance. I let $S_k = \mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{2^k-1}\mathbb{F}_2$, and so I defined a Gray map $S_k^n \to \mathbb{F}_2^{2^k n}$ inductively as follows:

Definition 1.25. Let

$$\overline{a} = \overline{a}_0 + u\overline{a}_1 + \cdots + u^{2^k-1}\overline{a}_{2^k-1} \in S_k^n$$

be given with $\overline{a}_i \in \mathbb{F}_2^n$ for each $i = 0, 1, \ldots, 2^k - 1$. Write $\overline{a}$ in the following way:

$$\begin{aligned}\overline{a} &= \overline{a}_0 + u\overline{a}_1 + \cdots + u^{2^k-1}\overline{a}_{2^k-1} \\ &= (\overline{a}_0 + u^{2^{k-1}}\overline{a}_{2^{k-1}}) + u(\overline{a}_1 + u^{2^{k-1}}\overline{a}_{2^{k-1}+1}) + \cdots + u^{2^{k-1}-1}(\overline{a}_{2^{k-1}-1} + u^{2^{k-1}}\overline{a}_{2^k-1}).\end{aligned}$$

Then we define $\phi_k(\overline{a})$ as follows:

$$\phi_k(\overline{a}) = \big(\phi_{k-1}(A_1(\overline{a})) + \phi_{k-1}(A_2(\overline{a})), \phi_{k-1}(A_2(\overline{a}))\big) \tag{1.19}$$

where

$$A_1(\overline{a}) = \overline{a}_0 + u\overline{a}_1 + \cdots + u^{2^{k-1}-1}\overline{a}_{2^{k-1}-1} \tag{1.20}$$

and

$$A_2(\overline{a}) = \overline{a}_{2^{k-1}} + u\overline{a}_{2^{k-1}+1} + \cdots + u^{2^{k-1}-1}\overline{a}_{2^k-1}. \tag{1.21}$$

Then I was able to prove the following theorem:

Theorem 1.26. *Suppose that C is a linear binary code of length $2^k n$. Then C is invariant under the permutation group $\mathbb{Z}_{2^k}$ if and only if C is the image under ϕ_k of some linear code over S_k of length n.*

Chapter 2

Homogeneous Weights Modulo p^e of Linear Codes over Galois Rings

In this chapter, we will try to obtain results for the weight enumerators of linear codes over rings, in particular over Galois rings. The main motivation and the tools for the work in this chapter come from the work done by Wilson in [1]. Our goal is to improve on his results in the case of Galois ring codes with the homogeneous weights. We recall that his main results are as follows, which were introduced in Chapter 1 as Theorem 1.1 and Theorem 1.2.

Theorem 2.1. (Wilson, [1]) *Let G be a group of order p^s, p prime, let $\mathbf{C}$ be a subgroup of $G^n = G \times \cdots \times G$, and let $\mathbf{A}$ be a coset of $\mathbf{C}$ in G^n. Suppose $|\mathbf{A}| = |\mathbf{C}| = p^k$. Let μ be a mapping from G into integers and define for $\overline{a} = (a_1, \ldots, a_n) \in G^n$, $\mu(\overline{a}) = \sum_{i=1}^{n} \mu(a_i)$. If $k > s((m(p-1)+1)p^{e-1} - 1)$, then for any integer t, the number N of solutions $\overline{a} \in \mathbf{A}$ to the equation $\mu(\overline{a}) \equiv t \pmod{p^e}$ is divisible by p^m.*

Theorem 2.2. (Wilson, [1]) *Let c be an integer with $c \equiv 1 \pmod{p}$ where p is a prime. Then*

$$(cx-1)^{(m(p-1)+1)p^{e-1}-1} \equiv (-p)^{m-1} \sum_{j=0}^{p^e-1} x^j \pmod{p^m, x^{p^e}-1}$$

for all positive integers m.

Out of these, Theorem 2.1 is going to be the main tool that we use in proving our main result; this is also the result upon which we improve. Theorem 2.2 is going to serve as a main tool in proving that the main result is best possible.

In the first section, I will mention the early results that are mainly about the linear codes over $\mathbb{Z}_4$, in section 2, I will give a more detailed introduction about Galois rings, and in section 3, I will talk about linear codes over Galois rings and the homogeneous weights. In section 4, I will state and prove the main results about the homogeneous weight enumerators of linear codes over Galois rings, and in section 5, I will prove that the result in the main theorem is best possible. In the last section, I will talk about more generalized weights, the Hamming weights, and other extensions of the Lee weight.

2.1 Early Results

My interest in weight enumerators of linear codes over Galois rings started with the Lee weight enumerators of linear codes over $\mathbb{Z}_4$ after reading about the work of Sloane, Calderbank, et al. in [2]. In view of Wilson's theorem that I stated above, I wanted to know the power of 2 that would divide the number of codewords in a linear code over $\mathbb{Z}_4$ that have Lee weights in a particular congruence class modulo 4. Recall from Chapter 1 that the number of codewords in C that is in the congruence class i modulo 4 is denoted by $N_C(i,4)$.

Suppose that C is a linear code over $\mathbb{Z}_4$ of type $(4)^k$. Then applying Wilson's Theorem 2.1, we see that

$$N_C(i,4) \equiv 0 \pmod{2^{\lfloor \frac{k-2}{2} \rfloor}}, \qquad i = 0,1,2,3. \tag{2.1}$$

My initial goal was to see whether or not I could improve on this. To this extent, I did some experiments with randomly generated linear codes over $\mathbb{Z}_4$. For example, in one such experiment, I looked at 500 randomly generated linear $\mathbb{Z}_4$-codes of type $(4)^6$, and I looked at the common divisor of $N_C(i,4)$'s for $i = 0,1,2,3$. According to (2.1), this common divisor should be $2^2 = 4$. But, at the end of the experiment, I saw that
in 217 of the codes, the common divisor of $N_C(i,4)'s$ was 32,
in 133 of the codes, the common divisor of $N_C(i,4)'s$ was 64,
in 15 of the codes, the common divisor of $N_C(i,4)'s$ was 128,
in 134 of the codes, the common divisor of $N_C(i,4)'s$ was 1024,
and in 1 of these codes, the common divisor of $N_C(i,4)'s$ was 2048,

which made it seem that the best possible result could be much higher than was given by (2.1). I then conjectured and proved the following theorem, which was the first result I obtained:

Theorem 2.3. *Suppose that C is a linear code over $\mathbb{Z}_4$ of type $(4)^k$. Then*

$$N_C(i,4) \equiv 0 \pmod{2^{k-1}}, \qquad i = 0,1,2,3,$$

and this is the best possible result.

The proof involved some elementary counting methods that are not relevant to the rest of the work here and so it will be omitted here.

I then extended this result to $N_C(i,2^e)$ by imitating the proof of Wilson's Theorem 2.1, and also by proving the following lemma:

Lemma 2.4. *Let $\mathbf{A} \subseteq \mathbb{Z}_4^j$ be a coset of a subgroup of $\mathbb{Z}_4^j$, with*

$$|\mathbf{A}| = 2^{2j-r},\ r \leq j.$$

Then for any such r, the sum

$$S_A := \sum_{(b_1,b_2,\ldots,b_j)\in\mathbf{A}} \binom{\phi(b_1)}{i_1}\binom{\phi(b_2)}{i_2}\cdots\binom{\phi(b_j)}{i_j}$$

is divisible by 2^{j-r}. Here, $i_1, i_2, \ldots, i_j$ are fixed integers with $0 \leq i_\ell \leq 2$ with

$$i_1 + i_2 + \cdots + i_j = j,$$

and ϕ denotes the Lee weight in $\mathbb{Z}_4$.

The extended result that I proved was the following:

Theorem 2.5. *Suppose that C is a linear code over $\mathbb{Z}_4$ of type $(4)^k$, then*

$$N_C(i,2^e) \equiv 0 \pmod{2^q}, \qquad i = 0,1,\ldots,2^e-1$$

where

$$q = \left\lfloor \frac{k - 2^{e-2}}{2^{e-2}} \right\rfloor,$$

and this is the best possible result.

After these preliminary results, I finally came up with a method to extend all these results to linear codes over $\mathbb{Z}_4$ of type $(4)^{k_1}(2)^{k_2}$, and this method proved to be useful in extending the result to other rings as well. Recall that a linear code over $\mathbb{Z}_4$ is said to be of type $(4)^{k_1}(2)^{k_2}$ if it is permutationally equivalent to a code with generating matrix

$$G = \begin{bmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2C \end{bmatrix} \tag{2.2}$$

where A and C are $\mathbb{Z}_2$-matrices, and B is a $\mathbb{Z}_4$-matrix. The most general result for linear codes over $\mathbb{Z}_4$ was then the following:

Theorem 2.6. *Suppose C is a linear code over $\mathbb{Z}_4$ of type $(4)^{k_1}(2)^{k_2}$. If $N_C(i, 2^e)$ denotes the number of codewords in C that have Lee weights congruent to i modulo 2^e, then*

$$N_C(i, 2^e) \equiv 0 \pmod{2^q}, \qquad i = 0, 1, \ldots, 2^e - 1$$

where

$$q = \max\left\{0, \left\lfloor \frac{k_1 + k_2 - 2^{e-2}}{2^{e-2}} \right\rfloor\right\}$$

for all $e \geq 2$ and

$$q = 2k_1 + k_2 - 1$$

for $e = 1$.

This result turns out to be the best possible result and is certainly an improvement on the result in Theorem 2.1. The method applied in proving this theorem was useful in extending the result to linear codes over $\mathbb{Z}_{2^m}$, $\mathbb{Z}_{p^m}$ and finally to $GR(p^\ell, m)$. The proof will be given for the most general case, which is the Galois ring case.

2.2 Galois Rings

For the rest of this section, p denotes a prime, and ℓ and m positive integers. We will denote by $\mathbb{Z}_{p^\ell}$ the ring of integers modulo p^ℓ. $GR(p^\ell, m)$ will denote the Galois ring extension of $\mathbb{Z}_{p^\ell}$. The following introduction about Galois rings is taken from [14], [15], [16], which in turn was taken from [24]:

Let $\phi(x) \in \mathbb{Z}_{p^\ell}[x]$ be a basic irreducible polynomial of degree m that divides $x^{p^m-1} - 1$. Such a polynomial always exists by Hensel's lemma. Then, the Galois ring $GR(p^\ell, m)$ is defined as the quotient $\mathbb{Z}_{p^\ell}[x]/(\phi(x))$. If m_1 is a positive integer such that $m_1|m$, then $GR(p^\ell, m_1)$ is a subring of $GR(p^\ell, m)$. A very important property of Galois rings is that it is a finite chain ring and it also has a unique maximal ideal that is given by $(p) = pGR(p^\ell, m)$. The quotient field is

$$\frac{GR(p^\ell, m)}{pGR(p^\ell, m)} \simeq F_{p^m}. \tag{2.3}$$

All the ideals of $GR(p^\ell, m)$ can be ordered as

$$\{0\} = p^\ell GR(p^\ell, m) \subset p^{\ell-1} GR(p^\ell, m) \subset \cdots \subset pGR(p^\ell, m) \subset GR(p^\ell, m). \tag{2.4}$$

The Abelian group $GR^*(p^\ell, m)$ is a direct product of two groups H_1 and H_2 where H_1 is cyclic of order $p^m - 1$ and H_2 is of order $p^{(\ell-1)m}$. Suppose $H_1 = \{1, \xi, \xi^2, \ldots, \xi^{p^m-2}\}$. Then we introduce a special set called the *Teichmuller set* as

$$T_m = H_1 \cup \{0\} = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^m-2}\},$$

which forms a set of coset representatives of $GR(p^\ell, m)$ modulo $pGR(p^\ell, m)$. So, every element $u \in GR(p^\ell, m)$ can be uniquely expressed as

$$u = u_0 + pu_1 + \cdots + p^{\ell-1} u_{\ell-1} \tag{2.5}$$

where $u_0, u_1, \ldots, u_{\ell-1} \in T_m$.

We define the Frobenius automorphism $\psi : GR(p^\ell, m) \to GR(p^\ell, m)$ such that for

$u = u_0 + pu_1 + \cdots + p^{\ell-1}u_{\ell-1} \in GR(p^\ell, m)$ we have

$$\psi(u) = u_0^p + pu_1^p + \cdots + p^{\ell-1}u_{\ell-1}^p.$$

Note that ψ is an automorphism of order m. This enables us to introduce the trace operator on $GR(p^\ell, m)$:

$$\mathrm{Tr}(u) = u + \psi(u) + \psi^2(u) + \cdots + \psi^{m-1}(u). \tag{2.6}$$

Then the trace function Tr, defines a $\mathbb{Z}_{p^\ell}$-linear function from $GR(p^\ell, m)$ to $\mathbb{Z}_{p^\ell}$.

2.3 Linear Codes over Galois Rings and the Homogeneous Weight

A linear code C over the Galois ring $GR(p^\ell, m)$ of length n is a $GR(p^\ell, m)$-submodule of $GR(p^\ell, m)^n$. The following theorem from [17] helps us understand the question of type and dimension for linear codes over Galois rings:

Theorem 2.7. (Huffman, [17]) *A $GR(p^\ell, m)$-linear code C is permutation-equivalent to a code with generating matrix of the form*

$$G = \begin{bmatrix} I_{k_1} & A_1 & . & . & . & A_\ell \\ 0 & pI_{k_2} & pB_1 & . & . & pB_{\ell-1} \\ 0 & 0 & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & . & 0 & p^{\ell-1}I_{k_\ell} & p^{\ell-1}C \end{bmatrix}$$

where the matrices A_i's, B_j's and so on are matrices over $GR(p^\ell, m)$ and the columns are grouped into blocks of size $k_1, k_2, \ldots, k_\ell$. The size of C is $p^{m\alpha}$, where

$$\alpha = \sum_{i=1}^{\ell} k_i(\ell + 1 - i).$$

In this case, we say that C is of type

$$(p^{\ell m})^{k_1}(p^{(\ell-1)m})^{k_2}\dots(p^m)^{k_\ell}.$$

We next define the *homogeneous weight* for linear codes over Galois rings. Before the particular definition for the Galois rings, we will introduce the general definition of a homogeneous weight for a ring from [25]:

Definition 2.8. A real valued function w on the finite ring R is called a (left) *homogeneous weight* if $w(0) = 0$ and the following is true:

(H1) For all $x, y \in R$, $Rx = Ry$ implies $w(x) = w(y)$.

(H2) There exists a real number γ such that

$$\sum_{y\in Rx} w(y) = \gamma|Rx|, \qquad \text{for all } x \in R\setminus\{0\}.$$

It turns out that, because of the ideal structure of the Galois rings, the homogeneous weight for the Galois rings is then the following which is obtained from [18]; some of the weight structure comes from the conditions **(H1)** and **(H2)** from above:

$$w_{\text{hom}}(x) := \begin{cases} 0 & \text{if } x = 0 \\ p^{m(\ell-1)} & \text{if } 0 \neq x \in p^{\ell-1}GR(p^\ell, m) \\ (p^m-1)p^{m(\ell-2)} & \text{otherwise.} \end{cases}$$

We naturally extend this definition to linear codes by letting, for $\overline{c} = (c_1, c_2, \dots, c_n) \in GR(p^\ell, m)^n$,

$$w_{\text{hom}}(\overline{c}) = \sum_{i=1}^{n} w_{\text{hom}}(c_i).$$

At this point we want to make the following remark to connect this weight with the Lee weight:

Remark 2.9. For $p = 2$, $m = 1$ and $\ell = 2$, we get the Galois ring to be $\mathbb{Z}_4$ and in that case, the definition of w_{hom} coincides with the definition of the Lee weight on $\mathbb{Z}_4$-codes. So, in this sense, we can view the homogeneous weight to be an extension of the Lee weight on

$\mathbb{Z}_4$. At the end of the chapter, we will talk about other possible ways of extending the Lee weight.

Remark 2.9 brings up the question as to why this particular weight is used for the Galois rings. The answer comes from [18] in the form of the following theorem which relates the homogeneous weights to the exponential sums:

Theorem 2.10. (Voloch, [18]) *For any $x \in GR(p^\ell, m)$ we have*

$$w_{\hom}(x) = (p^m - 1)p^{m(\ell-2)} - \frac{1}{p^m} \sum_{a \in U} \gamma^{\mathrm{Tr}(ax)}$$

where U is the group of units in $GR(p^\ell, m)$, Tr *is the trace function defined over the Galois rings from 2.2, and γ is a primitive p^ℓth root of unity.*

Several authors have used this connection of the homogeneous weights with the exponential sums to get results about linear codes over Galois rings. For some of these we refer to [8],[15], [18], [19].

We denote by $N_C^{\hom}(j, p^e)$, the number of codewords in C that have homogeneous weights congruent to j modulo p^e. Finally by $\nu_p(k)$, we will denote the highest power of a prime p that divides a non-negative integer k, i.e., the p-adic valuation of k, with the convention that $\nu_p(0) = \infty$.

2.4 The Main Results

In this section, we will state and prove the main results about the homogeneous weights modulo p^e of linear codes over Galois rings.

We introduce our main result for linear codes over $GR(p^\ell, m)$ of this chapter in the following theorem:

Theorem 2.11. *Suppose that C is a linear code over $GR(p^\ell, m)$ of type*

$$(p^{\ell m})^{k_1}(p^{(\ell-1)m})^{k_2} \cdots (p^m)^{k_\ell}.$$

Suppose, also, that $N_C^{\hom}(j,p^e)$ *denotes the number of codewords in* C *that have homogeneous weights congruent to* j *modulo* p^e*, then*

$$N_C^{\hom}(j,p^e) \equiv 0 \pmod{p^q}, \qquad j = 0,1,\ldots,p^e-1$$

where

$$q = \max\left\{0, \left\lfloor \frac{k_1+k_2+\cdots+k_\ell - p^{e-(\ell-1)m-1}}{(p-1)(p^{e-(\ell-1)m-1})} \right\rfloor\right\}$$

and $e \geq (\ell-1)m+1$.

Proof. Before proving the theorem, we note that, the homogeneous weight of every codeword in C is divisible by $p^{(\ell-2)m}$, and so, we can introduce a new weight function w' by letting

$$w'(x) = \frac{1}{p^{(\ell-2)m}} w_{\hom}(x), \qquad x \in GR(p^\ell,m). \tag{2.7}$$

Then we can write this new weight as:

$$w'(x) := \begin{cases} 0 & \text{if } x = 0 \\ p^m & \text{if } 0 \neq x \in p^{\ell-1}GR(p^\ell,m) \\ (p^m-1) & \text{otherwise.} \end{cases}$$

Now, suppose that $N'_C(j,p^e)$ denotes the number of codewords in C that have the w'-weights congruent to j modulo p^e, then, we see that

$$N_C^{\hom}(j,p^e) = N'_C(j/p^{(\ell-2)m}, p^{e-(\ell-2)m}). \tag{2.8}$$

So, it is enough to prove the result for $N'_C(j,p^e)$ first and then we will use (2.8) to extend it to $N_C^{\hom}(j,p^e)$.

Suppose that the code C has a generating matrix of the form that appears in Theorem 2.7 above, and let

$$\{\overline{c_1},\ldots,\overline{c}_{k_1},\overline{b}_1,\ldots,\overline{b}_{k_2},\ldots,\overline{a}_1,\ldots,\overline{a}_{k_\ell}\}$$

be the rows of the matrix, i.e., the generators of C. So, $\overline{c}_i$'s are $GR(p^\ell,m)$-independent,

and $\{p\overline{c}_i, \overline{b}_j | i, j\}$ are independent in $pGR(p^\ell, m)$ and so on and finally

$$\left\{p^{\ell-1}\overline{c}_i, p^{\ell-2}\overline{b}_j, \ldots, \overline{a}_k \;\middle|\; i, j, \ldots, k\right\}$$

are independent in $p^{\ell-1}GR(p^\ell, m)$. Let $\tilde{C}$ be the linear code over $GR(p^\ell, m)$ that is generated by

$$\left\{p^{\ell-1}\overline{c}_1, \ldots, p^{\ell-1}\overline{c}_{k_1}, p^{\ell-2}\overline{b}_1, \ldots, p^{\ell-2}\overline{b}_{k_2}, \ldots, \overline{a}_1, \ldots, \overline{a}_{k_m}\right\}.$$

Then, we note that $\tilde{C}$ is a linear code over $p^{\ell-1}GR(p^\ell, m)$ and is $(k_1 + k_2 + \cdots + k_\ell)$-dimensional by the type of C. We also note that, if w_{H} denotes the Hamming weight, then we have

$$w'(\overline{c}) = p^m w_{\mathrm{H}}(\overline{c}), \qquad \forall \overline{c} \in \tilde{C}. \tag{2.9}$$

But this means that, if $N_C^{\mathrm{H}}(j, p^e)$ denotes the number of codewords in C that have their Hamming weights congruent to j modulo p^e, then we have

$$N'_{\tilde{C}}(j, p^e) = N_{\tilde{C}}^{\mathrm{H}}(j/p^m, p^{e-m}), \tag{2.10}$$

for all $j = 0, p^m, \ldots, p^e - p^m$. But note that applying Theorem 2.1 to $\tilde{C}$ with the Hamming weight gives us

$$\nu_p\big(N_{\tilde{C}}^{\mathrm{H}}(j/p^m, p^{e-m})\big) \geq \left\lfloor \frac{k_1 + k_2 + \cdots + k_\ell - p^{e-m-1}}{(p-1)p^{e-m-1}} \right\rfloor$$

for all j and $e \geq m + 1$, putting this into (2.10) gives us

$$\nu_p\big(N'_{\tilde{C}}(j, p^e)\big) \geq \left\lfloor \frac{k_1 + k_2 + \cdots + k_\ell - p^{e-m-1}}{(p-1)p^{e-m-1}} \right\rfloor \tag{2.11}$$

for all j and $e \geq m + 1$. Since the result in Theorem 2.1 is actually true for the cosets of linear codes as well, we see that we actually have

$$\nu_p\big(N'_{\overline{a}+\tilde{C}}(j, p^e)\big) \geq \left\lfloor \frac{k_1 + k_2 + \cdots + k_\ell - p^{e-m-1}}{(p-1)p^{e-m-1}} \right\rfloor \tag{2.12}$$

as well, where $\overline{a} \in \left(p^{\ell-1}GR(p^\ell, m)\right)^n$.

Now, by the choice of $\tilde{C}$, we see that C can be written as the union of a finite number of cosets of $\tilde{C}$. We already have the result for $p^{\ell-1}GR(p^\ell, m)$-cosets of $\tilde{C}$. So, now let $\overline{a} \in GR(p^\ell, m)^n$ be any codeword and suppose that we are looking at the coset

$$A = \overline{a} + \tilde{C}.$$

We will apply induction on r, the number of coordinates in $\overline{a}$ that are in $GR(p^\ell, m) \setminus p^{\ell-1}GR(p^\ell, m)$.

If $r = 0$, then the result is proved by (2.12).

Now, suppose the result in (2.12) is proven for all cosets that have up to $r-1$ coordinates in $GR(p^\ell, m) \setminus p^{\ell-1}GR(p^\ell, m)$ and suppose that $\overline{a}$ has r such coordinates. Without loss of generality we might assume that $\overline{a}$ starts with such a coordinate, and since $w'(x+y) = p^m - 1$ for all $x \in GR(p^\ell, m) \setminus p^{\ell-1}GR(p^\ell, m)$ and $y \in p^{\ell-1}GR(p^\ell, m)$ we can assume that $\overline{a}$ starts with 1. So we can write

$$A = \overline{a} + \tilde{C} = 1\overline{0} + \overline{b} + \tilde{C} = 1\overline{0} + B$$

where $B = \overline{b} + \tilde{C}$ is a coset of $\tilde{C}$ with $\overline{b}$ starting with 0 and $\overline{b}$ having $r-1$ coordinates from $GR(p^\ell, m) \setminus p^{\ell-1}GR(p^\ell, m)$. Since

$$w'(1 + p^{\ell-1}x) = p^m - 1$$

for all $x \in GR(p^\ell, m)$ we see that

$$N'_A(j, p^e) = N'_{\dot{B}}(j - p^m + 1, p^e), \tag{2.13}$$

for all $j = 0, 1, \ldots, p^e - 1$, where $\dot{B}$ is B with its first coordinate deleted. But notice that

$$\dot{B} = \dot{\overline{b}} + \dot{\tilde{C}}$$

with $\dot{\tilde{C}}$ denoting, in the same way, $\tilde{C}$ with its first coordinate deleted. Now, we can apply the induction hypothesis to $\dot{B}$ because we might still assume that $\dot{B}$ is of length n by just adding a zero coordinate to it. Note that, because of the type of the generating matrix that $\tilde{C}$ has, $\dot{\tilde{C}}$ is either still $(k_1+k_2+\cdots+k_\ell)$-dimensional or p^m copies of a $(k_1+k_2+\cdots+k_\ell-1)$-dimensional code. So, applying the induction hypothesis and using (2.13), we get

$$\nu_p\big(N'_A(j,p^e)\big) \geq \left\lfloor \frac{k_1+k_2+\cdots+k_\ell-p^{e-m-1}}{(p-1)p^{e-m-1}} \right\rfloor$$

or

$$\nu_p\big(N'_A(j,p^e)\big) \geq m+\left\lfloor \frac{k_1+k_2+\cdots+k_\ell-1-p^{e-m-1}}{(p-1)p^{e-m-1}} \right\rfloor.$$

But since the latter is greater than or equal to the former whenever $e \geq m+1$, and p is a prime, we see that, we get

$$\nu_p\big(N'_A(j,p^e)\big) \geq \left\lfloor \frac{k_1+k_2+\cdots+k_\ell-p^{e-m-1}}{(p-1)p^{e-m-1}} \right\rfloor \tag{2.14}$$

for all j and $e \geq m+1$ where A is any coset of $\tilde{C}$. But since the original code C is just a union of a finite number of cosets of $\tilde{C}$, the result of the theorem now follows easily from (2.14) and (2.8). □

We used the fact that $e \geq (\ell-1)m+1$ in the latter parts of the proof of the main theorem. Since every weight is divisible by $p^{(\ell-2)m}$ because of the structure of the homogeneous weight, we still have to figure out what happens when we have $(\ell-2)m+1 \leq e \leq (\ell-1)m$. For the remaining part of this section, we will let C be a linear code of the same type as in Theorem 2.11, and $\tilde{C}$ be the same code as was defined in the proof above. We first note that

$$w_{\text{hom}}(\overline{a}+\overline{c}) \equiv w_{\text{hom}}(\overline{a}) \pmod{p^e} \tag{2.15}$$

for all $\overline{c} \in \tilde{C}$, $\overline{a} \in \big(GR(p^\ell,m)\big)^n$ when $(\ell-2)m+1 \leq e \leq (\ell-1)m$. This implies that we have the following quick corollary for this case:

Corollary 2.12. *With C being the same as in Theorem 2.11, we have*

$$N_C^{\text{hom}}(j, p^e) \equiv 0 \pmod{p^{m(k_1+k_2+\cdots+k_\ell)}}$$

for all j, and $(\ell-2)m+1 \le e \le (\ell-1)m$.

It turns out however that we have a better result than Corollary 2.12 and we can give the result in the following theorem:

Theorem 2.13. *Suppose that C is a linear code over $GR(p^\ell, m)$ of type*

$$(p^{\ell m})^{k_1}(p^{(\ell-1)m})^{k_2}\cdots(p^m)^{k_\ell}.$$

Then, for $(\ell-2)m+1 \le e \le (\ell-1)m$, we have

$$N_C^{\text{hom}}(j, p^e) \equiv 0 \pmod{p^q}, \qquad j = 0, 1, \ldots, p^e - 1$$

where

$$q = m(k_1+k_2+\cdots+k_\ell) + \left\lfloor \frac{k_1+k_2+\cdots+k_{\ell-1}-p^{e-(\ell-2)m-1}}{(p-1)(p^{e-(\ell-2)m-1})} \right\rfloor.$$

Proof. We will again replace w_{hom} by w' and $N_C^{\text{hom}}(j, p^e)$ by $N'_C(j, p^e)$ and when we do that, we will have replaced e by $e-(\ell-2)m$ and so we will assume that $1 \le e \le m$. Suppose C has the same generators as in the proof of Theorem 2.11, and let $\tilde{C}$ be the same code as was defined in the proof of the theorem. We know that

$$C = \bigcup_{\overline{a} \in S} (\overline{a} + \tilde{C}) \tag{2.16}$$

where S is the set that is defined as

$$S = \Big\{ \sum_{i=1}^{k_1} \alpha_i \overline{c}_i + \sum_{j=1}^{k_2} \beta_j \overline{b}_j + \cdots + \sum_{t=1}^{k_{\ell-1}} \gamma_t \overline{d}_t \;\Big|\; \alpha_i, \beta_j, \ldots, \gamma_t \Big\}$$

where

$$\alpha_i \in \big\{ u_0 + pu_1 + \cdots + p^{\ell-2}u_{\ell-2} \;\big|\; u_0, u_1, \ldots, u_{\ell-2} \in T_m \big\},$$

$$\beta_j \in \{v_0 + pv_1 + \cdots + p^{\ell-3}v_{\ell-3} \mid v_0, v_1, \ldots, v_{\ell-3} \in T_m\},$$

and so on and

$$\gamma_t \in \{w_0 \mid w_0 \in T_m\}$$

where T_m is the Teichmuller set defined in Section 2.2.

We see that, by (2.15), we have

$$N'_C(j, p^e) = p^{m(k_1+k_2+\cdots+k_\ell)} N'_S(j, p^e), \qquad 1 \le e \le m. \tag{2.17}$$

Now, suppose that we introduce a map μ on $GR(p^\ell, m)$ that reduces every element in $GR(p^\ell, m)$ modulo $p^{\ell-1}$. Suppose $R = \mu\big(GR(p^\ell, m)\big)$. Then $\mu(S)$ becomes a linear code over R and, furthermore we have

$$N'_S(j, p^e) = N^{\mathrm{H}}_{\mu(S)}(j/(p^m - 1), p^e) \tag{2.18}$$

where $N^{\mathrm{H}}_{\mu(S)}(i, p^e)$ denotes the number of codewords that are in $\mu(S)$ with Hamming weights congruent to i modulo p^e and $1 \le e \le m$. The equation (2.18) is true, because

$$w'(\overline{a}) \equiv (p^m - 1) w_{\mathrm{H}}(\mu(\overline{a})) \pmod{p^e}$$

for all $\overline{a} \in S$ and $1 \le e \le m$. Now applying the methods used in the proof of Theorem 2.11, one can however easily show that

$$\nu_p\big(N^{\mathrm{H}}_{\mu(S)}(i, p^e)\big) \ge \left\lfloor \frac{k_1 + k_2 + \cdots + k_{\ell-1} - p^{e-1}}{(p-1)p^{e-1}} \right\rfloor, \tag{2.19}$$

for all $i = 0, 1, \ldots, p^e - 1$. Now, the theorem follows from combining (2.8), (2.17),(2.18) and (2.19). □

2.5 The Result in the Main Theorem is Best Possible

One of the differences in the work that we have done in this chapter and the work done by Wilson in [1] is that we are trying to improve the results to the best possible extent, and in order to accomplish that, we need to show that the results that we obtained in section 2.4 are best possible. We will first give some preliminaries that will serve as tools for the rest of the section.

We will first make an observation about the general weight distributions of trivial block codes over groups. Suppose that G is a finite abelian group. Assume that a weight function w is defined on the elements of G, and that the weight of a word in G^k is the sum of the weight of the coordinates. Let $P_k(z)$ denote the weight distribution polynomial of G^k, that is,

$$P_k(z) = \sum_{(g_1,\ldots,g_k)\in G^k} z^{w(g_1)+w(g_2)+\cdots+w(g_k)}.$$

But then, this is the same as

$$\begin{aligned} P_k(z) &= \sum_{(g_1,\ldots,g_k)\in G^k} z^{w(g_1)+w(g_2)+\cdots+w(g_k)} \\ &= \sum_{g_1,g_2,\ldots,g_k\in G} z^{w(g_1)} z^{w(g_2)} \cdots z^{w(g_k)} \\ &= \Big(\sum_{g_1\in G} z^{w(g_1)}\Big)\cdot\Big(\sum_{g_2\in G} z^{w(g_2)}\Big)\cdot\cdots\cdot\Big(\sum_{g_k\in G} z^{w(g_k)}\Big) \\ &= \Big(\sum_{g\in G} z^{w(g)}\Big)^k. \end{aligned}$$

Similarly if G_1 and G_2 are two abelian groups with the same weight function w defined on them, we can write the weight distribution polynomial of the trivial block code $C = G_1^{k_1} G_2^{k_2}$

as

$$\begin{aligned} P_C(z) &= \sum_{(g_1,\ldots,g_{k_1},h_1,\ldots,h_{k_2})\in G_1^{k_1}G_2^{k_2}} z^{w(g_1)+\cdots+w(g_{k_1})+w(h_1)+\cdots+w(h_{k_2})} \\ &= \big(\sum_{g_1\in G_1} z^{w(g_1)}\big)\cdot\cdots\cdot\big(\sum_{g_{k_1}\in G_1} z^{w(g_{k_1})}\big)\cdot\big(\sum_{h_1\in G_2} z^{w(h_1)}\big)\cdot\cdots\cdot\big(\sum_{h_{k_2}\in G_2} z^{w(h_{k_2})}\big) \\ &= \big[\sum_{g\in G_1} z^{w(g)}\big]^{k_1}\cdot\big[\sum_{h\in G_2} z^{w(h)}\big]^{k_2}. \end{aligned} \tag{2.20}$$

An obvious inductive argument then gives us the following useful lemma:

Lemma 2.14. *Suppose, $G_1, G_2, \ldots, G_r$ are finite abelian groups with a weight function w defined on them and suppose*

$$C = G_1^{k_1}G_2^{k_2}\cdots G_r^{k_r}$$

is the trivial block code. If $P_C(z)$ denotes the weight enumerator of C, we have

$$P_C(z) = \big[\sum_{g\in G_1} z^{w(g)}\big]^{k_1}\cdot\big[\sum_{h\in G_2} z^{w(h)}\big]^{k_2}\cdot\cdots\cdot\big[\sum_{s\in G_r} z^{w(s)}\big]^{k_r}.$$

The next observation will be a sort of modification on Theorem 2.2 in the form of the following corollary:

Corollary 2.15. *Suppose*

$$\big(1+(p-1)x^{p^{(\ell-1)m}}\big)^k \equiv A_0 + A_1x + \cdots + A_{p^e-1}x^{p^e-1} \pmod{x^{p^e}-1},$$

then

$$\min\Big\{\nu_p(A_i)\Big|i=0,1,\ldots,p^e-1\Big\} = \Big\lfloor\frac{k-p^{e-(\ell-1)m-1}}{(p-1)p^{e-(\ell-1)m-1}}\Big\rfloor$$

for $e \geq (\ell-1)m+1$.

Proof. Note that, in the equation above, $A_i = 0$ when $i \neq 0 \pmod{p^{(\ell-1)m}}$. So, we can make the substitution of $y = x^{p^{(\ell-1)m}}$. Then the above equation would turn into

$$\big(1+(p-1)y\big)^k \equiv B_0 + B_1y + \cdots + B_{p^{e-(\ell-1)m}-1}y^{p^{e-(\ell-1)m}-1} \pmod{y^{p^{e-(\ell-1)m}}-1} \tag{2.21}$$

with

$$\min\Big\{\nu_p(A_i)\big|i=0,1,\ldots,p^e-1\Big\}=\min\Big\{\nu_p(B_j)\big|j=0,1,\ldots,p^{e-(\ell-1)m}-1\Big\}.$$

Now, the result follows by applying Theorem 2.2 directly to (2.21).

□

After these initial observations, we are ready to prove that the result in the main theorem proved in the previous section is best possible.

Theorem 2.16. *Let*

$$C=\big(GR(p^\ell,m)\big)^{k_1}\times\big(pGR(p^\ell,m)\big)^{k_2}\times\cdots\times\big(p^{\ell-1}GR(p^\ell,m)\big)^{k_\ell} \tag{2.22}$$

be the trivial block code over $GR(p^\ell,m)$ of type

$$(p^{\ell m})^{k_1}(p^{(\ell-1)m})^{k_2}\ldots(p^m)^{k_\ell}.$$

Then

$$\min\Big\{\nu_p\big(N_C^{\hom}(j,p^e)\big)\big|j=0,1,\ldots,p^e-1\Big\}=\left\lfloor\frac{k_1+k_2+\cdots+k_\ell-p^{e-(\ell-1)m-1}}{(p-1)p^{e-(\ell-1)m-1}}\right\rfloor \tag{2.23}$$

for all $e\geq(\ell-1)m+1$ except in the case when $e=\ell, m=1, p=2, k_\ell\neq 0$ and $k_1+k_2+\cdots+k_{\ell-1}>1$.

Proof. Let, $P_C(z)$ be the homogeneous weight distribution of C. Then by Lemma 2.14, we see that

$$\begin{aligned}P_C(z)=&\Big[1+(p^{\ell m}-p^m)z^{(p^m-1)p^{(\ell-2)m}}+(p^m-1)z^{p^{(\ell-1)m}}\Big]^{k_1}\cdot\\&\Big[1+(p^{(\ell-1)m}-p^m)z^{(p^m-1)p^{(\ell-2)m}}+(p^m-1)z^{p^{(\ell-1)m}}\Big]^{k_2}\cdot\cdots\cdot\Big[1+(p^m-1)z^{p^{(\ell-1)m}}\Big]^{k_\ell}.\end{aligned} \tag{2.24}$$

Now, notice that we can write, by binomial expansions,

$$P_C(z) = \Big[1 + (p^m - 1)z^{p^{(\ell-1)m}}\Big]^{k_1+k_2+\cdots+k_\ell} + p^m F_1\Big[1 + (p^m - 1)z^{p^{(\ell-1)m}}\Big]^{k_1+k_2+\cdots+k_\ell-1} + p^{2m} F_2\Big[1 + (p^m - 1)z^{p^{(\ell-1)m}}\Big]^{k_1+k_2+\cdots+k_\ell-2} + \ldots \quad (2.25)$$

where F_i are polynomials with integer coefficients. But now by Corollary 2.15, we know that the coefficients of

$$\big(1 + (p^m - 1)z^{p^{(\ell-1)m}}\big)^k$$

modulo $z^{p^e} - 1$ are strictly divisible by p^q where

$$q = \left\lfloor \frac{k - p^{e-(\ell-1)m-1}}{(p-1)p^{e-(\ell-1)m-1}} \right\rfloor. \quad (2.26)$$

But now, looking at (2.25), since we have

$$jm + \left\lfloor \frac{k_1 + k_2 + \cdots + k_\ell - j - p^{e-(\ell-1)m-1}}{(p-1)p^{e-(\ell-1)m-1}} \right\rfloor > \left\lfloor \frac{k_1 + k_2 + \cdots + k_\ell - p^{e-(\ell-1)m-1}}{(p-1)p^{e-(\ell-1)m-1}} \right\rfloor \quad (2.27)$$

for all $j \geq 1$ and for all p and $e \geq (\ell-1)m + 1$ except when $p = 2, m = 1, e = \ell$, we get

$$\min\Big\{\nu_p\big(N_C^{hom}(j, p^e)\big) \,\big|\, j = 0, 1, \ldots, p^e - 1\Big\} = \max\left\{0, \left\lfloor \frac{k_1 + k_2 + \cdots + k_\ell - p^{e-(\ell-1)m-1}}{(p-1)p^{e-(\ell-1)m-1}} \right\rfloor\right\} \quad (2.28)$$

in this case. □

What Theorem 2.16 accomplishes is that it proves that the result in Theorem 2.11 is best possible in all the cases except possibly in the case when $e = \ell, p = 2, m = 1$.

To see that the result in Theorem 2.13 is best possible, i.e., the case when $(\ell-2)m+1 \leq e \leq (\ell-1)m$, we look at (2.24), and we see that

$$P_C(z) \equiv p^{m(k_1+k_2+\cdots+k_\ell)}\big(1 + (p^{(\ell-1)m} - 1)z^{(p^m-1)p^{(\ell-2)m}}\big)^{k_1} \times \cdots \times \big(1 + (p^m - 1)z^{(p^m-1)p^{(\ell-2)m}}\big)^{k_{\ell-1}} \pmod{z^{p^e} - 1}.$$

But now, applying Corollary 2.15 in the same way we applied it above we can easily see that if

$$P_C(z)/p^{m(k_1+k_2+\cdots+k_\ell)} \equiv P_0 + P_1 z + \cdots + P_{p^e-1} z^{p^e-1} \pmod{z^{p^e}-1}, \tag{2.29}$$

then

$$\min\left\{ \nu_p(P_i) \;\middle|\; i = 0, 1, \ldots, p^e - 1 \right\} = \left\lfloor \frac{k_1 + k_2 + \cdots + k_{\ell-1} - p^{e-(\ell-2)m-1}}{(p-1)p^{e-(\ell-2)m-1}} \right\rfloor,$$

which means that the result in Theorem 2.13 is best possible. So the only case we haven't looked at so far is the case when $e = \ell, m = 1, p = 2, k_\ell \neq 0$, and $k_1 + \cdots + k_{\ell-1} > 1$.

The case when $e = \ell, p = 2, m = 1, k_\ell \neq 0$, and $k_1 + \cdots + k_{\ell-1} > 1$:
In this case, we are in the ring $\mathbb{Z}_{2^\ell}$. Let's first show that the trivial block code doesn't work in this case:

Lemma 2.17. *If $e = \ell, k_\ell \neq 0$, and $k_1 + \cdots + k_{\ell-1} > 1$, then*

$$C = (\mathbb{Z}_{2^\ell})^{k_1} \times (2\mathbb{Z}_{2^\ell})^{k_2} \times \cdots \times (2^{\ell-1}\mathbb{Z}_{2^\ell})^{k_\ell}$$

doesn't give us the best result for Theorem 2.11.

Proof. If $k_\ell \neq 0$, then we can write

$$C = C_1 0 \cup C_1 2^{\ell-1}$$

where

$$C_1 = (\mathbb{Z}_{2^\ell})^{k_1} \times (2\mathbb{Z}_{2^\ell})^{k_2} \times \cdots \times (2^{\ell-1}\mathbb{Z}_{2^\ell})^{k_\ell - 1}.$$

But then we have

$$N_C^{\hom}(i, 2^\ell) = N_{C_1}^{\hom}(i, 2^\ell) + N_{C_1}^{\hom}(i - 2^{\ell-1}, 2^\ell) = N_{C_1}^{\hom}(i, 2^{\ell-1}). \tag{2.30}$$

However, by Theorem 2.13, we have

$$N_C^{\hom}(i, 2^\ell) = N_{C_1}^{\hom}(i, 2^{\ell-1}) \equiv 0 \pmod{2^{2(k_1+k_2+\cdots+k_{\ell-1})+k_\ell-2}}. \tag{2.31}$$

But, since when $k_1 + k_2 + \cdots + k_{\ell-1} > 1$, we have

$$2(k_1 + k_2 + \cdots + k_{\ell-1}) + k_\ell - 2 > k_1 + k_2 + \cdots + k_\ell - 1,$$

we see that in this case we don't get the best possible result. □

So, how do we solve this problem? We will just make a slight modification. In this case, we will take

$$C = (\mathbb{Z}_{2^\ell})^{k_1} \times (2\mathbb{Z}_{2^\ell})^{k_2} \times \cdots \times (2^{\ell-2}\mathbb{Z}_{2^\ell})^{k_{\ell-1}} \times C_\ell$$

where C_ℓ is a $2^{\ell-1}\mathbb{Z}_{2^\ell}$-linear code generated by the generators

$$(\overline{0}_{k_1}, \ldots, \overline{0}_{k_{\ell-1}}, 2^{\ell-1}, 0, 0, \ldots, 0, 2^{\ell-1}), (\overline{0}_{k_1}, \ldots, \overline{0}_{k_{\ell-1}}, 0, 2^{\ell-1}, 0, \ldots, 0, 2^{\ell-1}), \ldots,$$
$$(\overline{0}_{k_1}, \ldots, \overline{0}_{k_{\ell-1}}, 0, 0, \ldots, 0, 2^{\ell-1}, 2^{\ell-1}).$$

Basically, we add another coordinate that is $2^{\ell-1}$ to the end of the usual generator that is $2^{\ell-1}e_{k_\ell}$. It is easy to observe that

$$w_{\hom}(\overline{c}) \equiv 0 \pmod{2^\ell}, \qquad \forall \overline{c} \in C_\ell. \tag{2.32}$$

This means that if $P_C(z)$ denotes the Homogeneous weight distribution of C modulo $z^{2^\ell} - 1$,

then we have

$$\begin{aligned}
P_C(z) &= 2^{k_\ell}\big(1+z^{2^{\ell-1}}+(2^\ell-2)z^{2^{\ell-2}}\big)^{k_1}\times \\
&\quad \times\big(1+z^{2^{\ell-1}}+(2^{\ell-1}-2)z^{2^{\ell-2}}\big)^{k_2}\times\cdots\times\big(1+z^{2^{\ell-1}}+2z^{2^{\ell-2}}\big)^{k_{\ell-1}} \\
&= 2^{k_\ell}\Big[\big(1-2z^{2^{\ell-2}}+z^{2^{\ell-1}}\big)+2^\ell z^{2^{\ell-2}}\Big]^{k_1}\times\cdots\times\Big[\big(1-2z^{2^{\ell-2}}+z^{2^{\ell-1}}\big)+4z^{2^{\ell-2}}\Big]^{k_{\ell-1}} \\
&= 2^{k_\ell}\big(1-2z^{2^{\ell-2}}+z^{2^{\ell-1}}\big)^{k_1+\cdots+k_{\ell-1}}+4\cdot 2^{k_\ell}B_1(z)\big(1-2z^{2^{\ell-2}}+z^{2^{\ell-1}}\big)^{k_1+\cdots+k_{\ell-1}-1}+ \\
&\quad 4^2\cdot 2^{k_\ell}B_2(z)\big(1-2z^{2^{\ell-2}}+z^{2^{\ell-1}}\big)^{k_1+k_2+\cdots+k_{\ell-1}-2}+\ldots \qquad (2.33)
\end{aligned}$$

where $B_i(z)$ are polynomials with integer coefficients. But, we know, from Corollary 2.15 that the coefficients of

$$\big(1-2z^{2^{\ell-2}}+z^{2^{\ell-1}}\big)^k=(1-z^{2^{\ell-2}})^{2k}$$

modulo $z^{2^\ell}-1$ are strictly divisible by 2^{k-1}. But, since

$$2j+(k_1+k_2+\cdots+k_{\ell-1}-j-1)>k_1+k_2+\cdots+k_{\ell-1}-1$$

for all positive j, we see that (2.33) gives us

$$\min\Big\{\nu_2\big(N_C^{\mathrm{hom}}(i,2^\ell)\big)\big|i=0,1,\ldots,2^\ell-1\Big\}=k_1+k_2+\cdots+k_\ell-1, \qquad (2.34)$$

which means that the result of Theorem 2.11 is best possible for the case when $p=2, m=1$ and $e=\ell$ as well.

We can summarize all we have done so far in this section in the following theorem:

Theorem 2.18. *The results in Theorem 2.11 and Theorem 2.13 that we obtained in Section 2.4 are best possible in all the cases.*

2.6 Concluding Remarks and Questions

The first observation that we make is that the result we obtained in the form of Theorem 2.11 and Theorem 2.13 is indeed a generalization of the result that we obtained earlier for the Lee weights of linear codes over $\mathbb{Z}_4$ in the form of Theorem 2.6 by letting $\ell=2, m=1, p=2$.

The results we obtained in Section 2.4 don't however generalize the case of the Hamming weight. In fact by applying the same methods that we applied in the proof of Theorem 2.11, we can extend these results to a slightly more generalized weight than the homogeneous weight. To this end, we will introduce the following weight for $GR(p^\ell, m)$:

$$w(x) := \begin{cases} 0 & \text{if } x = 0 \\ d_1 & \text{if } 0 \neq x \in p^{\ell-1}GR(p^\ell, m), \\ d_2 & \text{otherwise.} \end{cases}$$

We will introduce the restriction that $\nu_p(d_2) \leq \nu_p(d_1)$. It is obvious that this weight easily generalizes the homogeneous weight. But, even more interesting is that this weight generalizes the Hamming weight for Galois ring codes as well, whereas the original homogeneous weight didn't. We can then extend the results we obtained in Section 2.4 for the homogeneous weight enumerators of linear codes over Galois rings to the newly defined w-weight:

Theorem 2.19. *Suppose C is a linear code over $GR(p^\ell, m)$ of type*

$$(p^{\ell m})^{k_1}(p^{(\ell-1)m})^{k_2}\dots(p^m)^{k_\ell},$$

and suppose that $N_C^w(j, p^e)$ denotes the number of codewords in C that have w-weights congruent to j modulo p^e. Then we have

$$N_C^w(j, p^e) \equiv 0 \pmod{p^q}, \qquad j = 0, 1, \dots, p^e - 1$$

where

$$q = \max\left\{0, \left\lfloor \frac{k_1 + k_2 + \cdots + k_\ell - p^{e-\nu_p(d_1)-1}}{(p-1)p^{e-\nu_p(d_1)-1}} \right\rfloor\right\}$$

for all $e \geq \nu_p(d_1) + 1$, and

$$q = m(k_1 + \cdots + k_\ell) + \max\left\{0, \left\lfloor \frac{k_1 + k_2 + \cdots + k_{\ell-1} - p^{e-\nu_p(d_2)-1}}{(p-1)p^{e-\nu_p(d_2)-1}} \right\rfloor\right\}$$

for all $\nu_p(d_2) + 1 \leq e \leq \nu_p(d_1)$. Moreover, the result above is best possible.

As we said above, this new weight does generalize the Hamming weights for binary codes to the codes over Galois rings, so we will give the particular result about the Hamming weight case:

Corollary 2.20. *Suppose C is a linear code over $GR(p^\ell, m)$ of type*

$$(p^{\ell m})^{k_1}(p^{(\ell-1)m})^{k_2}\dots(p^m)^{k_\ell},$$

and suppose that $N_C^{\mathrm{H}}(j, p^e)$ denotes the number of codewords in C that have Hamming weights congruent to j modulo p^e. Then we have

$$N_C^{\mathrm{H}}(j, p^e) \equiv 0 \pmod{p^q}, \qquad j = 0, 1, \dots, p^e - 1$$

where

$$q = \max\left\{0, \left\lfloor \frac{k_1 + k_2 + \cdots + k_\ell - p^{e-1}}{(p-1)p^{e-1}} \right\rfloor\right\}$$

for all $e \geq 1$.

Note that this is a generalization of Corollary 1.5 that was a particular result of Pless about the Hamming weights modulo 4 of binary linear codes.

Comparing with the result in [1]:

As we stated at the beginning of the chapter, we want to improve on the result that Wilson obtained in [1], in particular Theorem 2.1. A good way of understanding the extent of the improvement that we have gotten would be to compare the power of p that divides $N_C^{\mathrm{hom}}(j, p^e)$'s by using Theorem 2.1, which was Wilson's result, and by using Theorem 2.11, which is our result:

Suppose that C is a linear code over $GR(p^\ell, m)$ of type

$$(p^{\ell m})^{k_1}(p^{(\ell-1)m})^{k_2}\dots(p^m)^{k_\ell}.$$

Then applying Wilson's Theorem 2.11 directly to the code C with the homogeneous weights, we see that

$$N_C^{\mathrm{hom}}(j, p^e) \equiv 0 \pmod{p^{q_1}}$$

where

$$q_1 = \left\lfloor \frac{k_1 + \frac{\ell-1}{\ell}k_2 + \cdots + \frac{2}{\ell}k_{\ell-1} + \frac{1}{\ell}k_\ell - p^{e-1}}{(p-1)p^{e-1}} \right\rfloor \tag{2.35}$$

whereas if we apply our result of Theorem 2.11 we see that

$$N_C^{\hom}(j, p^e) \equiv 0 \pmod{p^{q_2}}$$

where

$$q_2 = \left\lfloor \frac{k_1 + k_2 + \cdots + k_\ell - p^{e-(\ell-1)m-1}}{(p-1)(p^{e-(\ell-1)m-1})} \right\rfloor. \tag{2.36}$$

Comparing q_1 and q_2, and noting that q_2 is roughly $p^{(\ell-1)m}$ times q_1, we see that our result is a significant improvement to Wilson's in the particular case of homogeneous weights of linear codes over Galois rings when the type of the code is known. The reason for this improvement is because Wilson uses only the size of the code, whereas in our case we are using the type of the code, which obviously gives more information about the code than just the size. At this point, we want to make the following remark about how to find the type of a linear code:

Remark 2.21. We know that a linear code over a finite field is a vector space for which we could talk about the notion of the *dimension*. In our works so far, we have focused instead on linear codes over rings. A linear code over a ring R is an R-submodule of R^n. But this submodule doesn't have to be a free module, so we cannot talk about a dimension, but instead we talk about the type of the linear code. As an example of how to find the type of a code, we will look at a linear code over $\mathbb{Z}_{p^m}$. So, suppose that C is a linear code over $\mathbb{Z}_{p^m}$. Then C will be of type $(p^m)^{k_1}(p^{m-1})^{k_2}\ldots(p)^{k_m}$ for some non-negative integers $k_1, k_2, \ldots, k_m$. Given the code C, we want to find $k_1, k_2, \ldots, k_m$. Our algorithm is going to be a step-by-step process in which we will obtain the numbers $k_1, k_2, \ldots, k_m$ in order.

(1) Let $C_1 = p^{m-1}C$. Then C_1 is a linear code over $\{0, p^{m-1}, \ldots, (p-1)p^{m-1}\}$ of type $(p)^{k_1}$. So, the size of C_1 will directly give us the exponent k_1.

(2) Let $C_2 = p^{m-2}C$. Then C_2 is a linear code over $\{0, p^{m-2}, \ldots, p^m - p^{m-2}\}$ of type $(p^2)^{k_1}(p)^{k_2}$. So, we have

$$|C| = p^{2k_1+k_2}.$$

Since we already know k_1, we can find k_2 by just looking at the size of C_2.

It is obvious that continuing with this algorithm we will find the exact type of C after a finite number of steps.

An interesting thing to observe is that when we compare Corollary 2.20, which is our result for the Hamming weights, and Wilson's result of Theorem 2.1, which is about any weight function, we see that we get very similar results. In fact, comparing q_1 of (2.34) with q of Corollary 2.20, we see that q_1 and q are very close, in particular, if the code is of type $(p^{\ell m})^k$, then both results are the same. This brings the question to mind whether the Hamming weight is the *worst* weight function in the sense of the work done in this chapter. Certainly, when the code is of type $(p^{\ell m})^k$, we see that Hamming weight is clearly the worst weight because the result in Corollary 2.20 is best possible whereas the result in Theorem 2.1 is not.

Other Generalizations of the Lee Weight

As we saw above, the homogeneous weight defined for the Galois rings is in fact a generalization of the Lee weight defined on $\mathbb{Z}_4$-codes. This however is not the only way to extend the Lee weight to higher rings. In fact, a more natural way to extend the Lee weight to the ring $\mathbb{Z}_{2^m}$ for example would be to consider the Lee weight for $\mathbb{Z}_4$ to be the circular distance to 0, in that case a Lee extension to $\mathbb{Z}_{2^m}$ would be as follows:

$$w_{\text{Lee}}(x) := \begin{cases} x & \text{if } x \leq 2^{m-1}, \\ 2^m - x & \text{otherwise.} \end{cases}$$

In fact, Carlet, in his work [8], did consider this weight as an extension of the Lee weight, but then dismissed it in favor of the homogeneous weight because it didn't turn out to give interesting results. I guess that a strong reason why many authors favored the homogenous weight as the extension was because of its strong relation to the exponential sums (viz. Theorem 2.9) and because of the extensive literature on exponential sums. So, a good question would be whether we could get interesting results in the sense of weights modulo prime powers for these other extensions. A good way to look at this question would be to see how *close* to Hamming weight they come; so the closer they are to the Hamming weight,

the worse the results obtained would be.

Another way to extend the Lee weight would be to look at the ideals and assign a weight to different ideals. So we could define a weight function w on $GR(p^\ell, m)$ and then we could say, let $w(0) = 0$ and $w(x) = d_i$ if $x \in p^{i-1}GR(p^\ell, m) \setminus p^i GR(p^\ell, m)$ for $i = 1, 2, \ldots, \ell$. In this case we would have exactly ℓ non-zero weights, in fact this would even generalize the homogeneous weight case. The methods that we applied in proving Theorem 2.11 however don't immediately apply to this kind of weight structure. So, we can't say how good a result we could obtain in this case.

Chapter 3

MacWilliams Identities for Linear Codes over Rings

The MacWilliams identity was first obtained as an identity that related the Hamming weight enumerator of a linear code over a finite field with that of its dual's. The following theorem from [6] and [20] illustrates this point:

Theorem 3.1. (MacWilliams, [6], [20]) *Let C be an $[n,k]$-code over $\mathbb{F}_q$ with weight enumerator $A(z)$ and let $B(z)$ be the weight enumerator of $C^{\perp}$. Then*

$$B(z) = q^{-k}(1+(q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right). \tag{3.1}$$

As the interest in codes over rings increased together with the notion of new weights, a natural question to ask was whether or not there existed analogues of Theorem 3.1 for the weight enumerators of these codes. The first step towards this goal was established in [2] by Sloane, Calderbank, et al. in which they introduced the notion of MacWilliams identities for the different weight enumerators of linear codes over $\mathbb{Z}_4$. Of interest among these were the notion of a *complete weight enumerator* and *symmetrized weight enumerator* for linear codes over $\mathbb{Z}_4$. With the help of MacWilliams identities for these weight enumerators, they were able to establish MacWilliams identities for the Hamming and Lee weight enumerators of linear codes over $\mathbb{Z}_4$.

Delsarte also considered the problem of MacWilliams identities in his work [5]; in his case he considered the general abelian group codes and he obtained MacWilliams identities for the Hamming weight enumerators of these codes.

In section 1, we will reiterate the results of Sloane, Calderbank, et al. about the MacWilliams identities for different weight enumerators of linear codes over $\mathbb{Z}_4$, and then we will resolve the question of existence of such an identity for the Euclidean weight enumerators of linear codes over $\mathbb{Z}_4$ by exhibiting a counter example.

In section 2, we will consider the general abelian group codes and we will prove a theorem about the MacWilliams identities for the complete weight enumerators of these codes.

In section 3, we will consider several rings and we will introduce new inner products that will give us linear codes as duals and that will also give us computational tools to obtain MacWilliams identities for the complete weight enumerators of linear codes over these rings.

In section 4, we will conclude with some remarks and some applications of these identities.

3.1 MacWilliams Identities for Euclidean Weight Enumerators of $\mathbb{Z}_4$-codes

We first recall the results of Sloane, Calderbank, et al. from [2], about the MacWilliams identities for linear codes over $\mathbb{Z}_4$. Suppose C is a linear code over $\mathbb{Z}_4$ and suppose that $C^{\perp}$ is the dual of C with respect to the Euclidean inner product modulo 4. Then

$$\mathrm{cwe}_C(W,X,Y,Z) = \sum_{a\in C} W^{n_0(a)}X^{n_1(a)}Y^{n_2(a)}Z^{n_3(a)} \tag{3.2}$$

where $n_j(a)$ is the number of coordinates in a that are congruent to j modulo 4. They defined the *symmetrized weight enumerator* of C, $\mathrm{swe}_C(W,X,Y)$ as

$$\mathrm{swe}_C(W,X,Y) = \mathrm{cwe}_C(W,X,Y,X). \tag{3.3}$$

They defined the *Lee Weight enumerator* of C as

$$\mathrm{Lee}_C(W,X) = \sum_{a\in C} W^{2n-w_{\mathrm{L}}(a)}X^{w_{\mathrm{L}}(a)} = \mathrm{swe}_C(W^2, WX, X^2) \tag{3.4}$$

and similarly, the Hamming weight enumerator was defined as

$$\mathrm{Ham}_C(W, X) = \mathrm{swe}_C(W, X, X). \tag{3.5}$$

Then the following analogous MacWilliams identities were obtained:

$$\mathrm{cwe}_{C^\perp}(W, X, Y, Z) = \\ \frac{1}{|C|}\mathrm{cwe}_C(W + X + Y + Z, W + iX - Y - iZ, W - X + Y - Z, W - iX - Y + iZ), \tag{3.6}$$

$$\mathrm{swe}_{C^\perp}(W, X, Y) = \frac{1}{|C|}\mathrm{swe}_C(W + 2X + Y, W - Y, W - 2X + Y), \tag{3.7}$$

$$\mathrm{Lee}_{C^\perp}(W, X) = \frac{1}{|C|}\mathrm{Lee}_C(W + X, W - X), \tag{3.8}$$

$$\mathrm{Ham}_{C^\perp}(W, X) = \frac{1}{|C|}\mathrm{Ham}_C(W + 3X, W - X). \tag{3.9}$$

Now, our aim is to see whether there is a similar MacWilliams identity like the ones above for the Euclidean weight enumerators of linear codes over $\mathbb{Z}_4$. Recall that the Euclidean weight w_{E} on $\mathbb{Z}_4$ is defined as

$$w_{\mathrm{E}}(0) = 0,\ w_{\mathrm{E}}(1) = w_{\mathrm{E}}(3) = 1,\ w_{\mathrm{E}}(2) = 2^2 = 4.$$

We can then define the Euclidean weight enumerator of a linear code C over $\mathbb{Z}_4$ as

$$\mathrm{Euc}_C(W, X) = \sum_{\overline{c} \in C} W^{4n - w_{\mathrm{E}}(\overline{c})} X^{w_{\mathrm{E}}(\overline{c})}. \tag{3.10}$$

Considering that

$$w_{\mathrm{E}}(\overline{c}) = n_1(\overline{c}) + n_3(\overline{c}) + 4n_2(\overline{c})$$

and that

$$n = n_0(\overline{c}) + n_1(\overline{c}) + n_2(\overline{c}) + n_3(\overline{c}),$$

putting these in (3.10) and using (3.2) and (3.3) we see that

$$\mathrm{Euc}_C(W,X) = \mathrm{cwe}_C(W^4, W^3X, X^4, W^3X) = \mathrm{swe}_C(W^4, W^3X, X^4). \tag{3.11}$$

Since MacWilliams identities exist for both the Hamming and the Lee weight enumerators of linear codes over $\mathbb{Z}_4$ in the form of (3.8) and (3.9), we naturally ask the same question for the Euclidean weight enumerators of linear codes over $\mathbb{Z}_4$. It turns out that no such identity exists for the Euclidean weight enumerators as we have a counter example. We will state the result in the form of the following theorem:

Theorem 3.2. *There exist linear codes C_1 and C_2 over $\mathbb{Z}_4$ such that*

$$\mathrm{Euc}_{C_1}(z) = \mathrm{Euc}_{C_2}(z)$$

but

$$\mathrm{Euc}_{C_1^\perp}(z) \neq \mathrm{Euc}_{C_2^\perp}(z).$$

Proof. The proof will be in the form of exhibiting an example of two such codes and calculating their Euclidean weight enumerators. We first note however that

$$\mathrm{Euc}_C(z) = \sum_{\bar{c}\in C} z^{w_{\mathrm{E}}(\bar{c})} = \mathrm{swe}_C(1, z, z^4). \tag{3.12}$$

Let

$$C_1 =< (102110010232323310103132303130), (012122330101323213010130121210) > \tag{3.13}$$

and

$$C_2 =< (102112230032101332323330123112), (010122130103123231030110123232) > \tag{3.14}$$

be two linear codes over $\mathbb{Z}_4$ of length 30, of size $4^2 = 16$. We first calculate their Euclidean

weight enumerators, and we see that

$$\mathrm{Euc}_{C_1}(z) = 1 + 2z^{37} + 2z^{41} + 2z^{44} + 2z^{45} + 2z^{48} + 2z^{49} + z^{52} + z^{64} + z^{68} \tag{3.15}$$

and

$$\mathrm{Euc}_{C_2}(z) = 1 + 2z^{37} + 2z^{41} + 2z^{44} + 2z^{45} + 2z^{48} + 2z^{49} + z^{52} + z^{64} + z^{68} \tag{3.16}$$

so that

$$\mathrm{Euc}_{C_1}(z) = \mathrm{Euc}_{C_2}(z). \tag{3.17}$$

Now, we need to calculate $\mathrm{Euc}_{C_1^\perp}(z)$ and $\mathrm{Euc}_{C_2^\perp}(z)$. But, notice that $C_1^\perp$ and $C_2^\perp$ are two linear codes over $\mathbb{Z}_4$ of size $4^{28} = 72057594037927936 > 7 \times 10^{16}$. Since these dual codes are so big in size, calculating their Euclidean weight enumerators present practical problems. We will calculate the Euclidean weight enumerators of the duals with a very simple method thanks to the identities we have for the symmetrized weight enumerators and the connection of the Euclidean weight enumerators with the symmetrized weight enumerators. So, by using (3.12) and (3.7), we see that

$$\mathrm{Euc}_{C^\perp}(z) = \mathrm{swe}_{C^\perp}(1, z, z^4) = \frac{1}{|C|}\mathrm{swe}_C(1 + 2z + z^4, 1 - z^4, 1 - 2z + z^4). \tag{3.18}$$

So in order to calculate $\mathrm{Euc}_{C_i^\perp}(z)$'s, all we need to do is to calculate the $\mathrm{swe}_{C_i}(W, X, Y)$'s, which is simple since $|C_i| = 16$, and then we will replace W by $1 + 2z + z^4$, X by $1 - z^4$ and Y by $1 - 2z + z^4$ in $\mathrm{swe}_{C_i}(W, X, Y)$ and divide the whole thing by 16.

Doing the replacement that we discussed above we see that

$$\mathrm{Euc}_{C_1^\perp}(z) = 1 + 4z + 86z^2 + 2036z^3 + 27627z^4 + 284782z^5 + 2377708z^6 + 16347588z^7 +$$
$$94342262z^8 + 464880164z^9 + 1980218040z^{10} + 7368253436z^{11} + 24208530074z^{12} +$$
$$71012429768z^{13} + 188046545636z^{14} + 454685931564z^{15} + 1015805935511z^{16} +$$
$$2120146461248z^{17} + 4170342704854z^{18} + 7780239010072z^{19} + 13838853631541z^{20} +$$
$$23579437100638z^{21} + 38631434684968z^{22} + 61037882494072z^{23} + 93259510341516z^{24} +$$
$$138141692522776z^{25} + 198754423575264z^{26} + 278171148477288z^{27} + 379340979921012z^{28} +$$
$$504858907125632z^{29} + 656429066099672z^{30} + 834513461551496z^{31} + 1038460479154001z^{32} +$$
$$1266305669090204z^{33} + 1514089055750494z^{34} + 1775990482137788z^{35} + 2045239387733099z^{36} +$$
$$2314171001268150z^{37} + 2573847080981220z^{38} + 2814871603243692z^{39} + 3028577613183130z^{40} +$$
$$3207345420856044z^{41} + 3344750078506968z^{42} + 3435702602280372z^{43} + 3476715824359798z^{44} +$$
$$3467259069419976z^{45} + 3409846523456236z^{46} + 3307239598474308z^{47} + 3162604975644207z^{48} +$$
$$2983349882069800z^{49} + 2778817634639326z^{50} + 2554551462107920z^{51} + 2316065303609069z^{52} +$$
$$2073682316787430z^{53} + 1835391661920368z^{54} + 1603095715951952z^{55} + 1381278557122792z^{56} +$$
$$1177300712038032z^{57} + 992250360511872z^{58} + 824378991716208z^{59} + 676604414460312z^{60} +$$
$$550350272053824z^{61} + 441801481745424z^{62} + 349419477646384z^{63} + 274044218802987z^{64} +$$
$$212840118547900z^{65} + 162467351970914z^{66} + 122685261377580z^{67} + 92199704580569z^{68} +$$
$$68096376678122z^{69} + 49437221567732z^{70} + 35880937163996z^{71} + 25733397440842z^{72} +$$
$$17961743846332z^{73} + 12524029711080z^{74} + 8747955634596z^{75} + 5895928830182z^{76} +$$
$$3918959742680z^{77} + 2661753922684z^{78} + 1748524880884z^{79} + 1101487834189z^{80} +$$
$$720587350448z^{81} + 466680325218z^{82} + 278946084440z^{83} + 172657254231z^{84} +$$
$$111268908090z^{85} + 63824738024z^{86} + 36451377848z^{87} + 23437352908z^{88} + 13219344088z^{89} +$$
$$6769316768z^{90} + 4286959272z^{91} + 2471178676z^{92} + 1114112064z^{93} + 665617048z^{94} +$$
$$410585544z^{95} + 165237507z^{96} + 85808932z^{97} + 59099242z^{98} + 22272676z^{99} + 8968529z^{100} +$$
$$7200626z^{101} + 2709180z^{102} + 717364z^{103} + 721254z^{104} + 297140z^{105} + 38536z^{106} +$$
$$55084z^{107} + 28490z^{108} + 1432z^{109} + 2868z^{110} + 2076z^{111} +$$
$$109z^{112} + 104z^{113} + 106z^{114} + 7z^{116} + 2z^{117}.$$

Similarly we get,

$$\mathrm{Euc}_{C_2^\perp} = 1 + 4z + 90z^2 + 2036z^3 + 27547z^4 + 284774z^5 + 2378292z^6 +$$
$$16347716z^7 + 94340982z^8 + 464879532z^9 + 1980211720z^{10} + 7368253052z^{11} +$$
$$24208573098z^{12} + 71012443312z^{13} + 188046488572z^{14} + 454685897772z^{15} +$$
$$1015805709975z^{16} + 2120146401112z^{17} + 4170343496026z^{18} + 7780239374616z^{19} +$$
$$13838853645781z^{20} + 23579436969070z^{21} + 38631431157656z^{22} + 61037880792952z^{23} +$$
$$93259514033292z^{24} + 138141694678536z^{25} + 198754431237152z^{26} + 278171152782952z^{27} +$$
$$379340964238804z^{28} + 504858897789936z^{29} + 656429059603304z^{30} + 834513456046472z^{31} +$$
$$1038460512419921z^{32} + 1266305691902252z^{33} + 1514089048651410z^{34} + 1775990482194108z^{35} +$$
$$2045239348026619z^{36} + 2314170966410462z^{37} + 2573847105371260z^{38} + 2814871615150124z^{39} +$$
$$3028577634068122z^{40} + 3207345452406852z^{41} + 3344750055627240z^{42} + 3435702583431476z^{43} +$$
$$3476715835220902z^{44} + 3467259060320000z^{45} + 3409846521506228z^{46} + 3307239607913540z^{47} +$$
$$3162604946830383z^{48} + 2983349864616432z^{49} + 2778817658602386z^{50} + 2554551471614736z^{51} +$$
$$2316065330415277z^{52} + 2073682346995270z^{53} + 1835391640368656z^{54} + 1603095697090384z^{55} +$$
$$1381278537374440z^{56} + 1177300684658992z^{57} + 992250365437568z^{58} + 824379003525488z^{59} +$$
$$676604429930968z^{60} + 550350290886368z^{61} + 441801487337328z^{62} + 349419477781552z^{63} +$$
$$274044208796971z^{64} + 212840107470108z^{65} + 162467345877678z^{66} + 122685255940140z^{67} +$$
$$92199707721641z^{68} + 68096381621682z^{69} + 49437224964588z^{70} + 35880941383772z^{71} +$$
$$25733398122570z^{72} + 17961742935924z^{73} + 12524028350808z^{74} + 8747953909540z^{75} +$$
$$5895927901270z^{76} + 3918959233968z^{77} + 2661754174884z^{78} + 1748525297652z^{79} +$$
$$1101488107341z^{80} + 720587720408z^{81} + 466680427822z^{82} + 278946051672z^{83} +$$
$$172657235447z^{84} + 111268845002z^{85} + 63824684248z^{86} + 36451358136z^{87} + 23437349068z^{88} +$$
$$13219334216z^{89} + 6769310048z^{90} + 4286962088z^{91} + 2471179796z^{92} + 1114112048z^{93} +$$
$$665622184z^{94} + 410589640z^{95} + 165238787z^{96} + 85811508z^{97} + 59100134z^{98} +$$
$$22271652z^{99} + 8967489z^{100} + 7199882z^{101} + 2708708z^{102} + 716980z^{103} +$$
$$721254z^{104} + 297244z^{105} + 38584z^{106} + 55212z^{107} + 28570z^{108} +$$
$$1440z^{109} + 2860z^{110} + 2076z^{111} + 109z^{112} + 96z^{113} + 102z^{114} + 7z^{116} + 2z^{117}.$$

That $\mathrm{Euc}_{C_1^\perp} \neq \mathrm{Euc}_{C_2^\perp}$ is obvious by looking at the coefficient of z^2 for example. But for completeness, we will actually calculate the difference:

$$\mathrm{Euc}_{C_2^\perp} - \mathrm{Euc}_{C_1^\perp} = 4z^2 - 80z^4 - 8z^5 + 584z^6 + 128z^7 - 1280z^8 - 632z^9 -$$
$$6320z^{10} - 384z^{11} + 43024z^{12} + 13544z^{13} - 57064z^{14} - 33792z^{15} - 225536z^{16} - 60136z^{17} +$$
$$791172z^{18} + 364544z^{19} + 14240z^{20} - 131568z^{21} - 3527312z^{22} - 1701120z^{23} + 3691776z^{24} +$$
$$2155760z^{25} + 7661888z^{26} + 4305664z^{27} - 15682208z^{28} - 9335696z^{29} - 6496368z^{30} -$$
$$5505024z^{31} + 33265920z^{32} + 22812048z^{33} - 7099084z^{34} + 56320z^{35} - 39706480z^{36} -$$
$$34857688z^{37} + 24390040z^{38} + 11906432z^{39} + 20884992z^{40} + 31550808z^{41} - 22879728z^{42} -$$
$$18848896z^{43} + 10861104z^{44} - 9099976z^{45} - 1950008z^{46} + 9439232z^{47} - 28813824z^{48} -$$
$$17453368z^{49} + 23963060z^{50} + 9506816z^{51} + 26806208z^{52} + 30207840z^{53} - 21551712z^{54} -$$
$$18861568z^{55} - 19748352z^{56} - 27379040z^{57} + 4925696z^{58} + 11809280z^{59} + 15470656z^{60} +$$
$$18832544z^{61} + 5591904z^{62} + 135168z^{63} - 10006016z^{64} - 11077792z^{65} - 6093236z^{66} -$$
$$5437440z^{67} + 3141072z^{68} + 4943560z^{69} + 3396856z^{70} + 4219776z^{71} + 681728z^{72} - 910408z^{73} -$$
$$1360272z^{74} - 1725056z^{75} - 928912z^{76} - 508712z^{77} + 252200z^{78} + 416768z^{79} + 273152z^{80} +$$
$$369960z^{81} + 102604z^{82} - 32768z^{83} - 18784z^{84} - 63088z^{85} - 53776z^{86} - 19712z^{87} - 3840z^{88} -$$
$$9872z^{89} - 6720z^{90} + 2816z^{91} + 1120z^{92} - 16z^{93} + 5136z^{94} + 4096z^{95} + 1280z^{96} + 2575z^{97} +$$
$$892z^{98} - 1024z^{99} - 1040z^{100} - 744z^{101} - 472z^{102} - 384z^{103} + 104z^{105} + 48z^{106} +$$
$$128z^{107} + 80z^{108} + 8z^{109} - 8z^{110} - 8z^{113} - 4z^{114}.$$

□

Note that Theorem 3.2 implies that we can't have a MacWilliams-like identity for the Euclidean weight enumerators of linear codes over $\mathbb{Z}_4$ unlike the Hamming and the Lee weight enumerators for which we have the identities (3.8) and (3.9).

3.2 MacWilliams Identities for Group Codes

In this section, we will consider abelian group codes and we will derive the Macwilliams identities for the complete weight enumerators and also Hamming weight enumerators of these codes. We first define an abelian group code:

Definition 3.3. Suppose G is an abelian group of order $q \geq 2$ and for an integer $n \geq 1$, we will consider the group G^n, the direct product of n copies of G. Then an *additive code* C of length n over G is just defined to be a subgroup of G^n.

A *weight* function w can be defined on such codes as usual, by assigning to each element of G a nonnegative integer, and letting the weight of a word be defined as the sum of the weights of the coordinates. A standard weight function is the *Hamming* weight, which assigns 1 to every nonzero element and zero to 0. A *weight enumerator* polynomial for C with respect to the weight w is the polynomial

$$W(z) = \sum_{\overline{c} \in C} z^{w(\overline{c})}. \tag{3.19}$$

Among the weight enumerators, an important one is the *complete weight enumerator* from which all the other weight enumerators can be derived:

Definition 3.4. The *complete weight enumerator* of C is the polynomial in q variables

$$\mathrm{cwe}_C(W_1, W_2, \ldots, W_q) = \sum_{\overline{c} \in C} \prod_{g_i \in G} W_i^{n_{g_i}(\overline{c})} \tag{3.20}$$

where $G = \{g_1, g_2, \ldots, g_q\}$ and $n_{g_i}(\overline{c})$ denotes the number of occurrences of g_i in $\overline{c}$.

Suppose now that the group G is of the form

$$G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r} \tag{3.21}$$

with

$$m_r \mid m_{r-1} \mid \ldots \mid m_1.$$

In particular, we might assume that

$$m_i = p_1^{e_{i1}} p_2^{e_{i2}} \dots p_k^{e_{ik}} \tag{3.22}$$

with $p_1 > p_2 > \cdots > p_k$ primes, and $e_{1j} \geq e_{2j} \geq \cdots \geq e_{rj} \geq 0$ for all $j = 1, 2, \dots, k$. We first define an inner product on G^n:

Definition 3.5. Define a symmetric function $< ., . >: G^n \times G^n \to Z_{m_1}$ such that

$$< (g_1, g_2, \dots, g_n), (h_1, h_2, \dots, h_n) >= \sum_{i=1}^{n} g_i * h_i \tag{3.23}$$

where

$$g_i * h_i = g_i(1)h_i(1) + \frac{m_1}{m_2} g_i(2)h_i(2) + \cdots + \frac{m_1}{m_r} g_i(r)h_i(r). \tag{3.24}$$

Here $g_i(j) \in \mathbb{Z}_{m_j}$ is the jth coordinate of g_i when it is written as an r-tuple in G.

Note that the inner product thus defined is symmetric and bilinear. It is a natural definition for an inner product, because if ξ is a primitive m_1^{st} root of unity over complex numbers then, ξ^{m_1/m_i} is a primitive m_i^{th} root of unity and hence a character of $\mathbb{Z}_{m_i}$.

Definition 3.6. Suppose C is an abelian group code over G defined above by (3.21) of length n. We define the *dual* C^* of C with respect to the inner product defined above in (3.23) and (3.24) as

$$C^* = \big\{ \overline{x} \in G^n \big| < \overline{x}, \overline{c} >= 0, \ \forall \overline{c} \in C \big\}. \tag{3.25}$$

We prove the following lemma for the inner product above that will be useful:

Lemma 3.7. *Suppose $(h_1, h_2, \dots, h_n) \in G^n$ is fixed. If*

$$< (g_1, g_2, \dots, g_n), (h_1, h_2, \dots, h_n) >= 0$$

for all $(g_1, g_2, \dots, g_n) \in G^n$, then $(h_1, h_2, \dots, h_n) = \overline{0}$, the zero vector in G^n.

Proof. By taking all but one of g_i's to be the zero element in G, we can reduce this to the

case $n = 1$. So, suppose $h \in G$ is fixed and that $< g, h >= 0$ for all $g \in G$. This means that

$$g * h = g(1)h(1) + \frac{m_1}{m_2}g(2)h(2) + \cdots + \frac{m_1}{m_r}g(r)h(r) = 0$$

for all $g \in G$ where $g = (g(1), \ldots, g(r))$ with $g(j) \in \mathbb{Z}_{m_j}$. Then take $g = (1, 0, \ldots, 0)$. We see that we get $h(1) = 0$ in $\mathbb{Z}_{m_1}$. Taking $g = (0, 1, 0, \ldots, 0)$ we see that $\frac{m_1}{m_2}h(2) = 0$ in $\mathbb{Z}_{m_1}$, which means that $h(2) = 0$ in $\mathbb{Z}_{m_2}$. Similarly it can be shown that $h(j) = 0$ in $\mathbb{Z}_{m_j}$ for $j = 1, 2, \ldots, r$ and so we get $h = 0$ in G. □

Remark 3.8. Lemma 3.7 implies that $\{0\}^* = G^n$ and $(G^n)^* = \{0\}$.

To prove a MacWilliams-like identity for the complete weight enumerators of abelian group codes, we first prove the following lemma:

Lemma 3.9. *Suppose H is a nontrivial subgroup of $\mathbb{Z}_{m_1}$ of order $s > 1$ and suppose ξ is a primitive m_1^{th} root of unity. Then we have*

$$\sum_{h \in H} \xi^h = 0.$$

Proof. Suppose $0 \neq h \in H$ is an element in H of order s. Then

$$H = \{0, h, 2h, \ldots, (s-1)h\}$$

with $sh = m_1 k$ for some positive m_1.But then we have

$$\sum_{h \in H} \xi^h = \sum_{\ell=0}^{s-1} (\xi^h)^\ell = \frac{\xi^{sh} - 1}{\xi^h - 1} = 0$$

since $\xi^{sh} = \xi^{m_1 k} = 1$. □

We are now ready to prove the following theorem that gives a MacWilliams-like identity for the complete weight enumerators of abelian group codes:

Theorem 3.10. *Suppose that $G = \{g_1, \ldots, g_q\}$ is an abelian group of order q and of the form given in (3.21). Suppose that ξ is a primitive m_1^{th} root of unity over complex numbers,*

and let C be a group code of length n over G, and let C^* be the dual of C with respect to the inner product defined in (3.23) and (3.24). Then we have

$$\mathrm{cwe}_{C^*}(W_1, W_2, \ldots, W_q) = \frac{1}{|C|}\mathrm{cwe}_C\big(\sum_{i=1}^{q}\xi^{g_1 * g_i}W_i, \sum_{i=1}^{q}\xi^{g_2 * g_i}W_i, \ldots, \sum_{i=1}^{q}\xi^{g_q * g_i}W_i\big). \quad (3.26)$$

Proof. The proof uses the same ideas and the same techniques used to prove the original MacWilliams theorem from [6] and [20]. We will first introduce a function over G^n as

$$F(\overline{u}) := \sum_{\overline{v}\in G^n}\xi^{<\overline{u},\overline{v}>}\prod_{i=1}^{q}W_i^{n_{g_i}(\overline{v})}. \quad (3.27)$$

Summing $F(\overline{u})$'s over all the codewords of the code C, we obtain

$$\sum_{\overline{u}\in C}F(\overline{u}) = \sum_{\overline{u}\in C}\sum_{\overline{v}\in G^n}\xi^{<\overline{u},\overline{v}>}\prod_{i=1}^{q}W_i^{n_{g_i}(\overline{v})} = \sum_{\overline{v}\in G^n}\prod_{i=1}^{q}W_i^{n_{g_i}(\overline{v})}\sum_{\overline{u}\in C}\xi^{<\overline{u},\overline{v}>}. \quad (3.28)$$

Now, suppose for fixed $\overline{v}\in G^n$, we consider the function

$$f_{\overline{v}} : C \to \mathbb{Z}_{m_1}$$

that takes $\overline{u}\in C$ to $<\overline{u},\overline{v}>$ modulo m_1. Note that $f_{\overline{v}}$ is a group homomorphism. Now, by definition of the dual, we have

$$\ker(f_{\overline{v}}) = C \Leftrightarrow <\overline{u},\overline{v}> \equiv 0 \pmod{m_1}\ \forall\overline{u}\in C \Leftrightarrow \overline{v}\in C^*.$$

This means the inner sum of (3.28) becomes $|C|$ for all $\overline{v}\in C^*$.

Now, suppose that $\overline{v}$ is not in C^*. This means that $\ker(f_{\overline{v}}) \neq C$ and so it is a non-trivial subgroup of C, which means that $\mathrm{Im}(f_{\overline{v}})$ is a non-trivial subgroup of $\mathbb{Z}_{m_1}$ and hence by Lemma 3.9, the inner sum becomes 0 for any such $\overline{v}\in G^n$. This means that

$$\sum_{\overline{u}\in C}F(\overline{u}) = |C|\sum_{\overline{v}\in C^*}\prod_{i=1}^{q}W_i^{n_{g_i}(\overline{v})} = |C|\mathrm{cwe}_{C^*}(W_1, W_2, \ldots, W_q), \quad (3.29)$$

which is equivalent to saying that

$$\mathrm{cwe}_{C^*}(W_1, W_2, \ldots, W_q) = \frac{1}{|C|} \sum_{\overline{u} \in C} F(\overline{u}). \tag{3.30}$$

Now we need to find what $F(\overline{u})$ is. Let $\delta(x, y)$ denote the Kronecker Delta function, which takes the value 1 if $x = y$ and 0 for all other values. So

$$\begin{aligned} F(\overline{u}) &= \sum_{\overline{v} \in G^n} \xi^{<\overline{u}, \overline{v}>} \prod_{i=1}^{q} W_i^{n_{g_i}(\overline{v})} \\ &= \sum_{(v_1, v_2, \ldots, v_n) \in G^n} \Big(\prod_{j=1}^{n} (\xi^{u_j * v_j} \prod_{i=1}^{q} W_i^{\delta(v_j, g_i)}) \Big) \\ &= \prod_{j=1}^{n} \Big(\sum_{i=1}^{q} \xi^{u_j * g_i} W_i \Big) \\ &= \Big(\sum_{i=1}^{q} \xi^{g_1 * g_i} W_i \Big)^{n_{g_1}(\overline{u})} \cdot \Big(\sum_{i=1}^{q} \xi^{g_2 * g_i} W_i \Big)^{n_{g_2}(\overline{u})} \cdots \Big(\sum_{i=1}^{q} \xi^{g_q * g_i} W_i \Big)^{n_{g_q}(\overline{u})}. \end{aligned}$$

Summing this last product over all the codewords of C, we get the desired result. □

As we said earlier, knowing the complete weight enumerator makes it easier to calculate all the other weight enumerators. Now, as an application we will obtain the MacWilliams identity for the Hamming weight enumerators of abelian group codes by using Theorem 3.10, which will be the exact same result that Delsarte obtained in [5].

MacWilliams identity for Hamming weight enumerators

For this section, we will assume $G = \{g_1, g_2, \ldots, g_q\}$ to be the abelian group over which the code is defined and $g_1 = 0$ the zero element in the group. We first define the Hamming weight enumerator for the group code in a similar way that it was defined for $\mathbb{Z}_4$-codes:

$$\mathrm{H}_C(W, X) = \sum_{\overline{c} \in C} W^{n - w_{\mathrm{H}}(\overline{c})} X^{w_{\mathrm{H}}(\overline{c})} = \sum_{\overline{c} \in C} W^{n_0(\overline{c})} X^{n_{g_2}(\overline{c}) + \cdots + n_{g_q}(\overline{c})} \tag{3.31}$$

where w_{H} is the Hamming weight. In fact, we note that it can be written in terms of the complete weight enumerator as

$$\mathrm{H}_C(W, X) = \mathrm{cwe}_C(W, X, X, \ldots, X). \tag{3.32}$$

Then using Theorem 3.10, we can relate the Hamming weight enumerator of C and C^*:

$$\begin{aligned} \mathrm{H}_{C^*}(W,X) &= \mathrm{cwe}_{C^*}(W,X,X,\ldots,X) \\ &= \frac{1}{|C|}\mathrm{cwe}_C\big(W+(q-1)X, W+X\sum_{i=2}^{q}\xi^{g_2*g_i},\ldots,W+X\sum_{i=2}^{q}\xi^{g_q*g_i}\big). \end{aligned} \tag{3.33}$$

At this point we want to introduce the following lemma:

Lemma 3.11. *For all $j>1$, we have*

$$\sum_{i=2}^{q}\xi^{g_i*g_j} = -1.$$

Proof. For any such fixed j, consider the map $f_j : G \to \mathbb{Z}_{m_1}$ such that $f_j(g_i) = g_i * g_j$. Then f_j is a group homomorphism. By Lemma 3.7, we know that $g_i * g_j = 0$ for all $j = 1,2,\ldots,q$ if and only if $g_i = g_1 = 0$. So, if $j>1$, then we have $\ker(f_j) \neq G$ and hence $\mathrm{Im}(f_j)$ is a non-trivial subgroup of $\mathbb{Z}_{m_1}$. But then, by Lemma 3.9 we get

$$\sum_{i=1}^{q}\xi^{g_j*g_i} = 0$$

for all such $j>1$. Since $g_j * g_1 = g_j * 0 = 0$ for all j, we get

$$\sum_{i=2}^{q}\xi^{g_i*g_j} = -1, \qquad j = 2,3,\ldots,q.$$

□

But using Lemma 3.11 in (3.33), we see that we have easily proved the following corollary of Theorem 3.10 that gives the MacWilliams identity for the Hamming weight enumerators of abelian group codes:

Corollary 3.12. *Suppose that C is a group code over G of length n with $|G| = q$. Let*

$$\mathrm{H}_C(W,X) = \sum_{\overline{c}\in C} W^{n-w_{\mathrm{H}}(\overline{c})}X^{w_{\mathrm{H}}(\overline{c})}$$

be the Hamming weight enumerator of C and let C^* be the dual of C with respect to the inner product defined in (3.23) and (3.24). Then we have the Macwilliams identity for the Hamming Weight enumerators of C and C^* as follows:

$$\mathrm{H}_{C^*}(W,X) = \frac{1}{|C|}\mathrm{H}_C\big(W+(q-1)X, W-X\big).$$

3.3 MacWilliams Identities for Linear Codes over Rings

In this section, we will see some applications of Theorem 3.10, which was proved in the previous section. In particular, we will focus on linear codes over rings, and we will consider several rings in this process. We first note that every linear ring-code can be viewed as an abelian-group code, while not every abelian group code is a ring code.

For example, the code $C = \big\{\overline{0}, (0,1,2,1,3,1), (0,2,0,2,2,2), (0,3,2,3,1,3)\big\}$ is an abelian group code over $GR(4,m)$ because $C < GR(4,m)^6$, but C is not a linear code over $GR(4,m)$, as for example $\xi \cdot (0,1,2,1,3,1)$ is not in C.

So, while the method and the results of Theorem 3.10 will be applied readily, we will have to make modifications in the form of introducing new inner products so that the dual with respect to the new inner product of any linear ring-code will also be linear over the same ring. The inner product defined in (3.23) and (3.24) certainly doesn't ensure this, as it only gives the dual as an abelian group code, not as a ring-code. So, for the rest of the section, we will consider different rings and we will introduce new inner products so that the duals will be linear over the same ring as well, and we will obtain analogous results for the complete weight enumerators of these codes:

Linear $\mathbb{Z}_m$-codes

Note that this is exactly the case that was discussed in Section 2.2, with $r = 1$. So there is no difference here because linear codes over $\mathbb{Z}_m$ are $\mathbb{Z}_m$-submodules of $\mathbb{Z}_m^n$, which are exactly subgroups of $\mathbb{Z}_m^n$. So, Theorem 3.10 and Corollary 3.12 remain the same for linear codes over $\mathbb{Z}_m$.

Linear Codes over $GR(p^\ell, m)$

For the general introduction about Galois rings we refer to Section 2.2. We will use the

notations used in that section. We recall that a linear code of length n over $GR(p^\ell, m)$ is a submodule of $GR(p^\ell, m)^n$.

We start by defining an inner product on $GR(p^\ell, m)^n$:

Definition 3.13. Suppose that

$$\overline{x} = (x_1, x_2, \ldots, x_n),\ \ \overline{y} = (y_1, y_2, \ldots, y_n) \in GR(p^\ell, m)^n$$

are two vectors; then we define a symmetric function $< ., . >$ from $GR(p^\ell, m)^n \times GR(p^\ell, m)^n$ to $\mathbb{Z}_{p^\ell}$ by letting

$$< \overline{x}, \overline{y} >= \mathrm{Tr}(x_1 y_1 + x_2 y_2 + \cdots + x_n y_n) \tag{3.34}$$

where $x_i y_i$ is the ordinary product in $GR(p^\ell, m)$, and Tr is the trace function defined for Galois rings in Section 2.2.

In order to understand some of the properties of this inner product, we will first prove some lemmas about the Trace operator, Tr.

We will define $f_p : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ to be the usual Frobenius map defined on finite fields, which acts as $f_p(a) = a^p$ for all $a \in \mathbb{F}_{p^m}$. Then, it is a well-known fact that the group

$$G = \{1, f_p, f_p^2, \ldots, f_p^{m-1}\}$$

forms the $\mathbb{F}_p$-automorphism group of $\mathbb{F}_{p^m}$ as an extension of $\mathbb{F}_p$. We define an $\mathbb{F}_p$-linear function tr on $\mathbb{F}_{p^m}$ called Trace, so that

$$\mathrm{tr}(a) = a + f_p(a) + f_p^2(a) + \cdots + f_p^{m-1}(a) = a + a^p + a^{p^2} + \cdots + a^{p^{m-1}}.$$

This is indeed $\mathbb{F}_p$-linear because $s^{p^i} \equiv s \pmod p$ for all $s \in \mathbb{F}_p$ and all $i \geq 0$. Then we can prove that tr is onto by the following lemma:

Lemma 3.14. *Assume that $\mathbb{F}_{p^m}$ is a finite field and that* $\mathrm{tr} : \mathbb{F}_{p^m} \to \mathbb{F}_p$ *is the Trace map. Then* tr *is non-zero.*

Proof. To prove the theorem we note that $G = \{1, f_p, f_p^2, \ldots, f_p^{m-1}\}$ is a distinct set of

automorphisms of $\mathbb{F}_{p^m}$ and so by Lemma 7.5. (Hungerford, [21]), we see that G is linearly independent. This means however that the map $1 + f_p + f_p^2 + \cdots + f_p^{m-1}$ cannot be the zero map on $\mathbb{F}_{p^m}$, and this means that the Trace map is non-zero. □

Note that the following is an immediate corollary of this lemma:

Corollary 3.15. *Assume that* $\mathbb{F}_{p^m}$ *is a finite field and that* $\mathrm{tr} : \mathbb{F}_{p^m} \to \mathbb{F}_p$ *is the Trace map. Then tr is onto.*

We remember from (2.3) that

$$\frac{GR(p^\ell, m)}{pGR(p^\ell, m)} \simeq \mathbb{F}_{p^m} \tag{3.35}$$

and let

$$T_m = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^m-2}\} \tag{3.36}$$

be the Teichmuller set defined for the Galois ring $GR(p^\ell, m)$. Let ψ be the Frobenius map defined on $GR(p^\ell, m)$ as in Section 2.2 and let Tr be the trace map on the Galois rings, so that

$$\mathrm{Tr}(u) = u + \psi(u) + \cdots + \psi^{m-1}(u), \tag{3.37}$$

which is a $\mathbb{Z}_{p^\ell}$-linear function on the Galois ring. Let $\mu : GR(p^\ell, m) \to GR(p^\ell, m)/pGR(p^\ell, m)$ be the canonical homomorphism. We first note that μ acts as reduction modulo p on $\mathbb{Z}_{p^\ell}$. We also note that, if $\theta = \mu(\xi)$, then

$$\mu(T_m) = \{0, 1, \theta, \theta^2, \ldots, \theta^{p^m-2}\} \simeq \mathbb{F}_{p^m}. \tag{3.38}$$

Then we prove the following lemma with a method very similar to the one used in [2]:

Lemma 3.16. *Suppose,* ψ*,* Tr*,* μ *be defined as above, and suppose that* f_p *and tr are the Frobenius automorphism and the trace map defined on* $\mathbb{F}_{p^m}$ *over* $\mathbb{F}_p$*. Then we have*

(i)

$$\mu \circ \psi = f_p \circ \mu$$

(ii)

$$\mu \circ \mathrm{Tr} = \mathrm{tr} \circ \mu.$$

Proof. **(i)** Suppose that $c = u_0 + pu_1 + \cdots + p^{\ell-1}u_{\ell-1}$ with $u_i \in T_m$. First assume that $u_0 = 0$. Then $\mu(c) = 0$ and so $f_p \circ \mu(c) = 0$. But, note that $\psi(c) = pu_1^p + p^2u_2^p + \cdots + p^{\ell-1}u_{\ell-1}^p$ and so $\mu \circ \psi(c) = 0$. So they are equal in this case.

Now suppose that $u_0 = \xi^j$ for some $j \geq 0$. Then $\mu(c) = \theta^j$ and hence $f_p \circ \mu(c) = \theta^{pj}$. On the other hand, we see that $\psi(c) = \xi^{pj} + pu_1^p + \cdots + p^{\ell-1}u_{\ell-1}^p$ and so $\mu \circ \psi(c) = \theta^{pj}$, which proves the first part.

(ii) This follows from part (i) easily by noting that $\mathrm{Tr} = 1 + \psi + \psi^2 + \cdots + \psi^{m-1}$ and $\mathrm{tr} = 1 + f_p + \cdots + f_p^{m-1}$. □

After all these preparations, we are ready to prove the following analogue of Lemma 3.14 for the trace map on Galois rings:

Lemma 3.17. *The Trace map* $\mathrm{Tr} : GR(p^\ell, m) \to \mathbb{Z}_{p^\ell}$ *is onto.*

Proof. We will restrict ourselves to the Teichmuller set

$$T_m = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^m-2}\}.$$

Now, we know that $\mu(T_m)$ is the same as $\mathbb{F}_{p^m}$ and tr is the usual trace operator on finite fields, and so by Lemma 3.14, we know that it is non-zero. This means that

$$\mu \circ \mathrm{Tr} \neq 0$$

on T_m by Lemma 3.16. Now, since Tr takes values in $\mathbb{Z}_{p^\ell}$ and μ acts as reduction modulo p on $\mathbb{Z}_{p^\ell}$, so

$$\mu \circ \mathrm{Tr} \neq 0$$

on T_m means that $\exists \xi^j \in T_m$ such that

$$\mathrm{Tr}(\xi^j) \neq 0 \pmod{p}. \tag{3.39}$$

But this means that if $\mathrm{Tr}(\xi^j) = s \in \mathbb{Z}_{p^\ell}$, then $GCD(s,p) = 1$ or that s is invertible in $\mathbb{Z}_{p^\ell}$. So, suppose that $r \in \mathbb{Z}_{p^e}$ is such that $rs = 1$ in $\mathbb{Z}_{p^\ell}$. But, then since Tr is $\mathbb{Z}_{p^\ell}$-linear, we get

$$\mathrm{Tr}(r \cdot \xi^j) = r \cdot \mathrm{Tr}(\xi^j) = rs = 1,$$

which proves that Tr is onto. □

After this introduction about the trace map on Galois rings, we are ready to explore some properties of the inner product defined in (3.34):

Lemma 3.18. *Suppose for fixed $\overline{u} \in GR(p^\ell, m)^n$ we have $< \overline{u}, \overline{x} > = 0$ for all $\overline{x} \in GR(p^\ell, m)^n$. Then $\overline{u} = 0$.*

Proof. By taking $\overline{x} \in GR(p^\ell, m)^n$ of the form $(x, 0, \ldots, 0)$, we might assume without loss of generality that $n = 1$. So, what we have is that for a fixed $u \in GR(p^\ell, m)$,

$$\mathrm{Tr}(ux) = 0, \qquad \forall x \in GR(p^\ell, m).$$

We will prove that $u = 0$ in this case. Note that $\{ux : x \in GR(p^\ell, m)\}$ is an ideal of $GR(p^\ell, m)$, and so is of the form $uGR(p^\ell, m)$. Since we know all the non-zero ideals of $GR(p^\ell, m)$, if $u \neq 0$, then the ideal must be of the form $p^i GR(p^\ell, m)$ for some $0 \leq i \leq \ell - 1$. So, assuming that $u \neq 0$ will then lead us to having the Trace function Tr vanishing on the whole ideal $p^i GR(p^\ell, m)$. But this is impossible, since by Lemma 3.17 we saw that Tr is onto. So, $\mathrm{Tr}(c) = 1$ for some $c \in GR(p^\ell, m)$, which means that $\mathrm{Tr}(p^i c) = p^i \neq 0$ in $\mathbb{Z}_{p^\ell}$. The contradiction gives us the desired result. □

We now introduce the dual of C with respect to this inner product.

Definition 3.19. Suppose C is a linear code over $GR(p^\ell, m)$ of length n. Then we define the dual C^* of C with respect to the inner product defined in (3.34) as

$$C^* = \left\{ \overline{y} \in GR(p^\ell, m)^n \middle| \ < \overline{x}, \overline{y} >= 0 \ \ \forall \overline{x} \in C \right\}. \tag{3.40}$$

Remark 3.20. We note that Lemma 3.18 implies $\{\overline{0}\}^* = GR(p^\ell, m)^n$ and $(GR(p^\ell, m)^n)^* = \{\overline{0}\}$.

The main difference between this definition and the general definition made previously for general Group codes is that the dual that we obtain in this way is indeed a linear $GR(p^\ell, m)$-code as we will prove in the following lemma:

Lemma 3.21. *The dual C^* to the linear $GR(p^\ell, m)$-code C that we obtained in (3.40) is indeed a linear code over $GR(p^\ell, m)$.*

Proof. Since additivity is obvious by the basic properties of Tr and $< ., . >$, all we need to prove is that for any $\overline{y} \in C^*$, we have $u \cdot \overline{y} \in C^*$ for all $u \in GR(p^\ell, m)$. Now, fix $\overline{x} \in C$. Then we have

$$\begin{aligned} < \overline{x}, u \cdot \overline{y} > &= \mathrm{Tr}\big(x_1 \cdot (uy_1) + x_2 \cdot (uy_2) + \cdots + x_n \cdot (uy_n)\big) \\ &= \mathrm{Tr}\big(ux_1y_1 + ux_2y_2 + \cdots + ux_ny_n\big) \\ &= < u\overline{x}, \overline{y} > . \end{aligned} \tag{3.41}$$

But we know that $< \overline{x}, \overline{y} >= 0$ for all $\overline{x} \in C$ and since C is linear over $GR(p^\ell, m)$, we know that $u\overline{x} \in C$ for all $u \in GR(p^\ell, m)$. Thus, we see that $< u\overline{x}, y >= 0$ for all $u \in GR(p^\ell, m)$. But, by (3.41), then we see that

$$< \overline{x}, u\overline{y} >=< u\overline{x}, \overline{y} >= 0.$$

Since this is true for all $\overline{x} \in C$ we see that $u\overline{y} \in C^*$ for any $\overline{y} \in C^*$ and $u \in GR(p^\ell, m)$. Thus, we see that C^* is indeed a linear code over $GR(p^\ell, m)$ of length n. □

We are finally ready to state the corollary of Theorem 3.10 for linear codes over Galois rings:

Corollary 3.22. *Suppose that $GR(p^\ell, m) = \{u_0, u_1, \ldots, u_{p^{\ell m}-1}\}$ is the Galois Ring extension of $\mathbb{Z}_{p^\ell}$, and suppose that C is a linear code over $GR(p^\ell, m)$ of length n and let C^* be the dual of C with respect to the inner product defined in (3.34). Then C^* is also a linear*

code over $GR(p^\ell, m)$ of length n and moreover we have

$$\mathrm{cwe}_{C^*}(W_0, W_1, \ldots, W_{p^{\ell m}-1}) = \frac{1}{|C|}\mathrm{cwe}_C\Big(\sum_{i=0}^{p^{\ell m}-1} \alpha^{\mathrm{Tr}(u_0 u_i)} W_i, \sum_{i=0}^{p^{\ell m}-1} \alpha^{\mathrm{Tr}(u_1 u_i)} W_i, \ldots, \sum_{i=0}^{p^{\ell m}-1} \alpha^{\mathrm{Tr}(u_{p^{\ell m}-1} u_i)} W_i\Big)$$

*where α is a primitive p^ℓ*th *root of unity.*

The result for the Hamming weight enumerators is exactly the same as Corollary 3.12.

Linear Codes over $\mathbb{F}_{p^m}$

These are codes over the finite field $\mathbb{F}_{p^m}$, and since we have proved all the properties of the trace function $\mathrm{tr} : \mathbb{F}_{p^m} \to \mathbb{F}_p$ above, we can define an inner product exactly the same as (3.34) with the only modification being the replacement of Tr with tr. Everything else works just like in the case of Galois rings and we get the following corollary to Theorem 3.10:

Corollary 3.23. *Suppose C is a k-dimensional linear code over $\mathbb{F}_{p^m} = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^m-2}\}$. Suppose*

$$\mathrm{cwe}_C(W, W_0, W_1, \ldots, W_{p^m-2}) = \sum_{\overline{c}\in C} W^{n_0(\overline{c})} \prod_{i=0}^{p^m-2} W_i^{n_{\xi^i}(\overline{c})}$$

is the complete weight enumerator of C. Suppose that C^* is the dual of C with respect to the inner product defined in (3.34), and let γ be a primitive pth root of unity. Then, C^* is an $(n-k)$-dimensional linear code over $\mathbb{F}_{p^m}$ and we have

$$\mathrm{cwe}_{C^*}(W, W_0, W_1, \ldots, W_{p^m-2}) = \frac{1}{p^{mk}}\mathrm{cwe}_C\big(W + \sum_{i=0}^{p^m-2} \gamma^{\mathrm{tr}(0\cdot\xi^i)} W_i, W + \sum_{i=0}^{p^m-2} \gamma^{\mathrm{tr}(1\cdot\xi^i)} W_i, \ldots, W + \sum_{i=0}^{p^m-2} \gamma^{\mathrm{tr}(\xi^{p^m-2}\cdot\xi^i)} W_i\big).$$

Linear Codes over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$

Linear codes over these rings were considered by different authors including Gaborit, Dougherty, Betsumiya, Ling, et al. in works like [11], [12], [13]. We will give a very brief description of this ring and the codes over these rings and then give the analogous results for the

MacWilliams identities here, but these rings will be more extensively studied in Chapter 4 and Chapter 5.

The ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ is defined as

$$\big\{a + ub \,|\, a, b \in \mathbb{F}_{2^m},\ u^2 = 0\big\}.$$

It is easy to see that in fact

$$\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} \simeq \mathbb{F}_{2^m}[x]/(x^2). \tag{3.42}$$

A linear code C over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ of length n is defined as usual to be a submodule of $(\mathbb{F}_{2^m} + u\mathbb{F}_{2^m})^n$. We define an inner product on this ring so that the dual of the linear codes will be linear as well. In what follows, we denote by tr the usual trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. We define the inner product on this ring as

$$< (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) >= \mathrm{tr}(x_1 * y_1 + x_2 * y_2 + \cdots + x_n * y_n) \tag{3.43}$$

where $(x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n)$ are vectors in $(\mathbb{F}_{2^m} + u\mathbb{F}_{2^m})^n$ and the operation $*$ is from $(\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}) \times (\mathbb{F}_{2^m} + u\mathbb{F}_{2^m})$ to $\mathbb{F}_{2^m}$ defined as

$$(a + bu) * (c + du) = ac + ad + bc \tag{3.44}$$

for $a + bu, c + du \in \mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ and the addition on the right hand side is addition in $\mathbb{F}_{2^m}$. Using the properties of the trace function that we proved above, similar results to Lemma 3.18 can be obtained for this inner product as well.

We now define the dual of a linear code C over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ of length n with respect to the inner product defined in (3.43) and (3.44) as before:

$$C^* = \big\{\overline{y} \in (\mathbb{F}_{2^m} + u\mathbb{F}_{2^m})^n \big| < \overline{x}, \overline{y} >= 0 \quad \forall \overline{x} \in C\big\}.$$

The main thing is to show that the dual of a linear code is linear over this ring as well. But

this is done in the usual way like we did above in the case of Galois rings. The main point then is to show that

$$< (a+bu)\overline{x}, \overline{y} >=< \overline{x}, (a+bu)\overline{y} >$$

for all $\overline{x}, \overline{y} \in (\mathbb{F}_{2^m} + u\mathbb{F}_{2^m})^n$, and $a, b \in \mathbb{F}_{2^m}$. Now, since tr is additive, we can assume $n = 1$, that is we can consider the problem coordinate-wise. So, suppose $x = c + du$, $y = e + fu$ with $c, d, e, f \in \mathbb{F}_{2^m}$. Then we have

$$\begin{aligned} < (a+bu)(c+du), (e+fu) > &=< ac + (ad+bc)u, e+fu > \\ &= \mathrm{tr}(ace + acf + ade + bce) \\ &= \mathrm{tr}(aec + aed + (af+be)c) \\ &=< c+du, ae + (af+be)u > \\ &=< (c+du), (a+bu)(e+fu) >, \end{aligned}$$

which proves the assertion. This means that, we obtain the following corollary to Theorem 3.10 for linear codes over the ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$:

Corollary 3.24. *Suppose that*

$$\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} = \{a_i | i = 0, 1, \ldots, 2^{2m} - 1\}$$

with $a_0 = 0$ and let C be a linear code over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ of length n and suppose C^* is the dual of C with respect to the inner product defined in (3.43) and (3.44). Then C^* is also a linear code over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ of length n and moreover we have

$$\begin{aligned} &\mathrm{cwe}_{C^*}\big(W_0, W_1, \ldots, W_{2^{2m}-1}\big) = \\ &\quad \frac{1}{|C|}\mathrm{cwe}_C\Big(\sum_{i=0}^{2^{2m}-1} (-1)^{\mathrm{tr}(0*a_i)} W_i, \sum_{i=0}^{2^{2m}-1} (-1)^{\mathrm{tr}(a_1*a_i)} W_i, \ldots, \sum_{i=0}^{2^{2m}-1} (-1)^{\mathrm{tr}(a_{2^{2m}-1}*a_i)} W_i\Big). \end{aligned}$$

Linear codes over $\mathbb{F}_2 + u\mathbb{F}_2$

This is just a special case of what we did above with $m = 1$ with the trace function tr being the identity function. The reason we want to single out this case is because it is very

similar to the ring $\mathbb{Z}_4$, with u playing the role of 2. In fact a corresponding Lee weight w_{L} is defined for this ring,

$$w_{\mathrm{L}}(0) = 0,\ \ w_{\mathrm{L}}(1) = w_{\mathrm{L}}(1+u) = 1,\ \ w_{\mathrm{L}}(u) = 2. \tag{3.45}$$

Let the complete weight enumerator for a linear code C over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ be defined in the usual way:

$$\mathrm{cwe}_C(W, X, Y, Z) = \sum_{\overline{c} \in C} W^{n_0(\overline{c})} X^{n_1(\overline{c})} Y^{n_u(\overline{c})} Z^{n_{1+u}(\overline{c})}. \tag{3.46}$$

Then, calculating the corresponding $a_i * a_j$'s in Corollary 3.24, we see that if C^* is the dual of C with respect to the inner product defined in (3.43) and (3.44), then we get

$$\mathrm{cwe}_{C^*}\big(W, X, Y, Z\big) = \frac{1}{|C|}\mathrm{cwe}_C\big(W+X+Y+Z, W-X-Y+Z, W-X+Y-Z, W+X-Y-Z\big). \tag{3.47}$$

which is very similar to (3.6), the corresponding result for the $\mathbb{Z}_4$-codes that was done in [2].

Identifying 1 and $1 + u$ in the complete weight enumerator, we again obtain a similar definition for the symmetrized weight enumerators for codes over $\mathbb{F}_2 + u\mathbb{F}_2$ as well. This means, the symmetrized weight enumerator can be written in terms of the complete weight enumerator as

$$\mathrm{swe}_C(W, X, Y) = \mathrm{cwe}_C(W, X, Y, X).$$

But, then putting this in (3.47) we see that we get the following:

$$\mathrm{swe}_{C^*}(W, X, Y) = \frac{1}{|C|}\mathrm{swe}_C\big(W + 2X + Y, W - Y, W - 2X + Y\big). \tag{3.48}$$

Note that this is exactly the same result (3.7) that was obtained for $\mathbb{Z}_4$-codes in [2].

Finally, we can obtain a MacWilliams identity for the Lee weight enumerators of such

codes by noting

$$\begin{aligned}\mathrm{Lee}_C(W,X) &= \sum_{\overline{c}\in C} W^{2n-w_L(\overline{c})}X^{w_L(\overline{c})} \\ &= \sum_{\overline{c}\in C} W^{2n_0(\overline{c})+n_1(\overline{c})+n_{1+u}(\overline{c})}X^{n_1(\overline{c})+n_{1+u}(\overline{c})+2n_u(\overline{c})} \\ &= \mathrm{cwe}_C\big(W^2, WX, X^2, WX\big) \\ &= \mathrm{swe}_C\big(W^2, WX, X^2\big). \end{aligned} \tag{3.49}$$

So, by exactly the same methods as were used in [2], we can obtain the following identity for the Lee weight enumerators of linear codes over $\mathbb{F}_2 + u\mathbb{F}_2$:

$$\mathrm{Lee}_{C^*}(W,X) = \frac{1}{|C|}\mathrm{Lee}_C\big(W+X, W-X\big), \tag{3.50}$$

which is exactly the same identity as (3.8) that was obtained in [2] for linear codes over $\mathbb{Z}_4$.

3.4 Concluding Remarks and Some Applications

C^* and $C^\perp$

In the previous section, we found MacWilliams identities for the complete weight enumerators of linear codes over several rings by introducing new inner products so that the duals C^* of these codes with respect to these inner products are also linear over the same rings. Another purpose of introducing those inner products was to get better numerical results in the formulas. For example, in the case of the Galois rings $GR(p^\ell, m)$, we defined the inner product so that it takes values in $\mathbb{Z}_{p^\ell}$. This made it easier to calculate for example $\xi^{u_i * u_j}$, since the values taken by $u_i * u_j$ were in $\mathbb{Z}_{p^\ell}$.

We know that in the case of all those rings, a natural inner product to define would be the *Euclidean inner product*, for example in the case of $GR(p^\ell, m)$ we could define $< .,. >_2$: $GR(p^\ell, m)^n \times GR(p^\ell, m)^n \to GR(p^\ell, m)$ so that

$$< (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) >_2 = x_1y_1 + x_2y_2 + \cdots + x_ny_n \tag{3.51}$$

for all $(x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in GR(p^\ell, m)^n$ where $x_i y_i$ is the ordinary ring product in $GR(p^\ell, m)$.

Let us recall that in the previous section we defined a different inner product for calculation purposes as:

$$< (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) >_1 = \mathrm{Tr}(x_1 y_1 + x_2 y_2 + \cdots + x_n y_n) \tag{3.52}$$

for all $(x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in GR(p^\ell, m)^n$.

Now, we recall the definitions of C^* and $C^\perp$ in

$$C^* = \big\{ (y_1, y_2, \ldots, y_n) \in GR(p^\ell, m)^n \big| < \overline{x}, \overline{y} >_1 = 0, \quad \forall \overline{x} \in C \big\} \tag{3.53}$$

and

$$C^\perp = \big\{ (y_1, y_2, \ldots, y_n) \in GR(p^\ell, m)^n \big| < \overline{x}, \overline{y} >_2 = 0, \quad \forall \overline{x} \in C \big\}. \tag{3.54}$$

Note that, $C^\perp$ seems to give us more information because the Euclidean product is a more natural inner product, but in fact it turns out that these two duals are not different:

Lemma 3.25. *Suppose that C is a linear code over $GR(p^\ell, m)$ of length n and let C^* and $C^\perp$ be the duals of C with respect to $< ., . >_1$ and $< ., . >_2$, respectively.Then we have $C^* = C^\perp$.*

Proof. We first prove the obvious inclusion. Let $\overline{y} \in C^\perp$. This means that

$$x_1 y_1 + x_2 y_2 + \cdots + x_n y_n = 0, \quad \forall (x_1, x_2, \ldots, x_n) \in C,$$

but $\mathrm{Tr}(0) = 0$, which means that in this case we have

$$\mathrm{Tr}(x_1 y_1 + x_2 y_2 + \cdots + x_n y_n) = 0, \quad \forall (x_1, x_2, \ldots, x_n) \in C,$$

which means that $\overline{y} \in C^*$, hence we get

$$C^\perp \subseteq C^*. \tag{3.55}$$

Now, suppose that $\overline{z} = (z_1, z_2, \ldots, z_n) \in C^*$. This means that

$$\mathrm{Tr}(x_1z_1 + x_2z_2 + \cdots + x_nz_n) = 0, \quad \forall (x_1, x_2, \ldots, x_n) \in C.$$

Now, fix one such $\overline{x} = (x_1, x_2, \ldots, x_n) \in C$. But since C is a linear code over $GR(p^e, m)$, this means that

$$r(x_1, x_2, \ldots, x_n) = (rx_1, rx_2, \ldots, rx_n) \in C$$

for all $r \in GR(p^\ell, m)$. So, this means that we have

$$\mathrm{Tr}\big(r(x_1z_1 + x_2z_2 + \cdots + x_nz_n)\big) = 0, \quad \forall r \in GR(p^\ell, m).$$

But then by Lemma 3.18, we must have

$$x_1z_1 + x_2z_2 + \cdots + x_nz_n = 0$$

in $GR(p^\ell, m)$ and since this is true for all $(x_1, x_2, \ldots, x_n) \in C$, we see, by definition of $C^\perp$, that $\overline{z} \in C^\perp$, which means

$$C^* \subseteq C^\perp. \tag{3.56}$$

Then combining (3.55) and (3.56), we see that we must have $C^* = C^\perp$. □

Similar conclusions can be drawn for the case of $\mathbb{F}_{p^m}$-codes as well as $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$. So, we see that the duals that we have obtained are not entirely unknown objects, but in fact they are the same as the usual duals with respect to the Euclidean product. This will give us some information about the size and the type of the codes.

The Type of C^*

Now that we proved that $C^* = C^\perp$, in order to find the type of C^*, we only need to find the type of $C^\perp$. We will only demonstrate this in the case of $\mathbb{Z}_{p^m}$-codes and we will give the analogous results for the case of Galois rings, finite fields, and $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$.

Theorem 3.26. *Suppose C is a linear code over $\mathbb{Z}_{p^m}$ of length n and of type*

$$(p^m)^{k_1}(p^{m-1})^{k_2}\dots(p)^{k_m}.$$

Then the dual $C^\perp$ of C is a linear code over $\mathbb{Z}_{p^m}$ of length n and of type

$$(p^m)^{n-k_1-k_2-\cdots-k_m}(p^{m-1})^{k_m}(p^{m-2})^{k_{m-1}}\dots(p)^{k_2}.$$

Proof. Note that, by Theorem 2.7, C is permutationally equivalent to a code with a generating matrix

$$G = \begin{bmatrix} I_{k_1} & A_1 & . & . & . & A_m \\ 0 & pI_{k_2} & pB_1 & . & . & pB_{m-1} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & . & 0 & p^{m-1}I_{k_m} & p^{m-1}C \end{bmatrix}.$$

So, the definition of the dual will give us

$$(x_1, x_2, \dots, x_n) \in C^\perp \Leftrightarrow \begin{bmatrix} I_{k_1} & A_1 & . & . & . & A_m \\ 0 & pI_{k_2} & pB_1 & . & . & pB_{m-1} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & . & 0 & p^{m-1}I_{k_m} & p^{m-1}C \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ . \\ . \\ x_n \end{bmatrix} \equiv 0 \pmod{p^m}.$$

This will lead to equations of the sort

$$x_1 + (\overline{a}_{1,1}, \overline{a}_{2,1}, \dots, \overline{a}_{m,1}) \cdot (x_{k_1+1}, \dots, x_n) = 0$$

$$x_2 + (\overline{a}_{1,2}, \overline{a}_{2,2}, \dots, \overline{a}_{m,2}) \cdot (x_{k_1+1}, \dots, x_n) = 0$$

...

...

$$x_{k_1} + (\overline{a}_{1,k_1}, \overline{a}_{2,k_1}, \ldots, \overline{a}_{m,k_1}) \cdot (x_{k_1+1}, \ldots, x_n) = 0$$

where $\overline{a}_{i,j}$'s where $j = 1, \ldots, k_1$ are the rows of A_i. Similarly we have equations

$$px_{k_1+1} + p(\overline{b}_{1,1}, \ldots, \overline{b}_{m-1,1}) \cdot (x_{k_1+k_2+1}, \ldots, x_n)$$

$$px_{k_1+2} + p(\overline{b}_{1,2}, \ldots, \overline{b}_{m-1,2}) \cdot (x_{k_1+k_2+1}, \ldots, x_n)$$

...

...

$$px_{k_1+k_2} + p(\overline{b}_{1,k_2}, \ldots, \overline{b}_{m-1,k_2}) \cdot (x_{k_1+k_2+1}, \ldots, x_n)$$

where $\overline{b}_{i,j}$'s with $j = 1, 2, \ldots, k_2$ are the rows of B_i.

Continuing this way we get all these kinds of equations with the common multiple being increasing exponents of p, and thus we end up with

$$p^{m-1}x_{k_1+k_2+\cdots+k_{m-1}+1} = p^{m-1}\overline{c}_1\big(x_{k_1+k_2+\cdots+k_m+1}, \ldots, x_n\big)$$

$$p^{m-1}x_{k_1+k_2+\cdots+k_{m-1}+2} = p^{m-1}\overline{c}_2\big(x_{k_1+k_2+\cdots+k_m+1}, \ldots, x_n\big)$$

...

...

$$p^{m-1}x_{k_1+k_2+\cdots+k_{m-1}+k_m} = p^{m-1}\overline{c}_{k_m}\big(x_{k_1+k_2+\cdots+k_m+1}, \ldots, x_n\big)$$

where $\overline{c}_i$'s are rows of C.

All the above equations show that $x_{k_1+k_2+\cdots+k_m+1}, \ldots, x_n$ are all free $\mathbb{Z}_{p^m}$-variables. However, for each $x_{k_1+\cdots+k_{m-1}+1}, \ldots, x_{k_1+\cdots+k_{m-1}+k_m}$, we have p^{m-1} choices, for each $x_{k_1+\cdots+k_{m-2}+1}, \ldots, x_{k_1+\cdots+k_{m-2}+k_{m-2}}$, we have p^{m-2} choices, and so on and finally for each $x_{k_1+1}, \ldots, x_{k_1+k_2}$, we have p choices, while $x_1, x_2, \ldots, x_{k_1}$ are uniquely determined. This

proves the theorem. □

We will give the analogous corollaries for the case of the other rings:

Corollary 3.27. *Suppose C is a linear code of length over $GR(p^\ell, m)$ of length n and of type*

$$(p^{\ell m})^{k_1}(p^{(\ell-1)m})^{k_2}\dots(p^m)^{k_\ell}.$$

Then $C^* = C^\perp$ is also a linear code over $GR(p^e, m)$ of length n and of type

$$(p^{\ell m})^{n-k_1-k_2-\dots-k_\ell}(p^{(\ell-1)m})^{k_\ell}(p^{(\ell-2)m})^{k_{\ell-1}}\dots(p^m)^{k_2}.$$

Corollary 3.28. *Suppose that C is an $[n,k]$ linear code over $\mathbb{F}_{p^m}$. Then C^* is an $[n,n-k]$ linear code over $\mathbb{F}_{p^m}$.*

Corollary 3.29. *Suppose C is a linear code over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ of type $(2^{2m})^{k_1}(2^m)^{k_2}$. Then C^* is a linear code over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ of type $(2^{2m})^{n-k_1-k_2}(2^m)^{k_2}$.*

Remark 3.30. Looking at Theorem 3.26 and the subsequent corollaries, we see that, for a linear code C over the ring R of length n, where R is one of the rings considered above, we have

$$|C^*| = \frac{|R|^n}{|C|}. \tag{3.57}$$

Remark 3.31. The result in the above remark is obvious for the case of group codes, as was proved by Delsarte in [5], where he proved that if C is an abelian group code of length n and C^* is its dual, then

$$C^* \simeq G^n/C \tag{3.58}$$

where $\simeq$ is the group isomorphism.

Note that the inclusion $C \subseteq (C^*)^*$ is obvious, and so the remarks we made above about the sizes give us the following corollary:

Corollary 3.32. *For a linear code C over the ring R of length n, where R is one of the*

rings considered in this chapter, we have

$$(C^*)^* = C. \tag{3.59}$$

Benefits of the identities for complete weight enumerators

In this chapter, we found MacWilliams-like identities for the complete weight enumerators of linear codes over rings. One of the benefits of this comes from that fact that we can find any weight enumerator from the complete weight enumerator. This is especially very useful if we are looking at a linear code with a high dimension.

As an example, we will go back to the code that gave us the counter example in Section 3.1. Note that in that example, we had a linear code C over $\mathbb{Z}_4$ of type $(4)^2$ and length 30, and we needed to calculate the Euclidean weight enumerator of the dual $C^\perp$, which is a linear code of type $(4)^{28}$ and has $4^{28} = 72057594037927936 > 7 \times 10^{16}$ codewords. If we try to calculate the Euclidean weight enumerator of this code by brute force with a computer, assuming that the computer can calculate the weight enumerators of one million codewords in one second, then we would need more than 2000 years to finish the calculation. With a computer that would calculate the weight enumerator of one billion codewords in a second, we would still need more than 2 years. Looking however at the dual of this code, which happens to be a small code, only of size 16, for which we can easily calculate the complete weight enumerator, and then using the identities (3.6), (3.7) and (3.12), we were easily able to calculate the Euclidean weight enumerator of the code in a matter of seconds.

Knowing the MacWilliams identities for complete weight enumerators can help us find the weight enumerators of high-dimensional codes that have small duals as we saw in the above example. So, even though the counter example in Section 3.1 proved that we cannot have a MacWilliams-like identity for the Euclidean weight enumerators of linear codes over $\mathbb{Z}_4$ contrary to the case of Lee and Hamming weight enumerators, it still showed us a nice application and use of knowing the MacWilliams identities for the complete weight enumerators of linear codes over rings.

Lee weight and not the Euclidean weight is the homogeneous weight that was defined in 2.3. Since we have MacWilliams identities for the Lee weight enumerators, one can

ask the question whether a MacWilliams-like identity exists for the homogeneous weight enumerators of linear codes over $GR(p^\ell, m)$.

Chapter 4

Gray Maps

Gray maps from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$ were effectively used by Sloane, Calderbank, et al. in their work [2], as a tool to obtain the binary nonlinear Kerdock, Preparata, and Goethals codes as the Gray images of linear codes over $\mathbb{Z}_4$. Their definition of the Gray map is quite a simple one. To define it, they defined maps α, β, γ from $\mathbb{Z}_4$ to $\mathbb{Z}_2$ such that for any $c \in \mathbb{Z}_4$, $c = \alpha(c) + 2\beta(c)$ is the unique 2-adic expansion of c. The identity $\alpha(c) + \beta(c) + \gamma(c) = 0$ completed the definition of those maps. Then, extending these maps in an obvious way to $\mathbb{Z}_4^n$, they defined the Gray map $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ as

$$\phi(\overline{c}) = (\beta(\overline{c}), \gamma(\overline{c})), \qquad \overline{c} \in \mathbb{Z}_4^n. \tag{4.1}$$

The most important property of this map is that it is a distance preserving map, that is, it is an isometry from

$$(\mathbb{Z}_4^n, \text{Lee distance}) \text{ to } (\mathbb{Z}_2^{2n}, \text{Hamming distance}).$$

Carlet, in [8], extended this map to $\mathbb{Z}_{2^k}$ with the homogeneous weight and used this to obtain the generalized Kerdock codes that were non-linear binary codes with large minimum distances. Several other authors, like Ling and Grefrath generalized the notion of Gray maps to more general rings with certain homogeneous weights defined on them in [10] and [22].

In section 1, we will use a Gray map from $\mathbb{Z}_9$ to $\mathbb{Z}_3^3$ and similar techniques to the ones used in [2] and [8] to obtain some non-linear ternary codes with comparably high minimum distances. In section 2, we will give an inductive and coordinate-wise construction of a

Gray map from $\mathbb{Z}_{p^k}$ to $\mathbb{Z}_p^{p^{k-1}}$, which will be distance preserving. In section 3, we will give a purely combinatorial construction of the Gray map that we defined earlier, using the affine geometries. In section 4, we will talk about the Gray map for the ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ and we will obtain some results about the Lee weights of linear codes over these rings.

4.1 A Ternary Gray Map

We will define a Gray map from $\mathbb{Z}_9$ to $\mathbb{Z}_3^3$ that will be distance preserving with the homogenous distance on $\mathbb{Z}_9$ and with the Hamming distance on $\mathbb{Z}_3$. Before getting into that we will make some observations about linear codes over $\mathbb{Z}_{p^2}$.

Recall from Section 2.3 that the homogeneous weight on $\mathbb{Z}_{p^2}$ is defined as

$$w_{\text{hom}}(u) = \begin{cases} 0 & \text{if } u = 0 \\ p-1 & \text{if } u \in \mathbb{Z}_{p^2} \setminus p\mathbb{Z}_{p^2} \\ p & \text{if } u \in p\mathbb{Z}_{p^2} \setminus \{0\}. \end{cases}$$

Note that $\mathbb{Z}_{p^2} \setminus p\mathbb{Z}_{p^2} = (\mathbb{Z}_{p^2})^*$, the set of units in $\mathbb{Z}_{p^2}$.

A very important property of the homogeneous weight is that it can be expressed in terms of exponential sums. So, suppose $f(x)$ is a $\mathbb{Z}_{p^2}$-valued function over a set Ω. Then

$$w_{\text{hom}}(f) = \sum_{x \in \Omega} w_{\text{hom}}(f(x))$$

where we assume f denotes a codeword of length $|\Omega|$ as the value of f is evaluated at each element of Ω. We will prove the following useful lemma that relates the homogeneous weights to the exponential sums:

Lemma 4.1. *Suppose f is a $\mathbb{Z}_{p^2}$-valued function over a set Ω, and suppose we view f as a codeword of length $|\Omega|$ with the coordinates being the value that f takes at each element of Ω, and suppose $\omega = e^{\frac{2\pi i}{p^2}}$. Then we have*

$$w_{\text{hom}}(f) = (p-1)|\Omega| - \frac{1}{p} \sum_{\lambda \in (\mathbb{Z}_{p^2})^*} \left(\sum_{x \in \Omega} \omega^{\lambda f(x)} \right). \tag{4.2}$$

Proof. To understand the exponential sum, we will first calculate, for a fixed $x \in \Omega$,

$$\Upsilon_x = \sum_{\lambda \in (\mathbb{Z}_{p^2})^*} \omega^{\lambda f(x)}.$$

We will split this into a few obvious cases:

(i) Suppose $f(x) = 0$. Then $\omega^{\lambda f(x)} = 1$ for all $\lambda \in \mathbb{Z}_{p^2} \setminus p\mathbb{Z}_{p^2}$. So, we see that in this case we have

$$\Upsilon_x = |(\mathbb{Z}_{p^2})^*| = p^2 - p. \tag{4.3}$$

(ii) Suppose $f(x) \in p\mathbb{Z}_{p^2} \setminus \{0\}$. Then $w^{f(x)}$ is a primitive p^{th} root of unity, and without loss of generality we might assume that $\omega^{f(x)} = e^{2\pi i/p} = \theta$. Then, we get

$$\Upsilon_x = \sum_{\lambda \in (\mathbb{Z}_{p^2})^*} \theta^\lambda = (\theta + \theta^2 + \cdots + \theta^{p-1}) + \theta^p(\theta + \theta^2 + \cdots + \theta^{p-1}) + \cdots + \theta^{(p-1)p}(\theta + \theta^2 + \cdots + \theta^{p-1}). \tag{4.4}$$

Now, we know that $\theta^{pi} = 1$ for all $i = 0, 1, \ldots, p-1$. On the other hand since θ is a primitive p^{th} root of unity, $1 + \theta + \cdots + \theta^{p-1} = 0$, which means that $\theta + \theta^2 + \cdots + \theta^{p-1} = -1$. Putting all these into (4.4), we get, in the case $f(x) \in p\mathbb{Z}_{p^2} \setminus \{0\}$,

$$\Upsilon_x = -p. \tag{4.5}$$

(iii) Finally, we assume that $f(x) \in (\mathbb{Z}_{p^2})^* = \mathbb{Z}_{p^2} \setminus p\mathbb{Z}_{p^2}$. Note that, in this case, $\omega^{f(x)}$ is still a primitive $(p^2)^{th}$ root of unity, and hence, without loss of generality we might assume $f(x) = 1$.

Then, the sum we want to calculate becomes

$$\begin{aligned}
\Upsilon_x &= \omega + \omega^2 + \cdots + \omega^{p-1} + \omega^{p+1} + \cdots + \omega^{2p-1} + \cdots + \omega^{p(p-1)+1} + \cdots + \omega^{p^2-1} \\
&= 1 + \omega + \cdots + \omega^{p^2-1} - (1 + \omega^p + \omega^{2p} + \cdots + \omega^{p(p-1)}) \\
&= 0
\end{aligned}$$

since

$$1 + \omega + \cdots + \omega^{p^2-1} = \frac{1-\omega^{p^2}}{1-\omega} = 0$$

and $(\omega^p)^p = 1$ and w^p is not 1, and so from

$$0 = (\omega^p)^p - 1 = (\omega^p - 1)(1 + \omega^p + \omega^{2p} + \cdots + \omega^{p(p-1)}),$$

we get

$$1 + \omega^p + \omega^{2p} + \cdots + \omega^{p(p-1)} = 0.$$

So, combining (i), (ii), and (iii) we get

$$\sum_{\lambda \in (\mathbb{Z}_{p^2})^*} \omega^{\lambda f(x)} = \begin{cases} p^2 - p & \text{if } f(x) = 0 \\ -p & \text{if } f(x) \in p\mathbb{Z}_{p^2} \setminus \{0\} \\ 0 & \text{if } f(x) \in \mathbb{Z}_{p^2} \setminus p\mathbb{Z}_{p^2}. \end{cases} \tag{4.6}$$

Now, (4.6) and a change of the order of summations gives us

$$\sum_{\lambda \in (\mathbb{Z}_{p^2})^*} \left(\sum_{x \in \Omega} \omega^{\lambda f(x)} \right) = (p^2 - p)\big|\{x \in \Omega | f(x) = 0\}\big| - p\big|\{x \in \Omega | f(x) \in p\mathbb{Z}_{p^2} \setminus \{0\}\}\big|. \tag{4.7}$$

Putting this into the right-hand side of (4.2) we get

$$\begin{aligned} \text{R.H.S} &= (p-1)|\Omega| - \frac{1}{p} \sum_{\lambda \in (\mathbb{Z}_{p^2})^*} \left(\sum_{x \in \Omega} \omega^{\lambda f(x)} \right) \\ &= (p-1)|\Omega| - (p-1)\big|\{x \in \Omega | f(x) = 0\}\big| + \big|\{x \in \Omega | f(x) \in p\mathbb{Z}_{p^2} \setminus \{0\}\}\big| \\ &= (p-1)\Big[\big|\{x \in \Omega | f(x) \in (\mathbb{Z}_{p^2})^*\}\big| + \big|\{x \in \Omega | f(x) \in p\mathbb{Z}_{p^2} \setminus \{0\}\}\big|\Big] \\ &\quad + \big|\{x \in \Omega | f(x) \in p\mathbb{Z}_{p^2} \setminus \{0\}\}\big| \\ &= (p-1)\big|\{x \in \Omega | f(x) \in (\mathbb{Z}_{p^2})^*\}\big| + p\big|\{x \in \Omega | f(x) \in p\mathbb{Z}_{p^2} \setminus \{0\}\}\big| \\ &= w_{\text{hom}}(f). \end{aligned}$$

□

We define a non-degenerate polynomial from [7]:

Definition 4.2. A polynomial $g(x) \in GR(p^2, m)[x]$ is said to be *non-degenerate* if it cannot be written in the form

$$g(x) = \varphi(f(x)) - f(x) + u \pmod{p^2}$$

for any $f(x) \in GR(p^2, m)[x]$ and $u \in GR(p^2, m)$, and φ is the Frobenius map defined on the Galois ring $GR(p^2, m)$ as was defined in Section 2.2.

The following theorem is taken from [7] and is a main tool used in [2] and [8] as well.

Theorem 4.3. *Let $f(x) \in GR(p^\ell, m)[x]$ be non-degenerate and of weighted degree N_ℓ and suppose $\omega = e^{\frac{2\pi i}{p^\ell}}$. Suppose also that $\lambda \in \mathbb{Z}_{p^\ell}$ is relatively prime to p^ℓ. Then we have*

$$\left| \sum_{x \in T_m} w^{\lambda \mathrm{Tr}(f(x))} \right| \leq (N_\ell - 1) p^{m/2}.$$

We need to say something about the weighted degree here. If $f(x) \in GR(p^\ell, m)[x]$, then it has a unique p-adic expression in the form

$$f(x) = F_0(x) + pF_1(x) + \cdots + p^{\ell-1} F_{\ell-1}(x), \;\; F_j(x) \in T_m[x]$$

where T_m is the Teichmuller set defined in Section 2.2. Suppose $n_j = deg(F_j)$. Then the weighted degree of f is defined as

$$N_\ell = \max\{n_0 p^{\ell-1}, n_1 p^{\ell-2}, \ldots, n_{\ell-1}\}.$$

After these introductions, we are finally ready to define a ternary Gray map and construct ternary codes. We will define $G : \mathbb{Z}_9 \to \mathbb{Z}_3^3$ coordinate-wise, as follows:

$$\begin{aligned} G(0) &= (0,0,0), \;\; G(1) = (1,1,0), \;\; G(2) = (0,1,1), \\ G(3) &= (2,1,2), \;\; G(4) = (0,2,2), \;\; G(5) = (1,0,2), \\ G(6) &= (1,2,1), \;\; G(7) = (2,0,1), \;\; G(8) = (2,2,0). \end{aligned} \tag{4.8}$$

We then extend this map in the obvious way to $\mathbb{Z}_9^n$.

Remark 4.4. By straightforward calculations, we can obtain a very important property of this map G, that is, G is distance preserving:

$$d_{\text{hom}}(u,v) = d_{\text{H}}(G(u),G(v)) = w_{\text{H}}(G(u)-G(v)), \qquad u,v \in \mathbb{Z}_9 \tag{4.9}$$

where d_{H} and w_{H} denote the Hamming distance and the Hamming weight, respectively.

A construction of ternary codes using the Gray map

We will use the same technique that Carlet used in [8] to get some non-linear ternary codes as images. We will use linear trace codes. We define a linear code C over $\mathbb{Z}_9$ as follows:

$$C = \left\{ \left(b, \text{Tr}(a)+b, \text{Tr}(a\xi)+b, \ldots, \text{Tr}(a\xi^{3^m-2})+b\right) \middle| a \in GR(9,m), b \in \mathbb{Z}_9 \right\} \tag{4.10}$$

where $T_m = \{0, 1, \xi, \ldots, \xi^{3^m-2}\}$. Note that since Tr is a $\mathbb{Z}_9$-linear function, we see that C is a linear code over $\mathbb{Z}_9$ of length 3^m and of size 3^{2m+2}. We will prove the following theorem that gives us the construction we wanted:

Theorem 4.5. *Suppose that C is the linear $\mathbb{Z}_9$-code of length 3^m and of size 3^{2m+2} given by (4.10). Let $\tilde{C} = G(C)$, the Gray image of C. Then $\tilde{C}$ is a ternary $[3^{m+1}, 3^{2m+2}, \geq 2\cdot 3^m - 4\cdot 3^{m/2}]$ code.*

Proof. Let $F(x) = \text{Tr}(ax) + b$. Since $\text{Tr} : GR(9,m) \to \mathbb{Z}_9$ is onto by Lemma 3.17, we know that $\exists u \in GR(9,m)$ so that $\text{Tr}(u) = 1$. For such $u \in GR(9,m)$, we can then write $F(x) = \text{Tr}(ax+bu)$. But then, by Lemma 4.1, we see that

$$w_{\text{hom}}(F) = 2\cdot 3^m - \frac{1}{3}\sum_{\lambda \in (\mathbb{Z}_9)^*} \left(\sum_{x \in T_m} e^{\frac{2\lambda\pi i}{9}\text{Tr}(ax+bu)} \right). \tag{4.11}$$

By Theorem 4.3 however, we see that, for each $\lambda \in (\mathbb{Z}_9)^*$,

$$\left| \sum_{x \in T_m} e^{\frac{2\lambda\pi i}{9}\text{Tr}(ax+bu)} \right| \leq 2\cdot 3^{m/2} \tag{4.12}$$

since the weighted degree of $ax + bu$ is 3. Combining (4.11) and (4.12) we see that

$$w_h(F) \geq 2 \cdot 3^m - 4 \cdot 3^{m/2} \tag{4.13}$$

for each codeword $F \in C$. The theorem now follows from the fact that the Gray map $G : Z_9 \to \mathbb{Z}_3^3$ is distance preserving. □

Remark 4.6. This construction would yield good results for codes with large size. As an illustration of how good our construction is, we refer to [9] in which the authors obtained a linear ternary code with parameters [190, 10, 110], which has size 3^{10}. To match the size, we take $m = 4$ in our construction, which then yields a non-linear ternary code with parameters $[243, 3^{10}, \geq 126]$. This shows that our construction might lead to ternary codes with comparably large minimum distances, especially when the size of the code is high.

4.2 An Inductive Construction of a Gray Map from $\mathbb{Z}_{p^k}$ to $\mathbb{Z}_p^{p^{k-1}}$

In this section, we will give an inductive construction of a Gray map from $\mathbb{Z}_{p^k}$ to $\mathbb{Z}_p^{p^{k-1}}$. Since it is going to be inductive, let's denote this by $G_k : \mathbb{Z}_{p^k} \to \mathbb{Z}_p^{p^{k-1}}$. Obviously, we will take $G_1 = \mathbf{1}_{\mathbb{Z}_p}$, the identity map on $\mathbb{Z}_p$. We will define the Gray map coordinate-wise, which is going to be different than the way it is defined in [10] and [22]. Our definition is however equivalent to those definitions because ours is just going to be a permutation of their definitions. Since we want to have a distance-preserving map from $\mathbb{Z}_{p^k}$ with homogeneous weight to $\mathbb{Z}_p^{p^{k-1}}$ with the Hamming distance, let us recall how the homogeneous weight w_{hom} was defined on $\mathbb{Z}_{p^k}$.

$$w_{\text{hom}}(u) = \begin{cases} 0 & \text{if } u = 0 \\ (p-1)p^{k-2} & \text{if } u \in \mathbb{Z}_{p^k} \setminus p^{k-1}\mathbb{Z}_{p^k} \\ p^{k-1} & \text{if } u \in p^{k-1}\mathbb{Z}_{p^k} \setminus \{0\}. \end{cases}$$

Definition 4.7. We define the map for coordinates of $\mathbb{Z}_{p^k}$ for different types of elements:

$$G_k(j \cdot p^{k-1}) = \Big(G_{k-1}(j \cdot p^{k-2}), \ldots, G_{k-1}(j \cdot p^{k-2}) \Big), \qquad j = 0, 1, \ldots, p-1. \tag{4.14}$$

$$G_k((mp+j)p^{k-2}+i) = \Big(G_{k-1}\big(\gamma(mjp^{k-2}+i)\big), G_{k-1}\big(\gamma((m+1)jp^{k-2}+i)\big), \ldots, G_{k-1}\big(\gamma((m+p-1)jp^{k-2}+i)\big) \Big) \tag{4.15}$$

for $0 \le m, j \le p-1$ and for $1 \le i \le p^{k-2}-1$, where $\gamma(.)$ is the map that takes a number to its residue modulo p^{k-1}. Finally, for $0 \le j \le p-1$ and $1 \le n \le p-1$, we define

$$G_k(j \cdot p^{k-1} + np^{k-2}) = \Big(G_{k-1}\big(\gamma((j+n\cdot 0)p^{k-2})\big), G_{k-1}\big(\gamma((j+n\cdot 1)p^{k-2})\big), \ldots, G_{k-1}\big(\gamma((j+n(p-1))p^{k-2})\big) \Big). \tag{4.16}$$

The main result of this section is proving the distance-preserving property of this map.

Theorem 4.8. *The map G_k defined above is a distance-preserving map from*

$$\big(\mathbb{Z}_{p^k},\ \textit{homogeneous distance}\big)\ \textit{to}\ \big(\mathbb{Z}_p^{p^{k-1}},\ \textit{Hamming distance}\big).$$

Proof. The proof will be just exhausting all the cases and verifying the distance-preserving property for all these. There are several things to check here:

(i) $w_{\mathrm{H}}(G_k(u)) = p^{k-1}$ for $u \in p^{k-1}\mathbb{Z}_{p^k} \setminus \{0\}$, $w_{\mathrm{H}}(G_k(v)) = (p-1)p^{k-2}$ for $v \in \mathbb{Z}_{p^k} \setminus p^{k-1}\mathbb{Z}_{p^k}$ where w_{H} denotes the Hamming weight.

(ii) Suppose that $u, v \in p^{k-1}\mathbb{Z}_{p^k}$ with $u \neq v$. Then $d_{\mathrm{H}}(G_k(u), G_k(v)) = p^{k-1}$.

(iii) Suppose that $u, v \in \mathbb{Z}_{p^k} \setminus p^{k-1}\mathbb{Z}_{p^k}$. Then $d_{\mathrm{H}}(G_k(u), G_k(v)) = (p-1)p^{k-2}$ if $u - v \in \mathbb{Z}_{p^k} \setminus p^{k-1}\mathbb{Z}_{p^k}$ and $d_{\mathrm{H}}(G_k(u), G_k(v)) = p^{k-1}$ if $u - v \in p^{k-1}\mathbb{Z}_{p^k} \setminus \{0\}$. Moreover, if $u \in p^{k-1}\mathbb{Z}_{p^k}$ and $v \in \mathbb{Z}_{p^k} \setminus p^{k-1}\mathbb{Z}_{p^k}$, then $d_{\mathrm{H}}(G_k(u), G_k(v)) = (p-1)p^{k-2}$.

Note that if we prove (i), (ii), and (iii), then we will have proved

$$d_{\mathrm{H}}(G_k(u), G_k(v)) = w_{\mathrm{H}}(G_k(u) - G_k(v)) = d_{\mathrm{hom}}(u, v), \qquad u, v \in \mathbb{Z}_{p^k}, \tag{4.17}$$

which will prove that the Gray map G_k is indeed distance preserving.

Proof of (i) First of all, if $u \in p^{k-1}\mathbb{Z}_{p^k} \setminus \{0\}$, then this means that $u = j \cdot p^{k-1}$ for some $1 \leq j \leq p-1$, and hence by the definition of the Gray map, we get

$$G_k(u) = \big(G_{k-1}(j \cdot p^{k-2}), \ldots, G_{k-1}(j \cdot p^{k-2})\big).$$

So, we get

$$\begin{aligned} w_{\mathrm{H}}(G_k(u)) &= p \cdot w_{\mathrm{H}}(G_{k-1}(j \cdot p^{k-2})) \\ &= p \cdot p^{k-2} \\ &= p^{k-1} \end{aligned}$$

since by induction hypothesis, G_{k-1} is a distance-preserving map.

Now, suppose $u \in \mathbb{Z}_{p^k} \setminus p^{k-1}\mathbb{Z}_{p^k}$ and suppose we have $u = (mp + j) \cdot p^{k-2} + i$ where $0 \leq m, j \leq p-1$ and for some $1 \leq i \leq p^{k-2} - 1$. But then we note that

$$\gamma\big((m+r)jp^{k-2} + i\big) \neq 0, \pmod{p^{k-2}} \qquad r = 0, 1, \ldots, p-1$$

since $(m+r)jp^{k-2} \equiv 0 \pmod{p^{k-2}}$ but $i \neq 0 \pmod{p^{k-2}}$. But this means, since by induction hypothesis G_{k-1} is a distance-preserving map, that we have

$$w_{\mathrm{H}}\Big(G_{k-1}\big(\gamma((m+r)jp^{k-2} + i)\big)\Big) = (p-1)p^{k-3}, \qquad r = 0, 1, \ldots, p-1. \tag{4.18}$$

By the definition of G_k however, we see that by using (4.18), we get

$$\begin{aligned} w_{\mathrm{H}}\big(G_k(u)\big) &= \sum_{r=0}^{p-1} w_{\mathrm{H}}\Big(G_{k-1}\big(\gamma((m+r)jp^{k-2}+i)\big)\Big) \\ &= p(p-1)p^{k-3} \\ &= (p-1)p^{k-2} \end{aligned}$$

as expected.

Now, suppose that $u \in \mathbb{Z}_{p^k} \setminus p^{k-1}\mathbb{Z}_{p^k}$ and we have $u = j \cdot p^{k-1} + np^{k-2}$ for some $0 \leq j \leq p-1$ and $1 \leq n \leq p-1$. Then note that

$$\big\{j + n\cdot 0, j + n\cdot 1, \ldots, j + n(p-1)\big\} = \big\{0, 1, \ldots, p\big\} \pmod{p}$$

since $\mathrm{GCD}(n, p) = 1$. But this means that

$$\begin{aligned} &\big\{\gamma((j+n\cdot 0)p^{k-2}), \gamma((j+n\cdot 1)p^{k-2}), \gamma((j+n(p-1))p^{k-2})\big\} \\ &\qquad = \big\{0, p^{k-2}, 2p^{k-2}, \ldots, (p-1)p^{k-2}\big\} \pmod{p^{k-1}}. \end{aligned}$$

So, using the induction hypothesis that G_{k-1} is a distance-preserving map, we get

$$\begin{aligned} w_{\mathrm{H}}\big(G_k(u)\big) &= \sum_{r=0}^{p-1} w_{\mathrm{H}}\Big(G_{k-1}\big(\gamma((j+n\cdot r)p^{k-2})\big)\Big) \\ &= (p-1)p^{k-2} \end{aligned}$$

as expected.

Proof of (ii) Suppose that $u, v \in p^{k-1}\mathbb{Z}_{p^k}$ and that $u \neq v$. This means that $u = j_1 p^{k-1}$ and $v = j_2 p^{k-1}$ where $j_1 \neq j_2$ with both j_1 and j_2 being in $\big\{0, 1, \ldots, p-1\big\}$. Then by the definition of the Gray map, however, we have

$$G_k(u) = \big(G_{k-1}(j_1 p^{k-2}), G_{k-1}(j_1 p^{k-2}), \ldots, G_{k-1}(j_1 p^{k-2})\big) \tag{4.19}$$

and

$$G_k(v) = \big(G_{k-1}(j_2 p^{k-2}), G_{k-1}(j_2 p^{k-2}), \ldots, G_{k-1}(j_2 p^{k-2})\big). \tag{4.20}$$

But then by induction hypothesis we get

$$\begin{aligned} d_{\mathrm{H}}\big(G_k(u), G_k(v)\big) &= p \cdot d_{\mathrm{H}}\big(G_{k-1}(j_1 p^{k-2}), G_{k-1}(j_2 p^{k-2})\big) \\ &= p \cdot p^{k-2} \\ &= p^{k-1}. \end{aligned} \tag{4.21}$$

Proof of (iii) First, we assume that $u \in p^{k-1}\mathbb{Z}_{p^k} \setminus \{0\}$ and $v \in \mathbb{Z}_{p^k} \setminus p^{k-1}\mathbb{Z}_{p^k}$. Then we know $u = j_1 \cdot p^{k-1}$ for some $1 \leq j_1 \leq p-1$. Hence

$$G_k(u) = \big(G_{k-1}(j_1 p^{k-2}), \ldots, G_{k-1}(j_1 p^{k-2})\big). \tag{4.22}$$

Now, for v we can have two forms.

Suppose that $v = j_2 p^{k-1} + n p^{k-2}$ where $0 \leq j_2 \leq p-1$ and $1 \leq n \leq p-1$. Now using the definition of G_k and using the hypothesis that G_{k-1} is distance preserving, we see that

$$d_{\mathrm{H}}(G_k(u), G_k(v)) = \sum_{r=0}^{p-1} d_{\mathrm{H}}\Big(G_{k-1}\big(j_1 \cdot p^{k-2}\big), G_{k-1}\big(\gamma((j_2 + nr)p^{k-2})\big)\Big). \tag{4.23}$$

However, as r ranges over $0, 1, \ldots, p-1$ so does $n \cdot r$ modulo p, which means that

$$d_{\mathrm{H}}\Big(G_{k-1}\big(j_1 \cdot p^{k-2}\big), G_{k-1}\big(\gamma((j_2 + nr)p^{k-2})\big)\Big) = p^{k-2}$$

for all r except the one r for which we have $j_1 \equiv j_2 + nr \pmod{p}$. Putting this into (4.23), we get

$$d_{\mathrm{H}}\big(G_k(u), G_k(v)\big) = (p-1)p^{k-2} \tag{4.24}$$

as expected.

Now, suppose that $v = (mp + j_3)p^{k-2} + i$ with $0 \leq m, j_3 \leq p-1$ and $1 \leq i \leq p^{k-2} - 1$.

But this means that

$$j_1 p^{k-2} - \gamma\big((m+r)j_3 p^{k-2} + i\big) \in \mathbb{Z}_{p^{k-1}} \setminus p^{k-2}\mathbb{Z}_{p^{k-1}}$$

for all $r = 0, 1, \ldots, p-1$, which by induction hypothesis means that

$$d_{\mathrm{H}}\Big(G_{k-1}\big(j_1 \cdot p^{k-2}\big), G_{k-1}\big(\gamma((m+r)j_3 p^{k-2} + i)\big)\Big) = (p-1)p^{k-3}$$

for all $r = 0, 1, \ldots, p-1$ and hence we get

$$\begin{aligned} d_H(G_k(u), G_k(v)) &= \sum_{r=0}^{p-1} d_H\Big(G_{k-1}\big(j_1 \cdot p^{k-2}\big), G_{k-1}\big(\gamma((m+r)j_3 p^{k-2} + i)\big)\Big) \\ &= (p-1)p^{k-2} \end{aligned} \tag{4.25}$$

as expected.

We now assume that both $u, v \in \mathbb{Z}_{p^k} \setminus p^{k-1}\mathbb{Z}_{p^k}$. Then there are three possibilities as to the form of u and v:

(a) Suppose that $u = j_1 p^{k-1} + n_1 p^{k-2}$ and $v = j_2 p^{k-1} + n_2 p^{k-2}$ for $0 \leq j_1, j_2 \leq p-1$ and some $1 \leq n_1, n_2 \leq p-1$. Now if $u - v \in p^{k-1}\mathbb{Z}_{p^k}$, then this can happen only if $n_1 = n_2$. Since we assume $u \neq v$, we see that $j_1 \neq j_2$ in this case. This means that $(j_1 + n_1 r) - (j_2 + n_2 r) = j_1 - j_2 \neq 0 \pmod{p}$ for each $r = 0, 1, \ldots, p-1$. This means that, by induction hypothesis, we have

$$d_{\mathrm{H}}\Big(G_{k-1}\big(\gamma((j_1 + n_1 r)p^{k-2})\big), G_{k-1}\big(\gamma((j_2 + n_2 r)p^{k-2})\big)\Big) = p^{k-2}$$

for each $r = 0, 1, \ldots, p-1$. But then we see that

$$\begin{aligned} d_{\mathrm{H}}(G_k(u), G_k(v)) &= \sum_{r=0}^{p-1} d_{\mathrm{H}}\Big(G_{k-1}\big(\gamma((j_1 + n_1 r)p^{k-2})\big), G_{k-1}\big(\gamma((j_2 + n_2 r)p^{k-2})\big)\Big) \\ &= p^{k-1} \end{aligned}$$

as expected.

If, on the other hand, $u - v \in \mathbb{Z}_{p^k} \setminus p^{k-1}\mathbb{Z}_{p^k}$, then this means that $n_1 \neq n_2$. Hence we get

$$\big\{(j_1 + n_1 r) - (j_2 + n_2 r) \big| r = 0, 1, \ldots, p-1\big\} = \big\{0, 1, \ldots, p-1\big\} \pmod{p},$$

which means, by induction hypothesis, that

$$d_{\mathrm{H}}\bigg(G_{k-1}\big(\gamma((j_1 + n_1 r)p^{k-2})\big), G_{k-1}\big(\gamma((j_2 + n_2 r)p^{k-2})\big)\bigg) = p^{k-2}$$

for all r except the r for which we have $j_1 + n_1 r \equiv j_2 + n_2 r \pmod{p}$ for which the above distance is 0. Then we get

$$\begin{aligned} d_{\mathrm{H}}(G_k(u), G_k(v)) &= \sum_{r=0}^{p-1} d_{\mathrm{H}}\bigg(G_{k-1}\big(\gamma((j_1 + n_1 r)p^{k-2})\big), G_{k-1}\big(\gamma((j_2 + n_2 r)p^{k-2})\big)\bigg) \\ &= (p-1)p^{k-2} \end{aligned}$$

as expected.

(b) Suppose now that $u = (mp + j_1)p^{k-2} + i$ and $v = j_2 p^{k-1} + np^{k-2}$ for some $0 \leq m, j_1, j_2 \leq p-1$, $1 \leq n \leq p-1$ and $1 \leq i \leq p^{k-2} - 1$. One readily observes that in this case we must have $u - v \in \mathbb{Z}_{p^k} \setminus p^{k-1}\mathbb{Z}_{p^k}$. It is also obvious, from the presence of i that

$$(m + r)j_1 p^{k-2} + i - (j_2 + n \cdot r)p^{k-2} \neq 0 \pmod{p^{k-2}}$$

for all $r = 0, 1, \ldots, p-1$. This means that, by induction hypothesis, we have

$$d_{\mathrm{H}}\bigg(G_{k-1}\big(\gamma((m + r)j_1 p^{k-2} + i)\big), G_{k-1}\big(\gamma((j_2 + nr)p^{k-2})\big)\bigg) = (p-1)p^{k-3}$$

for all $r = 0, 1, \ldots, p-1$. So, then we have

$$\begin{aligned} d_{\mathrm{H}}(G_k(u), G_k(v)) &= \sum_{r=0}^{p-1} d_{\mathrm{H}}\bigg(G_{k-1}\big(\gamma((m + r)j_1 p^{k-2} + i)\big), G_{k-1}\big(\gamma((j_2 + nr)p^{k-2})\big)\bigg) \\ &= (p-1)p^{k-2} \end{aligned}$$

as expected.

(c) Suppose that $u = (m_1p + j_1)p^{k-2} + i_1$ and $v = (m_2p + j_2)p^{k-2} + i_2$, for some $0 \leq m_1, m_2, j_1, j_2 \leq p-1$ and $1 \leq i_1, i_2 \leq p^{k-2} - 1$.

First, we assume that $u - v \in p^{k-1}\mathbb{Z}_{p^k} \setminus \{0\}$. This can happen if and only if $i_1 = i_2$ and $j_1 = j_2$, but since we don't want u to be the same as v, we must have $m_1 \neq m_2$. But this means that

$$\big((m_1 + r)j_1p^{k-2} + i_1\big) - \big((m_2 + r)j_2p^{k-2} + i_2\big) \in p^{k-2}\mathbb{Z}_{p^{k-1}} \setminus \{0\}$$

for all $r = 0, 1, \ldots, p-1$. Hence, by induction hypothesis, since G_{k-1} is distance preserving, we see that

$$d_{\mathrm{H}}\Big(G_{k-1}\big(\gamma((m_1 + r)j_1p^{k-2} + i_1)\big), G_{k-1}\big(\gamma((m_2 + r)j_2p^{k-2} + i_2)\big)\Big) = p^{k-2}$$

for all $r = 0, 1, \ldots, p-1$. But then we will have

$$\begin{aligned} d_{\mathrm{H}}(G_k(u), G_k(v)) &= \sum_{r=0}^{p-1} d_{\mathrm{H}}\Big(G_{k-1}\big(\gamma((m_1 + r)j_1p^{k-2} + i_1)\big), G_{k-1}\big(\gamma((m_2 + r)j_2p^{k-2} + i_2)\big)\Big) \\ &= p^{k-1} \end{aligned}$$

as expected.

Now, assume that $u - v \in \mathbb{Z}_{p^k} \setminus p^{k-1}\mathbb{Z}_{p^k}$. This can happen only if $i_1 \neq i_2$ or $j_1 \neq j_2$ or both. Now, suppose $i_1 \neq i_2$. Then

$$\big((m_1 + r)j_1p^{k-2} + i_1\big) - \big((m_2 + r)j_2p^{k-2} + i_2\big) \in \mathbb{Z}_{p^{k-1}} \setminus p^{k-2}\mathbb{Z}_{p^{k-1}}$$

for each $r = 0, 1, \ldots, p-1$. Hence, by induction hypothesis, we see that

$$d_{\mathrm{H}}\Big(G_{k-1}\big(\gamma((m_1 + r)j_1p^{k-2} + i_1)\big), G_{k-1}\big(\gamma((m_2 + r)j_2p^{k-2} + i_2)\big)\Big) = (p-1)p^{k-3}$$

for all $r = 0, 1, \ldots, p-1$. So, we see that

$$\begin{aligned} d_{\mathrm{H}}(G_k(u), G_k(v)) &= \sum_{r=0}^{p-1} d_{\mathrm{H}}\Big(G_{k-1}\big(\gamma((m_1+r)j_1p^{k-2}+i_1)\big), G_{k-1}\big(\gamma((m_2+r)j_2p^{k-2}+i_2)\big)\Big) \\ &= (p-1)p^{k-2} \end{aligned}$$

as expected. If, on the other hand, we have $i_1 = i_2$, but $j_1 \neq j_2$, then we get

$$\Big\{ \big((m_1+r)j_1p^{k-2}+i_1\big) - \big((m_2+r)j_2p^{k-2}+i_2\big) \Big| r = 0, 1, \ldots, p-1 \Big\} = \\ \big\{0, p^{k-2}, \ldots, (p-1)p^{k-2}\big\} \pmod{p^{k-1}}$$

since $\mathrm{GCD}(j_1 - j_2, p) = 1$. But this means, since G_{k-1} is distance preserving, that,

$$d_{\mathrm{H}}\Big(G_{k-1}\big(\gamma((m_1+r)j_1p^{k-2}+i_1)\big), G_{k-1}\big(\gamma((m_2+r)j_2p^{k-2}+i_2)\big)\Big) = p^{k-2}$$

for all r except the $0 \leq r \leq p-1$ for which we have

$$\big((m_1+r)j_1p^{k-2}+i_1\big) - \big((m_2+r)j_2p^{k-2}+i_2\big) \equiv 0 \pmod{p^{k-1}}.$$

But then we get

$$\begin{aligned} d_{\mathrm{H}}(G_k(u), G_k(v)) &= \sum_{r=0}^{p-1} d_{\mathrm{H}}\Big(G_{k-1}\big(\gamma((m_1+r)j_1p^{k-2}+i_1)\big), G_{k-1}\big(\gamma((m_2+r)j_2p^{k-2}+i_2)\big)\Big) \\ &= (p-1)p^{k-2} \end{aligned}$$

as expected. □

4.3 A Combinatorial Construction of the Gray Map

In the previous section, we introduced an algebraic construction of a Gray map from $\mathbb{Z}_{p^k}$ to $\mathbb{Z}_p^{p^{k-1}}$ that is distance preserving. In this section, we want to give a purely combinatorial construction using Affine geometries. So, we will divide this section into two parts, the first

part consisting of an introduction about Affine geometries and the second part consisting of the construction of the Gray map.

Affine geometries

Most of the material presented here was taken from [6]. An *Affine space* $AG_k(p)$ of order k over $\mathbb{F}_p$ is defined to be the set $V = \mathbb{F}_p^k$ of all points and all Affine subspaces of V. An *Affine subspace* of V is the empty set or a linear vector subspace of V or a coset of a linear subspace of V in the additive group.

An *Affine Hyperplane* in $AG_k(p)$ is defined to be an Affine subspace of V of dimension $k-1$. We observe the following remark:

Remark 4.9. Two hyperplanes in $AG_k(p)$ are either disjoint or they intersect in an Affine subspace of dimension $k-2$.

Definition 4.10. Suppose A, B are hyperplanes in $AG_k(p)$. We say that A and B are *parallel* if $A = B$ or A and B are disjoint. We denote this by writing $A \sim B$.

Lemma 4.11. *The relation $\sim$ on the set of all hyperplanes of $AG_k(p)$ is an equivalence relation.*

Proof. Since reflection and symmetry are obvious, we will try to prove transitiveness. So, suppose $A \sim B$ and $B \sim C$. If $A = B$ or $B = C$, then we obviously get $A \sim C$. So, suppose that $A \neq B$, and also $B \neq C$. Suppose for contradiction that $A \cap C \neq \emptyset$. Then $A \cap C$ is a $(k-2)$-dimensional Affine subspace of V. Now we know, from basic properties of Affine geometry, that the hyperplanes that contain $A \cap C$ partition the rest of the points in V. Hence there are a total of

$$\frac{p^k - p^{k-2}}{p^{k-1} - p^{k-2}} = p + 1$$

hyperplanes that contain $A \cap C$; call them $A, C, H_1, \ldots, H_{p-1}$. Now, $A, C, H_1, \ldots, H_{p-1}$ partition the rest of the points in V means, since $A \cap B = C \cap B = \emptyset$, that all the points in B lie in the hyperplanes $H_1, H_2, \ldots, H_{p-1}$. But, notice that $H_j \neq B$ for $j = 1, \ldots, p-1$ because H_j's intersect with A and C. But $H_j \cap B$ then can have at most p^{k-2} points, which means that $H_1, H_2, \ldots, H_{p-1}$ can contain at most $(p-1)p^{k-2}$ of the points in B, which is a contradiction since $|B| = p^{k-1}$. □

Let us define, by a *parallel class* of a hyperplane A, the equivalence class $\bar{A}$ of A with respect to $\sim$. The following lemma will be quite useful.

Lemma 4.12. *There are exactly p hyperplanes in each parallel class and there are $p^{k-1} + p^{k-2} + \cdots + p + 1$ parallel classes in $AG_k(p)$.*

Proof. Suppose A is a hyperplane. Then all cosets of A in the additive group are also hyperplanes. We know from group theory that two cosets of the same subgroup are either identical or disjoint. Since each element in V is in some coset of A, we see that there are at least p distinct cosets of A, but since distinct cosets are disjoint, it follows that there are exactly p disjoint cosets of A. Since two disjoint cosets are parallel, we see that the disjoint cosets of A make up the whole set $\bar{A}$ and hence the first part of the lemma is proved.

For the second part of the lemma, we observe that the number of parallel classes of hyperplanes is exactly the same as the number of $(k-1)$-dimensional vector subspaces of V, which is the same as

$$\begin{bmatrix} k \\ k-1 \end{bmatrix}_p = \frac{(p^k-1)(p^{k-1}-1)\dots(p^2-1)}{(p^{k-1}-1)(p^{k-2}-1)\dots(p-1)} = \frac{p^k-1}{p-1}.$$

□

Now, let's look at the parallel classes of lines. We know that in each parallel class of lines, there are exactly p^{k-1} lines. Let's fix one such parallel class in $AG_k(p)$. Suppose it is

$$\bar{L} = \{L_0, L_1, \dots, L_{p^{k-1}-1}\}$$

where each L_j is a line in the Affine space $AG_k(p)$. Let's write the lines in this parallel class as columns and let us label each element in each line with numbers in $\{0, 1, \dots, p-1\}$.

$$\bar{L} = \left\{ \begin{pmatrix} 0 \\ 1 \\ \vdots \\ p-1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ p-1 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ p-1 \end{pmatrix} \right\} \tag{4.26}$$

where we have p^{k-1} columns lined up above.

We observe that, if a hyperplane contains two points from a line, it contains the whole line. So, each hyperplane that doesn't contain any of the lines $L_0, L_1, \ldots, L_{p^{k-1}-1}$ contains exactly one point from each column in (4.26). Using this observation we will prove the following quick lemma:

Lemma 4.13. *Suppose that a hyperplane A doesn't contain any of the lines $L_0, L_1, \ldots, L_{p^{k-1}-1}$. If $B \in \bar{A}$ is any hyperplane, then B doesn't contain any of the lines $L_0, \ldots, L_{p^{k-1}-1}$ either.*

Proof. If $B \in \bar{A}$, this means that B and A are disjoint. By the above observation, we know that A must contain exactly one point from each line L_j, $j = 0, 1, \ldots, p^{k-1} - 1$. But if B contains one of the lines L_j, then we would have $A \cap B \neq \emptyset$, contradicting the fact that A and B are disjoint. □

Remark 4.14. The result of Lemma 4.13 implies that the hyperplanes that don't contain any of the lines $L_0, L_1, \ldots, L_{p^{k-1}-1}$ are partitioned into parallel classes of hyperplanes.

The following lemma will give us the number of hyperplanes that don't contain any of the lines:

Lemma 4.15. *There are exactly p^{k-1} parallel classes of hyperplanes that don't contain any of the lines $L_0, L_1, \ldots, L_{p^{k-1}-1}$, or equivalently there are exactly p^k hyperplanes that don't contain any of the lines $L_0, L_1, \ldots, L_{p^{k-1}-1}$.*

Proof. Since, by lemma 4.13, we know that the hyperplanes that don't contain any of the lines $L_0, L_1, \ldots, L_{p^{k-1}-1}$ are partitioned into parallel classes, we see that the hyperplanes that contain at least one of the lines $L_0, L_1, \ldots, L_{p^{k-1}-1}$ are also partitioned into parallel classes. So, the number of parallel classes of hyperplanes that contain at least one of the lines in $L_0, L_1, \ldots, L_{p^{k-1}-1}$ is the same as the number of $(k-1)$-dimensional subspaces of a k-dimensional vector space that contains a particular line, which is

$$\frac{p^{k-1}-1}{p-1} = p^{k-2} + p^{k-3} + \cdots + 1.$$

This means, however, that the number of the parallel classes of hyperplanes that don't contain any of the lines $L_0, L_1, \ldots, L_{p^{k-1}-1}$ is

$$(p^{k-1} + p^{k-2} + \cdots + p + 1) - (p^{k-2} + \cdots + p + 1) = p^{k-1}.$$

□

The Construction of G_k

Assume that $\Gamma_0, \Gamma_1, \ldots, \Gamma_{p^{k-1}-1}$ are the parallel classes of the hyperplanes that don't contain any of the lines $L_0, L_1, \ldots, L_{p^{k-1}-1}$. So, each hyperplane in these parallel classes is formed by taking one element from each column of (4.26). Suppose, without loss of generality that we have labelled (4.26) in such a way that there exists a hyperplane that corresponds to a labelling of $(0, 0, \ldots, 0)$ and that it is in Γ_0. From now on, by the vector that corresponds to a hyperplane, we will mean the $\{0, 1, \ldots, p-1\}$-vector of length p^{k-1}, which comes from the labelling of the elements of the hyperplane in accordance with the labelling of (4.26). So now we are finally ready to describe the Gray map $G_k : \mathbb{Z}_{p^k} \to (\mathbb{Z}_p)^{p^{k-1}}$.

Definition 4.16. For $u = jp^{k-1}$, $j = 0, 1, \ldots, p-1$, G_k maps u to the vector of the hyperplanes of Γ_0 bijectively in such a way that 0 is mapped to the hyperplane $(0, 0, \ldots, 0)$.

For $1 \leq j \leq p^{k-1} - 1$, we map $j, p^{k-1} + j, \ldots, (p-1)p^{k-1} + j$ to the vectors of the hyperplanes of Γ_j bijectively.

Note that this is a well-defined map from $\mathbb{Z}_{p^k}$ to $\mathbb{Z}_p^{p^{k-1}}$.

Theorem 4.17. *The map G_k defined above is indeed a distance-preserving map from $\mathbb{Z}_{p^k}$ with the homogeneous distance to $(\mathbb{Z}_p)^{p^{k-1}}$ with the Hamming distance.*

Proof. Suppose $u \in p^{k-1}\mathbb{Z}_{p^k} \setminus \{0\}$. Then this means that $G_k(u)$ is the vector of a hyperplane in Γ_0 that is disjoint from the hyperplane of $(0, 0, \ldots, 0)$. But this means that $G_k(u)$ doesn't have any zeros, which means that

$$w_{\mathrm{H}}(G_k(u)) = p^{k-1}.$$

If $v \in \mathbb{Z}_{p^k} \setminus p^{k-1}\mathbb{Z}_{p^k}$, then $G_k(v)$ is the vector of a hyperplane in some Γ_j with $j \neq 0$. But since any hyperplane in Γ_j will intersect with any hyperplane in Γ_0 in exactly p^{k-2} points and since $(0, 0, \ldots, 0)$ belongs to a hyperplane in Γ_0, we see that $G_k(v)$ has to have exactly p^{k-2} 0's. Hence we see that

$$w_{\mathrm{H}}(G_k(v)) = p^{k-1} - p^{k-2} = (p-1)p^{k-2}.$$

Now, suppose $u, v \in \mathbb{Z}_{p^k}$ so that $u - v \in p^{k-1}\mathbb{Z}_{p^k} \setminus \{0\}$. This means that $u \equiv v \pmod{p^{k-1}}$. Then by the construction of G_k, we see however that $G_k(u)$ and $G_k(v)$ come from two distinct hyperplanes in the same parallel class Γ_j for some j. But this means that $G_k(u)$ and $G_k(v)$ are different in each coordinate since their hyperplanes are disjoint, which means that

$$d_{\mathrm{H}}(G_k(u), G_k(v)) = p^{k-1}.$$

Suppose now that $u - v \in \mathbb{Z}_{p^k} \setminus p^{k-1}\mathbb{Z}_{p^k}$ and hence u and v are in different residue classes modulo p^{k-1}. This means that $G_k(u)$ and $G_k(v)$ correspond to hyperplanes from Γ_{j_1} and Γ_{j_2}, respectively, where $j_1 \neq j_2$. But since two hyperplanes from different parallel classes must necessarily intersect, and since they intersect in a $(k-2)$-dimensional Affine subspace, we see that $G_k(u)$ and $G_k(v)$ will have exactly p^{k-2} coordinates where the entries are equal. Hence we see that

$$d_{\mathrm{H}}(G_k(u), G_k(v)) = p^{k-1} - p^{k-2} = (p-1)p^{k-2}.$$

□

Note that, by the exact same methods that we applied above, we can come up with a combinatorial construction of a distance-preserving map from the Galois ring $GR(p^\ell, m)$ to $\mathbb{F}_{p^m}^{p^{(\ell-1)m}}$. The tools will be very similar; we will use the Affine geometry $AG_\ell(p^m)$.

4.4 Gray Maps over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ and the Lee Weight

In this section, we will study the linear codes over the ring $R_m = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ with $u^2 = 0$. Linear codes over these rings were studied in [11] by Betsumiya and Ling. We first introduce a special notion of a basis:

Definition 4.18. Suppose $B = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ is a basis for $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. We say that B is a *Trace Orthogonal Basis* (TOB), or *self-dual basis* if we have

$$\mathrm{tr}(\alpha_i \cdot \alpha_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{of } i \neq j \end{cases}$$

where tr is the usual Trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$.

Remark 4.19. By [23], there exist TOBs for $\mathbb{F}_{2^m}$ for all $m > 1$.

At this point, we will define some different types of Gray maps. First define

$$\psi'_{m,1} : \mathbb{F}_{2^m}^n \to \mathbb{F}_2^{mn}$$

with respect to a TOB B, as

$$\psi'_{m,1}(x_1\alpha_1 + x_2\alpha_2 + \cdots + x_m\alpha_m) = (x_1, x_2, \ldots, x_m) \tag{4.27}$$

where $x_1, x_2, \ldots, x_m$ are vectors in $\mathbb{F}_2^n$. We also define

$$\phi_m : R_m^n \to \mathbb{F}_{2^m}^{2n}$$

by letting

$$\phi_m(x + uy) = (y, x + y) \tag{4.28}$$

where x, y are vectors in $\mathbb{F}_{2^m}^n$.

Definition 4.20. A *linear code* over the ring $R_m = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ of length n is an R_m-submodule of R_m^n.

We will next define the Lee weight for such codes.

Definition 4.21. Suppose $B = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ is a TOB of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. Then for $x = x_1\alpha_1 + \cdots + x_m\alpha_m \in \mathbb{F}_{2^m}$, the *Lee weight* of x with respect to the basis B is defined to be the number of x_j's that are non-zero. The weight $w_{\mathrm{L}}^{\mathrm{B}}$ of $x = a + ub \in R_m$ is defined to be the sum of the Lee weight of $b \in \mathbb{F}_{2^m}$ and that of $a + b \in \mathbb{F}_{2^m}$.

We define an analogous Gray map

$$\psi_{m,1} : R_m^n \to R_1^{mn}$$

such that

$$\psi_{m,1}(x_1\alpha_1 + \cdots + x_m\alpha_m) = (x_1, x_2, \ldots, x_m)$$

where $x_1, x_2, \ldots, x_m$ are vectors in R_1^n. The way the weight is defined, it is easy to see that $\psi_{m,1}$ is Lee weight-preserving. Note that the Lee weight on $\mathbb{F}_2 + u\mathbb{F}_2$ is defined to be $w_{\mathrm{L}}(0) = 0$, $w_{\mathrm{L}}(1) = w_{\mathrm{L}}(1+u) = 1$, $w_{\mathrm{L}}(u) = 2$. We summarize some of the properties of the map $\psi_{m,1}$ in the following lemma:

Lemma 4.22. *(i) $\psi_{m,1}$ is an $\mathbb{F}_2 + u\mathbb{F}_2$-linear map.*
(ii) $\psi_{m,1}$ is a weight-preserving map where the map in R_m is the Lee weight defined with respect to the TOB B, and the weight for R_1 is the usual Lee weight.
(iii) $\psi_{m,1}$ is an injective map.

Proof. Let

$$c_1 = x_1\alpha_1 + \cdots + x_m\alpha_m, \;\; c_2 = y_1\alpha_1 + \cdots + y_m\alpha_m \in R_m^n.$$

It is enough to show that $\psi_{m,1}(c_1+c_2) = \psi_{m,1}(c_1)+\psi_{m,1}(c_2)$ and that $\psi_{m,1}(uc_1) = u\psi_{m,1}(c_1)$. Now,

$$\begin{aligned}
\psi_{m,1}(c_1 + c_2) &= \psi_{m,1}\big((x_1 + y_1)\alpha_1 + \cdots + (x_m + y_m)\alpha_m\big) \\
&= (x_1 + y_1, \ldots, x_m + y_m) \\
&= (x_1, \ldots, x_m) + (y_1, \ldots, y_m) \\
&= \psi_{m,1}(c_1) + \psi_{m,1}(c_2).
\end{aligned}$$

We also have

$$\begin{aligned}\psi_{m,1}(uc_1) &= \psi_{m,1}\big((ux_1)\alpha_1 + (ux_2)\alpha_2 + \cdots + (ux_m)\alpha_m\big)\\ &= (ux_1, ux_2, \ldots, ux_m)\\ &= u(x_1, x_2, \ldots, x_m)\\ &= u\psi_{m,1}(c_1).\end{aligned}$$

This proves the first part of the lemma, and the second part of the lemma just follows from the definition of the Lee weight on R_m.
For part (iii), we note that if $\psi_{m,1}(c_1) = \psi_{m,1}(c_2)$, then this means that $x_i = y_i$ for all i, which means that $c_1 = c_2$. □

The following theorem is a similar result obtained for linear codes over $\mathbb{Z}_4$ in Chapter 2, and the proof is exactly in the same lines and so will be omitted here:

Theorem 4.23. *Suppose that C is a linear code of type $(4)^{k_1}(2)^{k_2}$ over $\mathbb{F}_2+u\mathbb{F}_2$. If $N_C^{\mathrm{L}}(j, 2^e)$ denotes the number of codewords in C that have Lee weights congruent to j modulo 2^e, then*

$$N_C^{\mathrm{L}}(j, 2^e) \equiv 0 \pmod{2^q}, \qquad j = 0, 1, \ldots, 2^e - 1$$

where

$$q = \left\lfloor \frac{k_1 + k_2 - 2^{e-2}}{2^{e-2}} \right\rfloor$$

for all $e \geq 2$. Moreover,

$$N_C^{\mathrm{L}}(j, 2) \equiv 0 \pmod{2^{2k_1+k_2-1}}, \qquad j = 0, 1.$$

Now, suppose that C is a linear code over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ of length n. Then by [13], C is permutationally equivalent to a code with a generator matrix

$$G = \begin{bmatrix} I_{k_1} & A & B_1 + uB_2 \\ 0 & uI_{k_2} & uD \end{bmatrix}$$

where A, B_1, B_2, D are all $\mathbb{F}_{2^m}$-matrices. This means that our linear code C is a linear code of type $(2^{2m})^{k_1}(2^m)^{k_2}$ for some k_1 and k_2 nonnegative integers. We want to resolve the question of the Lee weights of C modulo 2^e as we did for $\mathbb{F}_2 + u\mathbb{F}_2$-codes above. Our basic tool will be to reduce the situation to the case of $\mathbb{F}_2 + u\mathbb{F}_2$-codes by using the Gray map $\psi_{m,1}$. We know that the weights are going to be preserved and, also by Lemma 4.22, we know that the image will be a linear code over $\mathbb{F}_2 + u\mathbb{F}_2$. But in order to get the results, we need to understand what kind of a linear code we get as the image of C under the map $\psi_{m,1}$. For this, we have the following lemma:

Lemma 4.24. *Suppose that C is a linear code over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ of type $(2^{2m})^{k_1}(2^m)^{k_2}$ and of length n. Then, $\psi_{m,1}(C)$ is a linear code over $\mathbb{F}_2 + u\mathbb{F}_2$ of type $(4)^{mk_1}(2)^{mk_2}$ of length mn.*

Proof. Suppose that $\psi_{m,1}(C)$ has type $(4)^r(2)^s$ for some non-negative integers r, s. The first observation we make is that, since by Lemma 4.22, $\psi_{m,1}$ is an injective map, the size of $\psi_{m,1}(C)$ has to be the same as the size of C. This gives us the following equation:

$$2mk_1 + mk_2 = 2r + s. \tag{4.29}$$

Now, suppose C has the generating matrix given above, and let the rows of the generating matrix be $c_1, c_2, \ldots, c_{k_1}, b_1, b_2, \ldots, b_{k_2}$. Let $\tilde{C}$ be the subcode of C generated by

$$\{uc_1, uc_2, \ldots, uc_{k_1}, b_1, b_2, \ldots, b_{k_2}\}.$$

Then $\tilde{C}$ is a linear subcode of C. In fact it is the largest $u\mathbb{F}_{2^m}$-subcode of C. Because if some non-$u\mathbb{F}_{2^m}$ combination of $c_1, c_2, \ldots, c_m$ were in $(u\mathbb{F}_{2^m})^n$, then multiplying the combination by u would yield a nontrivial combination of $c_1, c_2, \ldots, c_m$ being 0, contradicting the fact that they are linearly independent. This means that all the codewords in C that are in $(u\mathbb{F}_{2^m})^n$ are in $\tilde{C}$, which is a linear code of type $(2^m)^{k_1+k_2}$. Now, since $\psi_{m,1}$ is a $\mathbb{F}_2 + u\mathbb{F}_2$-linear map, all the codewords in $\psi_{m,1}$(C) that are in $(u\mathbb{F}_2)^{mn}$ come from $\tilde{C}$. Now, the type of $\psi_{m,1}(C)$ implies that there are exactly 2^{r+s} such codewords in $\psi_{m,1}(C)$. But since $\psi_{m,1}$ is an injective map, the size of such codewords in $\psi_{m,1}(C)$ has to be exactly the same as

the size of $\tilde{C}$, so this gives us another equation:

$$mk_1 + mk_2 = r + s. \tag{4.30}$$

So now, combining equations (4.29) and (4.30), we get

$$r = mk_1, \quad s = mk_2$$

as desired. □

We are now ready to introduce the following corollary to Theorem 4.23:

Corollary 4.25. *Suppose that C is a linear code of type $(2^{2m})^{k_1}(2^m)^{k_2}$ over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$. If $N_C^{\mathrm{L}}(j, 2^e)$ denotes the number of codewords in C that have Lee weights with respect to a given TOB $B = \{\alpha_1, \ldots, \alpha_m\}$ congruent to j modulo 2^e, then*

$$N_C^{\mathrm{L}}(j, 2^e) \equiv 0 \pmod{2^q}, \qquad j = 0, 1, \ldots, 2^e - 1$$

where

$$q = \left\lfloor \frac{mk_1 + mk_2 - 2^{e-2}}{2^{e-2}} \right\rfloor$$

for all $e \geq 2$. Moreover,

$$N_C^{\mathrm{L}}(j, 2) \equiv 0 \pmod{2^{2mk_1 + mk_2 - 1}}, \qquad j = 0, 1.$$

Proof. This result follows directly from Theorem 4.23 by using Lemma 4.22 and Lemma 4.24. □

We will also be interested in proving that the result in Corollary 4.25 is best possible. To do this, we need to understand the weight of a codeword with respect to a given TOB $B = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$.

Suppose $\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_r} \in \mathbb{F}_{2^m}$ is fixed with $1 \leq i_1 < i_2 < \cdots < i_r \leq m$. We will be

interested in the Lee weight with respect to B of

$$\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_r} + u(y_1\alpha_1 + y_2\alpha_2 + \ldots y_m\alpha_m)$$

where $y_1, y_2, \ldots, y_m$ runs through $\mathbb{F}_2$. Note that the Lee weight of such a coordinate is the Lee weight of

$$\big(y_1\alpha_1 + y_2\alpha_2 + \cdots + y_m\alpha_m, (x_1 \oplus y_1)\alpha_1 + (x_2 \oplus y_2)\alpha_2 + \cdots + (x_m \oplus y_m)\alpha_m\big)$$

where $\oplus$ denotes the summation modulo 2 and where $x_i = 1$ for all $i \in \{i_1, i_2, \ldots, i_r\}$ and 0 otherwise. Then, it follows that the Lee weight with respect to B of such a coordinate is

$$y_1 + y_2 + \cdots + y_m + (1 - y_{i_1}) + \cdots + (1 - y_{i_r}) + \left|\left\{ j \in \{1, 2, \ldots, m\} \setminus \{i_1, \ldots, i_r\} \middle| y_j = 1 \right\}\right|.$$

So the Lee weights with respect to B of the set of coordinates of the form

$$\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_r} + u(y_1\alpha_1 + y_2\alpha_2 + \ldots y_m\alpha_m)$$

where $y_1, y_2, \ldots, y_m$ runs through $\mathbb{F}_2$ is the set

$$\big\{2(z_1 + z_2 + \cdots + z_{m-r}) + r \big| z_1, \ldots, z_{m-r} \in \mathbb{F}_2\big\},$$

for all $y_{i_1}, \ldots, y_{i_r} \in \mathbb{F}_2$. This means that if

$$C = \left(\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}\right)^k,$$

then the Lee weight distribution polynomial of C is

$$P_C(z) = \left[\sum_{r=0}^{m}\sum_{j=0}^{m-r}\binom{m}{r}\binom{m-r}{j}2^r z^{2j+r}\right]^k. \tag{4.31}$$

Writing up the sums in their orders we get

$$\begin{aligned}\sum_{r=0}^{m}\sum_{j=0}^{m-r}\binom{m}{r}\binom{m-r}{j}2^r z^{2j+r} &= \sum_{r=0}^{m}\binom{m}{r}2^r z^r \sum_{j=0}^{m-r} z^{2j} \\ &= \sum_{r=0}^{m}\binom{m}{r}(2z)^r(1+z^2)^{m-r} \\ &= (1+2z+z^2)^m \\ &= (1+z)^{2m}.\end{aligned}$$

This means that, for

$$C = \Big(\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}\Big)^k,$$

the weight distribution polynomial $P_C(z)$ of C is simply given by

$$P_C(z) = (1+z)^{2mk}. \tag{4.32}$$

Now, what happens if we take an element of the form $u(\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_r})$ for $0 \le r \le m$. Then its Lee weight with respect to B is the weight of

$$(\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_r}, \alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_r}),$$

which is $2r$. So the Lee weight distribution polynomial of $C_u = \big(u\mathbb{F}_{2^m}\big)^k$ is

$$P_C(z) = \Big(\sum_{r=0}^{m}\binom{m}{r}z^{2r}\Big)^k = (1+z^2)^{mk}. \tag{4.33}$$

We are now ready to prove the following theorem:

Theorem 4.26. *The result in Corollary 4.25 is best possible.*

Proof. Let us take the trivial block code

$$C = \big(\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}\big)^{k_1}\big(u\mathbb{F}_{2^m}\big)^{k_2}. \tag{4.34}$$

Then, by (4.32) and (4.33), the Lee weight distribution polynomial of C is given by

$$P_C(z) = (1+z)^{2mk_1}(1+z^2)^{mk_2}. \tag{4.35}$$

This can be written as

$$(1+2z+z^2)^{mk_1}(1+z^2)^{mk_2} = (1+z^2)^{mk_1+mk_2} + 2z \cdot A(1+z^2)^{mk_1+mk_2-1} + 4z^2 \cdot B(1+z^2)^{mk_1+mk_2-2} + \dots$$

where A and B are polynomials with integer coefficients. Now, by Corollary 2.14, we know that the coefficients of $(1+z^2)^k$ modulo $z^{2^e}-1$ are strictly divisible by 2^q where

$$q = \left\lfloor \frac{k-2^{e-2}}{2^{e-2}} \right\rfloor.$$

But since

$$j + \left\lfloor \frac{mk_1+mk_2-j-2^{e-2}}{2^{e-2}} \right\rfloor > \left\lfloor \frac{mk_1+mk_2-2^{e-2}}{2^{e-2}} \right\rfloor$$

for all $e > 2$ and $j \geq 1$,we see that

$$\min\left\{ \nu_2\big(N_C^{\mathrm{L}}(j,2^e)\big) \,\middle|\, j = 0,1,\dots,2^e-1 \right\} = \left\lfloor \frac{mk_1+mk_2-2^{e-2}}{2^{e-2}} \right\rfloor \tag{4.36}$$

for all $e > 2$, which proves that the result in Corollary 4.25 is best possible when $e > 2$.

For $e = 1$, we have

$$\begin{aligned} P_C(z) &= (1+z)^{2mk_1}(1+z^2)^{mk_2} \\ &\equiv 2^{mk_2}(1+z)^{2mk_1} \\ &\equiv 2^{2mk_1+mk_2-1} + 2^{2mk_1+mk_2-1}z \pmod{z^2-1}. \end{aligned}$$

This means that the result in Corollary 4.25 is best possible for $e = 1$.

Just as in Chapter 2, the case when $e = 2$ will be considered separately. We will take

in this case

$$C_2 = \left(\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}\right)^{k_1} \times C_{k_2}$$

where C_{k_2} is the k_2-dimensional $u\mathbb{F}_{2^m}$-code that is generated by

$$\big\{(u,0,0,\ldots,0,u),(0,u,0,0,\ldots,0,u),\ldots,(0,0,\ldots,0,u,u)\big\}.$$

It can easily be seen that any codeword in C_{k_2} has a Lee weight that is divisible by 4, which means that, modulo z^4-1, we will have

$$P_{C_2}(z) \equiv 2^{mk_2}(1+z)^{2mk_1} \pmod{z^4-1},$$

but then by Corollary 2.14, the coefficients of $(1+z)^{2mk_1}$ modulo z^4-1 are strictly divisible by 2^{mk_1-1}, which means that the coefficients of $P_C(z)$, modulo z^4-1, are strictly divisible by $2^{mk_1+mk_2-1}$, which proves that the result in Corollary 4.25 is best possible for $e=2$ as well. □

Remark 4.27. Comparing the results obtained in Chapter 2 for linear $\mathbb{Z}_4$-codes with the results obtained in this section for linear codes over $\mathbb{F}_2+u\mathbb{F}_2$, we see that the results are exactly the same. In fact, these two rings are very similar, with the u in $\mathbb{F}_2+u\mathbb{F}_2$ working like the 2 in $\mathbb{Z}_4$. But there is one major difference between the two rings. The Gray map defined from $\mathbb{F}_2+u\mathbb{F}_2$ to $\mathbb{F}_2^2$ is a linear isometry while the Gray map defined from $\mathbb{Z}_4$ to $\mathbb{F}_2^2$ is not a linear map. More on this will be said in the next chapter.

Remark 4.28. While $\mathbb{F}_2+u\mathbb{F}_2$ is very similar to $\mathbb{Z}_4$, the extension of the Lee weight to the ring $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ is not a homogeneous weight unlike the extension of the Lee weight from $\mathbb{Z}_4$ to the Galois rings that we used in Chapter 2. In this aspect, the results that we obtained in this section, in particular the ones summarized in Corollary 4.25, are different than the results obtained in Chapter 2.

Chapter 5

Gray Images of Linear Codes and Permutation Invariance of Binary Codes

In this chapter we will see some applications of the Gray map in linking the invariance of some binary codes under some permutations with linearity over certain rings. The motivation for this chapter came from [2], in which the authors found necessary and sufficient conditions for a binary code to be the Gray image of a linear code over $\mathbb{Z}_4$. Using this, they reached some results about $\mathbb{Z}_4$-linearity of Reed-Muller codes that can be summarized in the following theorem:

Theorem 5.1. ([2]) *The rth order binary Reed-Muller code $RM(r, m)$ of length $n = 2^m, m \geq 1$, is $\mathbb{Z}_4$-linear for $r = 0, 1, 2, m-1, m$.*

When r doesn't have the form in Theorem 5.1, they conjectured that $RM(r, m)$ is not $\mathbb{Z}_4$-linear, and they proved this when $r = m - 2$.

In both [11] and [13], the authors linked linearity over the rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ with the so-called *swap map*, which essentially is the permutation group $\mathbb{Z}_2$, and so this led us to consider the question of whether the Reed-Muller codes are linear over these rings.

In section 1 we will give a brief introduction about permutations of binary codes in section 2, we will consider the connection between permutation invariance and linearity over certain rings, and in section 3 we will consider the Reed-Muller codes and we will answer the question about these codes being linear over the rings previously studied. In section 4 we will find the exact pre-images of the Reed-Muller codes that are linear over the

rings considered in section 2. In the last part of the chapter, we will settle the question of invariance of Reed-Muller codes under the permutation group $\mathbb{Z}_{2^k}$ and we will also consider linear codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{2^k-1}\mathbb{F}_2$.

5.1 Permutations of Binary Codes

Suppose that C is a binary code of length n. Then we know that the permutation group S_n acts on this code by acting on the coordinates. Suppose $\tau \in S_n$ is a permutation, and $\overline{c} = (c_1, c_2, \ldots, c_n) \in C$ is a codeword in C. Then

$$\tau(\overline{c}) = (c_{\tau(1)}, c_{\tau(2)}, \ldots, c_{\tau(n)}). \tag{5.1}$$

Definition 5.2. Suppose C is a binary code of length n. Then, for $\tau \in S_n$, we say that C is *invariant* under τ if

$$\tau(C) = C.$$

We will say C is invariant under a subgroup H of S_n if C is invariant under τ, for all $\tau \in H$, i.e.,

$$\tau(C) = C, \qquad \forall \tau \in H.$$

Remark 5.3. We note that τ is an injective map from C to $\tau(C)$, which means that $|C| = |\tau(C)|$ for all $\tau \in S_n$. So, we can modify the definition of τ-invariance of a code C by requiring that $\tau(\overline{c}) \in C$ for all $\overline{c} \in C$.

We start with a lemma that will be useful for the rest of the chapter:

Lemma 5.4. *Suppose that C is a k-dimensional linear binary code and suppose the generators are $\overline{c}_1, \overline{c}_2, \ldots, \overline{c}_k$ and let $\tau \in S_n$ be a permutation. Then we have:*

(i) $\tau(\overline{x} + \overline{y}) = \tau(\overline{x}) + \tau(\overline{y})$ *for all* $\overline{x}, \overline{y} \in C$.

(ii) $\tau(\overline{x} * \overline{y}) = \tau(\overline{x}) * \tau(\overline{y})$ *for all* $\overline{x}, \overline{y} \in C$ *where* $*$ *is the component-wise product.*

(iii) $\tau(C)$ *is a k-dimensional binary linear code with generators* $\tau(\overline{c}_1), \tau(\overline{c}_2), \ldots, \tau(\overline{c}_k)$.

(iv) $\tau(C^{\perp}) = \tau(C)^{\perp}$ *if* $\tau^2 = 1$.

Proof. Let $\overline{x} = (x_1, x_2, \ldots, x_n)$ and $\overline{y} = (y_1, y_2, \ldots, y_n)$ be two codewords in C. We then

see that

$$\begin{aligned}\tau(\overline{x}+\overline{y}) &= \tau(x_1+y_1, x_2+y_2, \ldots, x_n+y_n)\\ &= (x_{\tau(1)}+y_{\tau(1)}, x_{\tau(2)}+y_{\tau(2)}, \ldots, x_{\tau(n)}+y_{\tau(n)})\\ &= (x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}) + (y_{\tau(1)}, y_{\tau(2)}, \ldots, y_{\tau(n)})\\ &= \tau(\overline{x})+\tau(\overline{y}).\end{aligned}$$

The case when the operation is $*$ is exactly the same, which means that **(i)** and **(ii)** are proved.

To prove **(iii)**, note that by **(i)** and by the remark above, it suffices to show that $\tau(\overline{c}_1), \tau(\overline{c}_2), \ldots, \tau(\overline{c}_k)$ are linearly independent. Suppose that

$$\alpha_1\tau(\overline{c}_1) + \alpha_2\tau(\overline{c}_2) + \cdots + \alpha_k\tau(\overline{c}_k) = 0$$

with $\alpha_i \in \{0,1\}$ and not all α_i being 0. Since $\alpha_i = 0$ or 1, by **(i)** we see that the above equation is equivalent to

$$\tau(\alpha_1\overline{c}_1 + \alpha_2\overline{c}_2 + \cdots + \alpha_k\overline{c}_k) = \overline{0},$$

which is equivalent to saying that

$$\alpha_1\overline{c}_1 + \alpha_2\overline{c}_2 + \cdots + \alpha_k\overline{c}_k = \overline{0}$$

since τ is injective, which implies that $\alpha_i = 0$ for all $i = 1, 2, \ldots, k$ as $\overline{c}_1, \overline{c}_2, \ldots, \overline{c}_k$ form a set of generators for C and hence are linearly independent.

To prove **(iv)**, we first note that, since τ is injective, we have

$$|\tau(C^{\perp})| = |C^{\perp}| = 2^{n-k}. \tag{5.2}$$

However, since by **(iii)**, $\tau(C)$ is a k-dimensional binary linear code, we have

$$|\tau(C)^{\perp}| = 2^{n-k}. \tag{5.3}$$

Combining (5.2) and (5.3), we see that

$$|\tau(C)^{\perp}| = |\tau(C^{\perp})|. \tag{5.4}$$

So, in order to complete the proof, we only need to prove a one-sided inclusion. To this extent, suppose that $\overline{y} = (y_1, y_2, \ldots, y_n) \in \tau(C)^{\perp}$. Then we have

$$y_1 x_{\tau(1)} + y_2 x_{\tau(2)} + \cdots + y_n x_{\tau(n)} = 0$$

for all $(x_1, x_2, \ldots, x_n) \in C$. Now, since $\tau^2 = 1$, we know that $\tau(j) = i \Leftrightarrow \tau(i) = j$. Hence the above equation can be written in the form

$$x_1 y_{\tau(1)} + x_2 y_{\tau(2)} + \cdots + x_n y_{\tau(n)} = 0$$

for all $(x_1, x_2, \ldots, x_n) \in C$, which means that $\tau(\overline{y}) \in C^{\perp}$ or that $\overline{y} \in \tau(C^{\perp})$ since $\tau^2 = 1$, which proves that

$$\tau(C)^{\perp} \subseteq \tau(C^{\perp}).$$

□

5.2 Permutation Invariance and Linearity over Rings

We will first start with the ring $\mathbb{F}_2 + u\mathbb{F}_2$ that was studied in [13] and the permutation that we will discuss is the *swap map*.

The swap map and the ring $\mathbb{F}_2 + u\mathbb{F}_2$

We recall that the ring $\mathbb{F}_2 + u\mathbb{F}_2$ is constructed by letting $u^2 = 0$. We recall also that a

Gray map $\phi : (\mathbb{F}_2 + u\mathbb{F}_2)^n \to \mathbb{F}_2^{2n}$ is defined as

$$\phi(\overline{x} + u\overline{y}) = (\overline{x} + \overline{y}, \overline{y}), \qquad \overline{x}, \overline{y} \in F_2^n. \tag{5.5}$$

Definition 5.5. Suppose that C is a binary code of length $2n$ for some $n \in \mathbb{N}$. The *swap map* σ on C is defined to be the permutation

$$\sigma = (1, n+1)(2, n+2)\cdots(n, 2n). \tag{5.6}$$

So, if $\overline{c} = (\overline{x}, \overline{y})$ with $\overline{x}, \overline{y} \in \mathbb{F}_2^n$, then

$$\sigma(\overline{c}) = (\overline{y}, \overline{x}). \tag{5.7}$$

Remark 5.6. Note that $\sigma^2 = 1$ and hence if we let the permutation group H be $H = \{1, \sigma\}$, then we see that $H \simeq \mathbb{Z}_2$. In fact, for notational purposes that will be apparent in the latter part of the chapter, we will view the swap map as the permutation group $\mathbb{Z}_2$.

The connection between σ-invariance and linearity over $\mathbb{F}_2 + u\mathbb{F}_2$ was given in [13], but we still want to state the theorem and prove it here, as it will be a reference for the extensions that we will study.

Theorem 5.7. *A binary linear code C of even length is the Gray image of a linear code over $\mathbb{F}_2 + u\mathbb{F}_2$ if and only if C is invariant under the swap map.*

Proof. Suppose that $C = \phi(D)$ where D is a linear $\mathbb{F} + u\mathbb{F}_2$-code of length n, here $2n$ is the length of C. Suppose $\overline{c} = (\overline{x}, \overline{y}) = \phi(\overline{d})$ where $\overline{d} \in D$ and $\overline{x}$ and $\overline{y}$ are in $\mathbb{F}_2^n$. Note that, by the construction of the Gray map, we must have

$$\overline{d} = (\overline{x} + \overline{y}) + u\overline{y}. \tag{5.8}$$

Now, since D is a linear code over $\mathbb{F}_2 + u\mathbb{F}_2$, we see that $(1+u)\overline{d} = (\overline{x} + \overline{y}) + u\overline{x} \in D$ as well. Since $C = \phi(D)$, we see that $\phi\big((1+u)\overline{d}\big) \in C$ as well. But

$$\phi\big((1+u)\overline{d}\big) = \phi(\overline{x} + \overline{y} + u\overline{x}) = (\overline{y}, \overline{x}) = \sigma(\overline{c}). \tag{5.9}$$

This proves the necessary condition.

To prove sufficiency, suppose that C is invariant under the swap map. Then if we look at the inverse image of C under ϕ, we get an $\mathbb{F}_2$-additive code over $\mathbb{F}_2 + u\mathbb{F}_2$. To show that the pre-image is a $\mathbb{F}_2[u]$-module, we notice that the pre-image of the swap of a codeword is $(1+u)$ times the original codeword by the discussion in the first part of the proof. This means that the pre-image is invariant under multiplication by $(1+u)$ and hence by u, so it is $\mathbb{F}_2 + u\mathbb{F}_2$-linear. □

Since $\sigma^2 = 1$, we can use Lemma 5.4-(iv) to prove the following theorem:

Theorem 5.8. *Suppose that C is a binary linear code of length $2n$ for some n and let $C^\perp$ be its dual. If C is $\mathbb{F}_2 + u\mathbb{F}_2$-linear or equivalently if C is invariant under σ, the swap map, then so is $C^\perp$*

Because of Theorem 5.7, we will have the following corollary to Theorem 5.8, which in fact is a stronger way of stating the same theorem:

Corollary 5.9. *Suppose C is a binary linear code of length $2n$ and suppose that*

$$C = \phi(D)$$

for some $\mathbb{F}_2 + u\mathbb{F}_2$-linear code D of length n. Then

$$C^\perp = \phi(D^\perp).$$

Proof. Suppose that a binary linear code C of length $2n$ is the image under the Gray map of a linear code D over $\mathbb{F}_2 + u\mathbb{F}_2$ of length n. Now, suppose that $\overline{x} + u\overline{y} \in D^\perp$, which means that

$$(\overline{x} + u\overline{y}) \cdot (\overline{d}_1 + u\overline{d}_2) = 0$$

for all $\overline{d}_1 + u\overline{d}_2 \in D$, which is equivalent to saying that

$$\overline{x} \cdot \overline{d}_1 = 0, \quad \overline{x} \cdot \overline{d}_2 + \overline{y} \cdot \overline{d}_1 = 0 \tag{5.10}$$

for all $\overline{d}_1 + u\overline{d}_2 \in D$. However, then we see that

$$\begin{aligned}\phi(\overline{x} + u\overline{y}) \cdot \phi(\overline{d}_1 + u\overline{d}_2) &= (\overline{x} + \overline{y}, \overline{y}) \cdot (\overline{d}_1 + \overline{d}_2, \overline{d}_2) \\ &= \overline{y} \cdot \overline{d}_2 + \overline{x} \cdot \overline{d}_1 + \overline{x} \cdot \overline{d}_2 + \overline{y} \cdot \overline{d}_1 + \overline{y} \cdot \overline{d}_2 \\ &= \overline{x} \cdot \overline{d}_1 + \overline{x} \cdot \overline{d}_2 + \overline{y} \cdot \overline{d}_1 \\ &= 0\end{aligned}$$

by (5.10). This means that

$$\phi(D^{\perp}) \subseteq C^{\perp}. \tag{5.11}$$

Now, since ϕ is injective, we see that $|C| = |\phi(D)| = |D|$. And since $|C| \cdot |C^{\perp}| = |D| \cdot |D^{\perp}| = 4^n$, we see that $|C^{\perp}| = |D^{\perp}|$. Again, using the injective property of ϕ we conclude that

$$|\phi(D^{\perp})| = |C^{\perp}|. \tag{5.12}$$

The result of the corollary now follows from (5.11) and (5.12). □

The ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ and the permutation group $\mathbb{Z}_4$

The first natural extension to the swap map, that is, the permutation group $\mathbb{Z}_2$, will be the permutation group $\mathbb{Z}_4$, which we can denote as

$$\mathbb{Z}_4 = \{1, \rho, \rho^2, \rho^3\}$$

where ρ acts on a binary word of length $4n$ as the permutation

$$\rho = (1, n+1, 2n+1, 3n+1)(2, n+2, 2n+2, 3n+2) \cdots (n, 2n, 3n, 4n). \tag{5.13}$$

So, if

$$\overline{x} = (\overline{x}_1, \overline{x}_2, \overline{x}_3, \overline{x}_4)$$

is a binary codeword of length $4n$ for a positive integer n, then we can simply write

$$\rho(\overline{x}) = (\overline{x}_4, \overline{x}_1, \overline{x}_2, \overline{x}_3). \tag{5.14}$$

Definition 5.10. Suppose that C is a binary code of length $4n$ for some integer n. Then we say C is ρ-invariant or, equivalently, that it is invariant under the permutation group $\mathbb{Z}_4$ if we have

$$\rho(C) = C.$$

Remark 5.11. If $\rho(C) = C$, then $\rho^2(C) = \rho^3(C) = C$ so indeed $\mathbb{Z}_4$-invariance and ρ-invariance are equivalent.

The ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ is constructed in the usual way subject to the condition $u^4 = 0$ and the ring has characteristic 2. A *linear code* over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2+u^3\mathbb{F}_2$ of length n is defined as usual to be an $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$-submodule of $(\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2)^n$. As in the case of $\mathbb{F}_2 + u\mathbb{F}_2$-linear codes we can define a Gray map that is a linear map, denoted by ψ. So it is defined as

$$\psi : (\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2)^n \to \mathbb{F}_2^{4n}$$

in such a way that

$$\psi(\overline{a} + u\overline{b} + u^2\overline{c} + u^3\overline{d}) = (\overline{a} + \overline{b} + \overline{c} + \overline{d}, \overline{b} + \overline{d}, \overline{c} + \overline{d}, \overline{d}) \tag{5.15}$$

with $\overline{a}, \overline{b}, \overline{c}, \overline{d} \in \mathbb{F}_2^n$. Note that, ψ is an $\mathbb{F}_2$-linear map, and so it maps linear codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ of length n to binary linear codes of length $4n$. We are now ready to state the theorem that is analogous to Theorem 5.7.

Theorem 5.12. *Suppose C is a binary linear code of length $4n$. Then C is the Gray (ψ) image of a linear code over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2+u^3\mathbb{F}_2$ of length n if and only if C is $\mathbb{Z}_4$-invariant.*

Proof. The proof is exactly the same as the proof of Theorem 5.7, so most of it will be omitted. We will only note that any given binary codeword

$$\overline{x} = (\overline{a}, \overline{b}, \overline{c}, \overline{d})$$

can be considered as the image of a codeword

$$\overline{y} = (\overline{a} + \overline{b} + \overline{c} + \overline{d}) + u(\overline{b} + \overline{d}) + u^2(\overline{c} + \overline{d}) + u^3\overline{d}.$$

We then have

$$\psi((1+u)\overline{y}) = (\overline{d}, \overline{a}, \overline{b}, \overline{c}) = \rho(\overline{x}).$$

$$\psi((1+u^2)\overline{y}) = (\overline{c}, \overline{d}, \overline{a}, \overline{b}) = \rho^2(\overline{x}).$$

$$\psi((1+u+u^2+u^3)\overline{y}) = (\overline{b}, \overline{c}, \overline{d}, \overline{a}) = \rho^3(\overline{x}).$$

□

The ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ and the permutation group K_4

Suppose C is a binary code of length $4n$ for some integer n. Then we introduce the following permutations that are regarded as the elements of the Klein-4 group, $K_4 = \{1, \alpha, \beta, \gamma\}$:

$$\alpha = \big[(1, n+1)(2n+1, 3n+1)\big] \cdot \big[(2, n+2)(2n+2, 3n+2)\big] \cdots \big[(n, 2n)(3n, 4n)\big]$$

$$\beta = \big[(1, 2n+1)(n+1, 3n+1)\big] \cdot \big[(2, 2n+2)(n+2, 3n+2)\big] \cdots \big[(n, 3n)(2n, 4n)\big]$$

$$\gamma = \big[(1, 3n+1)(n+1, 2n+1)\big] \cdot \big[(2, 3n+2)(n+2, 2n+2)\big] \cdots \big[(n, 4n)(2n, 3n)\big].$$

Note that, if we denote a codeword $\overline{x}$ as $(\overline{x}_1, \overline{x}_2, \overline{x}_3, \overline{x}_4)$ where each $\overline{x}_i$ is a binary vector of length n, then we have

$$\begin{aligned} \alpha(\overline{x}_1, \overline{x}_2, \overline{x}_3, \overline{x}_4) &= (\overline{x}_2, \overline{x}_1, \overline{x}_4, \overline{x}_3) \\ \beta(\overline{x}_1, \overline{x}_2, \overline{x}_3, \overline{x}_4) &= (\overline{x}_3, \overline{x}_4, \overline{x}_1, \overline{x}_2) \\ \gamma(\overline{x}_1, \overline{x}_2, \overline{x}_3, \overline{x}_4) &= (\overline{x}_4, \overline{x}_3, \overline{x}_2, \overline{x}_1). \end{aligned} \tag{5.16}$$

Note that β is the same as the usual *swap* map defined in the previous sections.

As usual we define K_4-invariance of a binary code C of length $4n$ as being invariant under the permutations α, β, γ. We will connect the invariance under this permutation with linearity over a certain ring.

Let $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ be the ring of characteristic 2 that is constructed subject to $u^2 = v^2 = 0$ and $uv = vu$. As usual, we consider linear codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ of length n to be $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$-submodules of $(\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2)^n$. Let D be such a linear code. Then we can write any codeword $\overline{d} \in D$ in the form

$$\overline{d} = \overline{x}_1 + u\overline{x}_2 + v\overline{x}_3 + uv\overline{x}_4$$

where $\overline{x}_i \in \mathbb{F}_2^n$.

We define a Gray map $\varphi : (\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2)^n \to \mathbb{F}_2^{4n}$ as

$$\varphi(\overline{x}_1 + u\overline{x}_2 + v\overline{x}_3 + uv\overline{x}_4) = (\overline{x}_1 + \overline{x}_2 + \overline{x}_3 + \overline{x}_4, \overline{x}_3 + \overline{x}_4, \overline{x}_2 + \overline{x}_4, \overline{x}_4). \tag{5.17}$$

Note that φ is a linear map and it maps a linear code over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ of length n to a linear binary code of length $4n$. Moreover, it is obvious that φ is injective. The analogous theorem that connects the K_4-invariance to linearity over these rings can be stated as follows:

Theorem 5.13. *Suppose that C is a binary linear code of length $4n$. Then C is the Gray(φ) image of a linear code over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ of length n if and only if C is K_4-invariant.*

Proof. Suppose that C is the image of a linear code D over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ of length n. So, suppose $\overline{c} = (\overline{x}_1, \overline{x}_2, \overline{x}_3, \overline{x}_4) \in C$ is a codeword. Then it is easy to see that it is the image under the Gray map of the codeword

$$\overline{d} = (\overline{x}_1 + \overline{x}_2 + \overline{x}_3 + \overline{x}_4) + u(\overline{x}_3 + \overline{x}_4) + v(\overline{x}_2 + \overline{x}_4) + uv(\overline{x}_4).$$

But then we have

$$\varphi\big((1+u)\overline{d}\big) = (\overline{x}_3, \overline{x}_4, \overline{x}_1, \overline{x}_2) = \beta(\overline{c}).$$

$$\varphi\big((1+v)\overline{d}\big) = (\overline{x}_2, \overline{x}_1, \overline{x}_4, \overline{x}_3) = \alpha(\overline{c}).$$

$$\varphi\big((1+u+v+uv)\overline{d}\big) = (\overline{x}_4, \overline{x}_3, \overline{x}_2, \overline{x}_1) = \gamma(\overline{c})$$

which proves one side of the implication.

For the other implication, we suppose that we have a binary linear code of length $4n$ that is K_4-invariant. Suppose D is the code over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ of length n that is obtained as the pre-image of C, which is obviously additive. Now, from the above calculations, C being invariant under β means that D is invariant under left multiplication by $1+u$ and hence u. The invariance of C under α implies that D is invariant under left multiplication by $1+v$ and hence v. Finally, the invariance of C under γ implies that D is invariant under the left multiplication by $(1+u+v+uv)$, but since it is already invariant under multiplication by u and v and since it is additive, it implies that it is invariant under multiplication by uv. This proves that D is a $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$-submodule of $(\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2)^n$. □

5.3 Reed-Muller Codes and Permutation Invariance

In this section, we will apply the results of the previous sections to see that Reed-Muller codes, in most cases, are actually linear over the rings $\mathbb{F}_2+u\mathbb{F}_2$, $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2+u^3\mathbb{F}_2$ and $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ unlike the case of $\mathbb{Z}_4$-linearity. To do this, we will first introduce the Reed-Muller codes and see some of their properties. Most of the information can be found in books like [6] and [20].

We first let $v=(v_1,v_2,\ldots,v_m)$ denote a vector that ranges over $\mathbb{F}_2^m$, and we let $\mathbf{f}$ be the vector of length 2^m obtained from a Boolean function $f(v_1,v_2,\ldots,v_m)$, i.e., a polynomial in $v_1,v_2,\ldots,v_m$ where the degree of each v_i is at most 1. A Boolean function of this form will be an $\mathbb{F}_2$-linear combination of terms of the form $v_{i_1}v_{i_2}\ldots v_{i_r}$ with $1\leq i_1<i_2<\cdots<i_r\leq m$. The highest such $r>0$ in f is said to be the *degree* of f. So, if we consider f to be a polynomial in the variables $v_1,v_2,\ldots,v_m$, then the degree is the total degree of f. We then define the Reed-Muller codes as follows:

Definition 5.14. The r^{th} *order binary Reed-Muller* (or RM) code $RM(r,m)$ of length $n=2^m$, for $0\leq r\leq m$, is the set of all vectors $\mathbf{f}$, where $f(v_1,v_2,\ldots,v_m)$ is a Boolean function that is a polynomial of degree at most r.

Remark 5.15. $RM(r,m)$ is a linear binary code of length 2^m and is of dimension $1+\binom{m}{1}+\cdots+\binom{m}{r}$.

Remark 5.16. We can actually specify all the generators of $RM(r,m)$. A set of generators for $RM(r,m)$ would be

$$\{1, v_1, v_2, \ldots, v_m, v_1v_2, \ldots, v_{m-1}v_m, \ldots, v_1v_2\cdots v_r, \ldots, v_{m-r+1}\cdots v_m\}.$$

We can consider these as binary vectors of length 2^m, for example, 1 will correspond to the all 1 vector of length 2^m. v_1 will be the $\{0,1\}$-vector of length 2^m that has 1 that corresponds to the vectors in $\mathbb{Z}_2^m$ that have their first coordinate as 1 and 0 for all the others. Note also that v_iv_j, as a binary vector, is just $v_i * v_j$, the component-wise product of the vectors of v_i and v_j. This means that once we specify $v_1, v_2, \ldots, v_m$, we can find all the generators of $RM(r,m)$ for $0 \leq r \leq m$. It is obvious that we can define the Reed-Muller code $RM(r,m)$ uniquely up to a permutation equivalence by fixing a sort of ordering on the elements of $\mathbb{Z}_2^m$, which we will describe inductively as:

$$\mathbb{Z}_2^m = \mathbb{Z}_2^{m-1}0 \cup \mathbb{Z}_2^{m-1}1, \qquad m \geq 1. \tag{5.18}$$

For the rest of this work, when we talk about the Reed-Muller code $RM(r,m)$, we will consider the binary linear code obtained uniquely from the basic boolean generators $1, v_1, \ldots, v_m$ with the ordering that was fixed for $\mathbb{Z}_2^m$ in (5.18).

In [20], the automorphism group of $RM(r,m)$ is given as the *general Affine group*, denoted by $GA(m)$, which can be defined as the group of all Affine transformations:

$$T\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix} = A\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix} + b$$

where A is an $m \times m$ binary matrix and b is a binary m-tuple. MacWilliams and Sloane showed in [20] that

$$\mathrm{Aut}(RM(r,m)) = GA(m), \qquad 1 \leq r \leq m-2.$$

Of course we know that $RM(0,m)$, $RM(m-1,m)$, and $RM(m,m)$ are invariant under the whole S_{2^m}.

We are now ready to prove the first theorem about permutation invariance of $RM(r,m)$:

Theorem 5.17. *The Reed-Muller code $RM(r,m)$ is invariant under the permutation groups $\mathbb{Z}_2$, $\mathbb{Z}_4$, and K_4 for all $0 \leq r \leq m$.*

Proof. Recall that the permutation group $\mathbb{Z}_2$ means the swap map, $\mathbb{Z}_2 = \{1, \sigma\}$, and $\mathbb{Z}_4 = \{1, \rho, \rho^2, \rho^3\}$ while $K_4 = \{1, \alpha, \beta, \gamma\}$ with their actions defined in (5.7), (5.14), and (5.16), respectively. Let $v_1, v_2, \ldots, v_m$ be the basic boolean generators of $RM(r,m)$. It is enough then by Lemma 5.4 to show that the permutations acting on the Boolean functions of degree $\leq r$ will be in $RM(r,m)$ too.

In order to see this, we will write these generators in terms of the generators of $RM(r,m-2)$ by using the ordering (5.18). Note that we can write

$$\mathbb{Z}_2^m = \mathbb{Z}_2^{m-2}00 \cup \mathbb{Z}_2^{m-2}10 \cup \mathbb{Z}_2^{m-2}01 \cup \mathbb{Z}_2^{m-2}11, \tag{5.19}$$

which means if $w_1, w_2, \ldots, w_{m-2}$ are the basic boolean generators of $RM(r,m-2)$ of length 2^{m-2}, then we have

$$v_i = (w_i, w_i, w_i, w_i), \qquad \forall i = 1, 2, \ldots, m-2. \tag{5.20}$$

And for v_{m-1} and v_m we get

$$v_{m-1} = (0_{2^{m-2}}, 1_{2^{m-2}}, 0_{2^{m-2}}, 1_{2^{m-2}}), \quad v_m = (0_{2^{m-2}}, 0_{2^{m-2}}, 1_{2^{m-2}}, 1_{2^{m-2}}). \tag{5.21}$$

Let's start with σ, which is the swap map. By the above equations we see that

$$\sigma(v_i) = v_i, \qquad i = 1, 2, \ldots, m-2$$

and $\sigma(v_{m-1}) = v_{m-1}$ while $\sigma(v_m) = 1 + v_m$. So, if we apply σ to a Boolean function of $v_1, v_2, \ldots, v_m$ of degree r, then by Lemma 5.4, we will still get a Boolean function of $v_1, \ldots, v_m$ of degree r. This means that $RM(r,m)$ is invariant under $sigma$ or equivalently

under the permutation group $\mathbb{Z}_2$. We could also see this by noticing that σ defines an Affine transformation of $v_1, v_2, \ldots, v_m$ and hence is in the automorphism group of $RM(r,m)$.

To extend this to $\mathbb{Z}_4$, we only need to check the action of ρ. By (5.20) and (5.21), we see that

$$\rho(v_i) = v_i, \quad i = 1, \ldots, m-2, \quad \rho(v_{m-1}) = 1 + v_{m-1}, \quad \rho(v_m) = 1 + v_{m-1} + v_m. \tag{5.22}$$

Now, let's look at the binary vector $v_{i_1} * v_{i_2} * \cdots * v_{i_s}$, which is the vector that corresponds to the Boolean function $v_{i_1} \cdots v_{i_s}$. By Lemma 5.4 and by (5.22), we have

$$\rho(v_{i_1} * v_{i_2} * \cdots * v_{i_s}) = v_{i_1} * v_{i_2} * \cdots * v_{i_s} \in RM(r,m), \qquad i_1, \ldots, i_s \in \{1, 2, \ldots, m-2\}.$$

Since $\mathbb{F}_2$ is a field, multiplication is distributive over addition, which means that $\overline{x} * (\overline{y} + \overline{z}) = \overline{x} * \overline{y} + \overline{x} * \overline{z}$ for binary vectors $\overline{x}, \overline{y}, \overline{z}$. Note also that $\overline{x} * \overline{x} = \overline{x}$ for all binary vectors $\overline{x}$. But this means that

$$\sigma(v_{m-1} * v_{i_1} * \cdots * v_{i_s}) = v_{i_1} * v_{i_2} * \cdots * v_{i_s} + v_{m-1} * v_{i_1} * v_{i_2} * \cdots * v_{i_s}$$

and

$$\sigma(v_m * v_{i_1} * v_{i_2} * \cdots * v_{i_s}) = v_{i_1} * v_{i_2} * \cdots * v_{i_s} + v_{m-1} * v_{i_1} * v_{i_2} * \cdots * v_{i_s} + v_m * v_{i_1} * v_{i_2} * \cdots * v_{i_s}$$

for all $i_1 < i_2 < \cdots < i_s \in \{1, 2, \ldots, m-2\}$.

The only remaining case is to look at a vector of the form $v_{m-1} * v_m * v_{i_1} * \cdots * v_{i_s}$, but then by the above discussion we see that

$$\begin{aligned}\sigma(v_{m-1} * v_m * v_{i_1} * \cdots * v_{i_s}) = {} & v_{i_1} * \cdots * v_{i_s} + v_{m-1} * v_{i_1} * \cdots * v_{i_s} + v_m * v_{i_1} * \cdots * v_{i_s} \\ & + v_{m-1} * v_m * v_{i_1} * \cdots * v_{i_s},\end{aligned}$$

which is still in $RM(r,m)$. Since ρ takes all generators of $RM(r,m)$ to vectors in $RM(r,m)$, by Lemma 5.4 we can conclude that $RM(r,m)$ is invariant under the permutation ρ or

equivalently under the permutation group $\mathbb{Z}_4$.

To see the permutation invariance under K_4, we look at the images of the basic generators under the permutations of K_4:

$$\alpha(v_i) = v_i, \quad i = 1, \ldots, m-2, \quad \alpha(v_{m-1}) = 1 + v_{m-1}, \quad \alpha(v_m) = v_m$$

$$\beta(v_i) = v_i, \quad i = 1, \ldots, m-2, \quad \beta(v_{m-1}) = v_{m-1}, \quad \beta(v_m) = 1 + v_m$$

$$\gamma(v_i) = v_i, \quad i = 1, \ldots, m-2, \quad \gamma(v_{m-1}) = 1 + v_{m-1}, \quad \gamma(v_m) = 1 + v_m.$$

By the same reasoning as above in the case of $\mathbb{Z}_4$, we can easily see that all the generators of $RM(r, m)$ with $0 \leq r \leq m$ are mapped to vectors in $RM(r, m)$, which proves that $RM(r, m)$ is invariant under the action of the permutation group K_4 by Lemma 5.4.

Note that for $r = 0$, we have $RM(0, m) = \{\overline{0}, \overline{1}\}$ which is invariant under all permutations in S_{2^m}. So, the proof of the theorem is concluded. □

An immediate corollary of Theorem 5.17 comes from the results of the previous section, which were summarized in the form of Theorems 5.7, 5.12 and 5.13:

Corollary 5.18. *The Reed-Muller code $RM(r, m)$ is the Gray image of linear codes over the rings $\mathbb{F}_2 + u\mathbb{F}_2$, $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ and $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ for $0 \leq r \leq m$, for the appropriate Gray map defined for each ring as was done in Section 5.2.*

As we see, this turns out to be another big difference between $\mathbb{Z}_4$ and $\mathbb{F}_2 + u\mathbb{F}_2$, as another corollary could be stated as follows that is in contrast to Theorem 8 in [2] for the case of $\mathbb{Z}_4$.

Corollary 5.19. *The binary code $RM(m-2, m)$, i.e., the extended Hamming code of length $n = 2^m$, is $\mathbb{F}_2 + u\mathbb{F}_2$-linear.*

5.4 The Pre-images of Reed-Muller Codes under Gray Maps

Theorem 5.17 and Corollary 5.18 in the previous section tell us that the Reed-Muller codes $RM(r, m)$ can be obtained as the Gray image of linear codes over the rings $\mathbb{F}_2 + u\mathbb{F}_2$,

$\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ and $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ for all $0 \leq r \leq m$. We are curious to find these linear codes that give us the Reed-Muller codes in this section. Before starting to find the exact pre-images, we need to introduce a theorem about Reed-Muller codes that proves to be very useful in finding these pre-images:

Theorem 5.20. (Theorem 2, [20]) *For $0 \leq r \leq m$, we have the following identity for Reed-Muller codes:*

$$RM(r+1, m+1) = \{\ (\overline{c}, \overline{c}+\overline{d}) \mid \overline{c} \in RM(r+1, m), \overline{d} \in RM(r, m)\ \}.$$

We start by finding the pre-image of $RM(r, m)$ as a linear code over $\mathbb{F}_2 + u\mathbb{F}_2$.

Definition 5.21. Define by $FRM(r, m-1)$, for $r = 0, 1, 2, \ldots, m$, the linear code over $\mathbb{F}_2 + u\mathbb{F}_2$ that is generated by $RM(r-1, m-1)$ and $uRM(r, m-1)$.

Remark 5.22. We are making the conventions that $RM(-1, m-1) = RM(m, m-1) = 0$.

At this point we want to introduce the following useful lemma:

Lemma 5.23. *For $1 \leq r \leq m-1$, we have*

$$FRM(r, m-1) = \{\alpha\overline{c} + \beta u\overline{d} \mid \overline{c} \in RM(r-1, m-1), \overline{d} \in RM(r, m-1); \alpha, \beta \in \mathbb{Z}_2\}.$$

Proof. We know that

$$\begin{aligned} FRM(r, m-1) &= \{(\alpha+\gamma u)\overline{c} + \lambda u\overline{d} \big| \overline{c} \in RM(r-1, m-1), \overline{d} \in RM(r, m-1); \alpha, \gamma, \lambda \in \mathbb{Z}_2\} \\ &= \{\alpha\overline{c} + (\gamma+\lambda)u(\overline{c}+\overline{d}) \big| \overline{c} \in RM(r-1, m-1), \overline{d} \in RM(r, m-1); \alpha, \gamma, \lambda \in \mathbb{Z}_2\}. \end{aligned}$$

Now, as λ, γ run through the elements of $\mathbb{Z}_2$, so does $\beta = \lambda + \gamma$. Also, since $RM(r-1, m-1) \subset RM(r, m-1)$, we see that $\overline{c} + \overline{d}$ runs through the codewords of $RM(r, m-1)$ as $\overline{c}$ and $\overline{d}$ run through codewords of $RM(r-1, m-1)$ and $RM(r, m-1)$, respectively. Putting these into the above, we see that

$$FRM(r, m-1) = \{\alpha\overline{c} + \beta u\overline{d} \big| \overline{c} \in RM(r-1, m-1), \overline{d} \in RM(r, m-1); \alpha, \beta \in \mathbb{Z}_2\}$$

as expected. □

Remark 5.24. $FRM(r, m-1)$ is generated by

$$1, v_1, v_2, \ldots, v_{m-1}, \ldots, v_1 v_2 \ldots v_{r-1}, \ldots, v_{m-r+1} \ldots v_{m-1}, uv_1 v_2 \ldots v_r, \ldots, uv_{m-r} \ldots v_{m-1}.$$

So, as a code over $\mathbb{F}_2 + u\mathbb{F}_2$, it is of type

$$(4)^{1+(m-1)+\cdots+\binom{m-1}{r-1}}(2)^{\binom{m-1}{r}}.$$

We can observe the following lemma about the sizes of the codes $FRM(r, m-1)$ and $RM(r, m)$:

Lemma 5.25.

$$|FRM(r, m-1)| = |RM(r, m)|.$$

Proof. From Remark 5.24, we see that

$$|FRM(r, m-1)| = 2^q$$

where

$$q = 2\big[1 + (m-1) + \cdots + \binom{m-1}{r-1}\big] + \binom{m-1}{r}.$$

Now we will use the classical identity

$$\binom{m}{r} = \binom{m-1}{r} + \binom{m-1}{r-1}.$$

So we get

$$q = 2\big[1 + (m-1) + \cdots + \binom{m-1}{r-2}\big] + \binom{m-1}{r-1} + \binom{m}{r}.$$

Applying the same identity for $r-1$, we get

$$q = 2\big[1 + (m-1) + \cdots + \binom{m-1}{r-3}\big] + \binom{m-1}{r-2} + \binom{m}{r-1} + \binom{m}{r}.$$

Continuing in this manner, we see that inductively, we will get

$$q = 1 + m + \binom{m}{2} + \cdots + \binom{m}{r},$$

which is the dimension of $RM(r, m)$, proving the assertion. □

We observe, from Lemma 5.23 that since $\alpha\overline{c} \in RM(r-1, m-1)$ for all $\alpha \in \mathbb{Z}_2$, $\overline{c} \in RM(r-1, m-1)$ and also $\beta\overline{d} \in RM(r, m-1)$, for all $\beta \in \mathbb{Z}_2$, $\overline{d} \in RM(r, m-1)$, we have

$$FRM(r, m-1) = \{\overline{c} + u\overline{d} \mid \overline{c} \in RM(r-1, m-1), \overline{d} \in RM(r, m-1)\} \tag{5.23}$$

for all $1 \leq r \leq m-1$.

Theorem 5.26. *The image of $FRM(r, m-1)$ under the Gray map $\phi : (\mathbb{F}_2 + u\mathbb{F}_2)^n \to \mathbb{F}_2^{2n}$ is the Reed-Muller code $RM(r, m)$.*

Proof. We know by Lemma 5.23 and (5.23) that

$$FRM(r, m-1) = \{\overline{c} + u\overline{d} \mid \overline{c} \in RM(r-1, m-1), \overline{d} \in RM(r, m-1)\}.$$

Since $RM(r-1, m-1) \subset RM(r, m-1)$, we see that $\overline{c} + \overline{d}$ runs through the elements of $RM(r, m-1)$ as $\overline{c}$ runs through $RM(r-1, m-1)$ and $\overline{d}$ runs through $RM(r, m-1)$. So, if we call $\overline{a} = \overline{c} + \overline{d}$, then we get

$$\begin{aligned}
\phi\big(FRM(r, m-1)\big) &= \{(\overline{c} + \overline{d}, \overline{d}) \mid \overline{c} \in RM(r-1, m-1), \overline{d} \in RM(r, m-1)\} \\
&= \{(\overline{a}, \overline{a} + \overline{c}) \mid \overline{c} \in RM(r-1, m-1), \overline{a} \in RM(r, m-1)\} \\
&= RM(r, m)
\end{aligned}$$

by Theorem 5.20. □

Remark 5.27. When $r = 0$, $FRM(0, m-1)$ is generated by $u1_{2^{m-1}}$ whose image under the Gray map is $\{0_{2^m}, 1_{2^m}\} = RM(0, m)$.

When $r = m$, $FRM(m, m-1) = (\mathbb{F}_2 + u\mathbb{F}_2)^{2^{m-1}}$. The Gray map of this obviously is

$$\left\{(\overline{c} + \overline{d}, \overline{d}) \mid \overline{c}, \overline{d} \in \mathbb{F}_2^{2^{m-1}}\right\} = \mathbb{F}_2^{2^m} = RM(m, m).$$

This means that the result in Theorem 5.26 is true for all $0 \leq r \leq m$.

In exactly the same way as we did above, we can find the pre-images of the Reed-Muller code as linear codes over the rings $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ and $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. We will summarize them in the following theorems, but omit the proofs as they are very similar to the proof of Theorem 5.26.

Theorem 5.28. *Suppose that $SRM(r, m)$ is the linear code over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ of length 2^{m-2} generated by*

$$RM(r-2, m-2), uRM(r-1, m-2), u^2RM(r-1, m-2), u^3RM(r, m-2).$$

If $\psi : (\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2)^n \to \mathbb{F}_2^{4n}$ is the Gray map as defined in Section 5.2, then we have

$$\psi\big(SRM(r, m)\big) = RM(r, m).$$

Theorem 5.29. *Suppose that $DRM(r, m)$ is the linear code over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ of length 2^{m-2} generated by the codes*

$$RM(r-2, m-2), uRM(r-1, m-2), vRM(r-1, m-2), uvRM(r, m-2).$$

If $\phi : (\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2)^n \to \mathbb{F}_2^{4n}$ is the Gray map defined in Section 5.2, then

$$\phi\big(DRM(r, m)\big) = RM(r, m).$$

5.5 Reed-Muller Codes and the Permutation Group $\mathbb{Z}_{2^k}$

In sections 5.3 and 5.4, we proved that the Reed-Muller codes $RM(r, m)$ are invariant under the permutation groups of $\mathbb{Z}_2$, $\mathbb{Z}_4$, and K_4 by proving it directly as well as by proving that

they are the images under the Gray maps of certain linear codes over the rings $\mathbb{F}_2 + u\mathbb{F}_2$, $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ and $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, respectively. In fact, we were able to find the exact pre-images of Reed-Muller codes in these rings. Since the Reed-Muller codes are of length 2^m, it is natural to ask the question about the invariance of Reed-Muller codes under the permutation group $\mathbb{Z}_{2^k}$, of course with $k \leq m$. The work in the two previous sections tells us that $RM(r, m)$ is invariant under the permutation group $\mathbb{Z}_{2^k}$ for $k = 1$ and $k = 2$ for all $0 \leq r \leq m$.

Let us remember that the permutation group $\mathbb{Z}_{2^k}$ is generated by τ, where

$$\tau(\overline{x}) = (\overline{x}_{2^k}, \overline{x}_1, \overline{x}_2, \ldots, \overline{x}_{2^k-1}). \tag{5.24}$$

Here, $\overline{x} = (\overline{x}_1, \ldots, \overline{x}_{2^k})$ with $\overline{x}_i$ being binary vectors of length n.

We first start with a special case that rules out the possibility for the Reed-Muller codes to be invariant under $\mathbb{Z}_{2^k}$ for all k.

Lemma 5.30. *$RM(1, m)$ is not $\mathbb{Z}_{2^m}$-invariant when $m \geq 3$.*

Proof. We will use the construction that we have of Z_2^m as

$$\mathbb{Z}_2^{m-1}0 \cup \mathbb{Z}_2^{m-1}1,$$

which means that if $1, w_1, w_2, \ldots, w_{m-1}$ denote the basic generators of $RM(1, m-1)$, then we have

$$v_i = (w_i, w_i), \qquad i = 1, 2, \ldots, m-1$$

and

$$v_m = (0_{2^{m-1}}, 1_{2^{m-1}}).$$

Now, if we apply the permutation $\tau = (1, 2, \ldots, 2^m)$ to v_m, we get

$$\tau(v_m) = (1, 0_{2^{m-1}-1}, 0, 1_{2^{m-1}-1}).$$

Now, suppose $\tau(v_m) \in RM(1, m)$. Then this would be true if we were to restrict ourselves

to the left-half of the codes. But each codeword in the left-hand half of $RM(1,m)$ with $m \geq 3$ has even weight while the left hand half of $\tau(v_m)$ has weight 1, which gives us the contradiction we need. □

In order to get a result about $\mathbb{Z}_{2^k}$-invariance of $RM(r,m)$, we will need to impose some restrictions on k, r, and m. To do this we will first start with the basic generators of $RM(r,m)$ and we will use similar techniques to the ones we used in the previous section. Suppose $v_1, v_2, \ldots, v_m$ are the basic Boolean generators of $RM(r,m)$. We will have to prove that τ applied to each generator of $RM(r,m)$ will still be in $RM(r,m)$. Now, suppose $k \leq m$. We will construct $\mathbb{Z}_2^m$ inductively as

$$\mathbb{Z}_2^{m-k}000\ldots0 \cup \cdots \cup \mathbb{Z}_2^{m-k}1111\ldots1,$$

which means we will have the following forms for v_i in terms of the basic Boolean functions $w_1, w_2, \ldots, w_{m-k}$ of $\mathbb{Z}_2^{m-k}$:

$$v_i = (w_i, w_i, \ldots, w_i), \qquad i = 1, 2, \ldots, m-k$$

$$v_{m-k+1} = (\overline{0}, \overline{1}, \ldots, \overline{0}, \overline{1})$$

$$v_{m-k+2} = (\overline{0}, \overline{0}, \overline{1}, \overline{1}, \ldots, \overline{0}, \overline{0}, \overline{1}, \overline{1})$$

$$v_{m-k+3} = (\overline{0}, \overline{0}, \overline{0}, \overline{0}, \overline{1}, \overline{1}, \overline{1}, \overline{1}, \ldots, \overline{0}, \overline{0}, \overline{0}, \overline{0}, \overline{1}, \overline{1}, \overline{1}, \overline{1})$$

....

....

$$v_m = (\overline{0}, \overline{0}, \ldots, \overline{0}, \overline{1}, \overline{1}, \ldots \overline{1})$$

where each $\overline{0}$ and $\overline{1}$ is a vector of length 2^{m-k} that consists of 0's and 1's, respectively. So, then we have

$$\tau(v_i) = v_i$$

for all $i = 1, 2, \ldots, m-k$.

Now we need to see what happens when $i > m-k$. It is easy to see that

$$\tau(v_{m-k+1}) = (\overline{1}, \overline{0}, \ldots, \overline{1}, \overline{0}) = 1 + v_{m-k+1}, \tag{5.25}$$

and

$$\tau(v_{m-k+2}) = (\overline{1}, \overline{0}, \overline{0}, \overline{1}, \overline{1}, \ldots, \overline{0}, \overline{0}, \overline{1}) = v_{m-k+2} + \tau(v_{m-k+1}) = 1 + v_{m-k+1} + v_{m-k+2}. \tag{5.26}$$

Now let's look at v_{m-k+3}. It is easy to see that

$$\begin{aligned}
\tau(v_{m-k+3}) + v_{m-k+3} &= (\overline{1}, \overline{0}, \overline{0}, \overline{0}, \overline{1}, \overline{0}, \overline{0}, \overline{0}, \overline{1} \ldots, \overline{0}, \overline{0}, \overline{0}) \\
&= \tau(v_{m-k+1} * v_{m-k+2}) \\
&= \tau(v_{m-k+1}) * \tau(v_{m-k+2}) \\
&= (1 + v_{m-k+1}) * (1 + v_{m-k+1} + v_{m-k+2}) \\
&= 1 + v_{m-k+1} + v_{m-k+2} + v_{m-k+1} v_{m-k+2}.
\end{aligned}$$

This means that

$$\tau(m-k+3) = 1 + v_{m-k+1} + v_{m-k+2} + v_{m-k+1} v_{m-k+2} + v_{m-k+3}. \tag{5.27}$$

To see the general picture we look at $\tau(v_{m-k+i})$ inductively, and we see that for $i \geq 3$, we have

$$v_{m-k+i} + \tau(v_{m-k+i}) = ((\overline{1}, \overline{0}, \overline{0}, \ldots \overline{0}), (\overline{1}, \overline{0}, \overline{0}, \ldots, \overline{0}), \ldots, (\overline{1}, \overline{0}, \overline{0}, \ldots, \overline{0})) \tag{5.28}$$

where each $(\overline{1}, \overline{0}, \overline{0}, \ldots, \overline{0})$ is of length 2^i and hence can easily be seen to be

$$\tau(v_{m-k+1} * v_{m-k+2} * \cdots * v_{m-k+i-1}).$$

So we see that

$$\tau(v_{m-k+i}) = v_{m-k+i} + \tau(v_{m-k+1} * v_{m-k+2} * \cdots * v_{m-k+i-1}), \qquad i \geq 3. \tag{5.29}$$

However, by induction on i, we can conclude the following lemma:

Lemma 5.31. *$\tau(v_{m-k+i})$ is a Boolean function of $v_{m-k+1}, \ldots, v_{m-k+i}$ of degree $i-1$.*

This of course puts a restriction on k in terms of r because the codewords in $RM(r,m)$ are Boolean functions of $1, v_1, \ldots, v_m$ of degree at most r, and Lemma 5.31 tells us that $\tau(v_m)$ is a Boolean function of $v_{m-k+1}, \ldots, v_m$ of degree $k-1$. As an example if we look at $RM(2,4)$, with $1, v_1, v_2, v_3, v_4$ its basic Boolean generators, and if τ is the generator permutation of the permutation group $\mathbb{Z}_8$, we see that $\tau(v_1 v_4)$ is not in $RM(2,4)$. In fact, we have the following theorem that will basically tell us that invariance under $\mathbb{Z}_2$ and $\mathbb{Z}_4$ is, in a sense, the best we can expect.

Theorem 5.32. *Suppose $3 \leq k \leq m$ is an integer. Then $RM(r,m)$ is invariant under the permutation group $\mathbb{Z}_{2^k}$ if and only if $r = 0, r = m$, or $r = m-1$.*

Proof. Recall that $RM(0,m) = \{\overline{0}_{2^m}, \overline{1}_{2^m}\}$ and $RM(m,m) = \mathbb{F}_2^{2^m}$ which are both invariant under any permutation. Note also that from [20], we know that $RM(m-1,m)$ consists of all binary vectors of length 2^m that have even weight, and since weights are preserved under any permutation, $RM(m-1,m)$ will also be invariant under any permutation.

Now suppose that $r = 1$ and let τ be the generator of the permutation group $\mathbb{Z}_{2^k}$ and let $v_1, v_2, \ldots, v_m$ be the basic generators of the Reed-Muller code. Then, since by Lemma 5.31, $\tau(v_m)$ is a Boolean function of $v_{m-k+1}, v_{m-k+2}, \ldots, v_m$ of degree $k-1$ and since $k \geq 3$, we see that $\tau(v_m)$ is a Boolean function of degree $k-1 \geq 2$, which means that by the construction of the Reed-Muller codes, $\tau(v_m)$ is not in $RM(1,m)$.

Now let $2 \leq r < m-1$ and let $k < m$. Then, let's look at $v_m v_{i_1} v_{i_2} \cdots v_{i_{r-s-1}} v_1 \cdots v_s \in RM(r,m)$, where $1 \leq s \leq m-k$ and $i_1, i_2, \ldots i_{r-s-1}$ are distinct numbers that are in $\{m-k+1, \ldots, m-1\}$. Then, by (5.29) and by Lemma 5.31, we see that $\tau(v_m v_{i_1} v_{i_2} \cdots v_{i_{r-s-1}} v_1 \cdots v_s)$ is a Boolean function of $v_1, \ldots, v_s, v_{m-k+1}, \ldots, v_m$ of order $k-1+s$. Now, we want to take

the maximum possible s such that $s \leq r-1$ and $s \leq m-k$. We have to look at two cases then.

Suppose that $m-k \geq r-1$. Then, take $s = r-1$, which means that

$$\tau(v_m v_1 \cdots v_{r-1})$$

is a Boolean function of $v_1, \ldots, v_{r-1}, v_{m-k+1}, \ldots, v_m$ of degree $k-1+r-1$, which means that $\tau(v_m v_1 \cdots v_{r-1}) \in RM(r,m)$ if and only if $k-1+r-1 \leq r$, which means $k \leq 2$.

Now, suppose that $m-k \leq r-2$. Then, we will take $s = m-k$, which means that, in this case, we will have

$$\tau(v_m v_{i_1} v_{i_2} \cdots v_{i_{r-s-1}} v_1 \cdots v_s) = \tau(v_m v_{i_1} v_{i_2} \cdots v_{i_{r-m+k-1}} v_1 \cdots v_{m-k})$$

as a Boolean function of $v_1, v_2, \ldots, v_{m-k}, v_{m-k+1}, \ldots, v_m$ of degree $k-1+m-k = m-1 > r$, which means $RM(r,m)$ is not invariant under $\mathbb{Z}_{2^k}$ in this case. □

Remark 5.33. As we see in Theorem 5.32, we know that $RM(r,m)$ is not usually invariant under the permutation group $\mathbb{Z}_{2^k}$ except in special cases like $k = 1, k = 2$ or $r = 0, r = m, m-1$. This means that the discussion about the permutation invariance of Reed-Muller codes under the permutations in Section 5.3 is in a sense complete.

5.6 Linear Codes over $\mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{2^k-1}\mathbb{F}_2$ and $\mathbb{Z}_{2^k}$-invariance

We will finish this chapter by working out analogous results to Theorem 5.7 and Theorem 5.12. In fact we will be generalizing those results. To this extent, we will first define linear codes over the ring $S_k = \mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{2^k-1}\mathbb{F}_2$, which is constructed just like the previous cases of $k = 1$ and $k = 2$, where we have $u^{2^k} = 0$ here. Notice that we have

$$S_k \simeq \mathbb{F}_2[X]/(X^{2^k}). \tag{5.30}$$

Note that S_k is a finite chain ideal ring with all its ideals defined as $\{I_j = u^j S_k | j = 0, 1, 2, \ldots, 2^k\}$ where $u^{2^k} S_{2^k} = 0$, the zero ideal. A linear code C over the ring S_k of length

n is defined in the usual way, that is, C is an S_k-submodule of S_k^n.

Since the ring S_k is a finite chain ideal ring, we can talk about the *type* of the code C. So, every linear code C is permutational equivalent to a code with type

$$(2^{2^k})^{r_1}(2^{2^k-1})^{r_2}\dots(2)^{r_{2^k}}$$

with r_j's being non-negative integers. This means that the generating matrix of C will have the following form:

$$G = \begin{bmatrix} I_{r_1} & A_1 & . & . & . & A_m \\ 0 & uI_{r_2} & uB_1 & . & . & uB_{m-1} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & . & . & 0 & u^{m-1}I_{r_m} & u^{m-1}D \end{bmatrix}$$

where $m = 2^k$ and A_i, B_j and so on and D are matrices over S_k. Note that in this case we have

$$|C| = 2^{r_1 2^k + r_2(2^k-1)+\cdots+r_{2^k}}. \tag{5.31}$$

Next, we will define a Gray map $\phi_k : S_k^n \to \mathbb{F}_2^{2^k n}$.

Definition 5.34. Let

$$\overline{a} = \overline{a}_0 + u\overline{a}_1 + \cdots + u^{2^k-1}\overline{a}_{2^k-1} \in S_k^n$$

be given with $\overline{a}_i \in \mathbb{F}_2^n$ for each $i = 0, 1, \dots, 2^k - 1$. Write $\overline{a}$ in the following way:

$$\begin{aligned} \overline{a} &= \overline{a}_0 + u\overline{a}_1 + \cdots + u^{2^k-1}\overline{a}_{2^k-1} \\ &= (\overline{a}_0 + u^{2^{k-1}}\overline{a}_{2^{k-1}}) + u(\overline{a}_1 + u^{2^{k-1}}\overline{a}_{2^{k-1}+1}) + \cdots + u^{2^{k-1}-1}(\overline{a}_{2^{k-1}-1} + u^{2^{k-1}}\overline{a}_{2^k-1}). \end{aligned}$$

Then we define $\phi_k(\overline{a})$ as follows:

$$\phi_k(\overline{a}) = \big(\phi_{k-1}(A_0(\overline{a})) + \phi_{k-1}(A_1(\overline{a})), \phi_{k-1}(A_1(\overline{a}))\big) \tag{5.32}$$

where

$$A_0(\overline{a}) = \overline{a}_0 + u\overline{a}_1 + \cdots + u^{2^{k-1}-1}\overline{a}_{2^{k-1}-1} \tag{5.33}$$

and

$$A_1(\overline{a}) = \overline{a}_{2^{k-1}} + u\overline{a}_{2^{k-1}+1} + \cdots + u^{2^{k-1}-1}\overline{a}_{2^k-1}. \tag{5.34}$$

Remark 5.35. Note that this definition is indeed an extension of the Gray maps for $S_1 = \mathbb{F}_2 + u\mathbb{F}_2$ and $S_2 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ because $\phi_1 = \phi$ that was defined in (5.5) for S_1 and $\phi_2 = \psi$, which was defined for S_2 in (5.15).

Before stating and proving the main result of this section, which is an analogous result to those obtained in Section 5.2, we need to understand the map ϕ_k better.

We introduce the notation B_i^k by letting

$$\phi_k(\overline{a}_0 + u\overline{a}_1 + \cdots + u^{2^k-1}\overline{a}_{2^k-1}) = \big(B_0^k(\overline{a}_0, \ldots, \overline{a}_{2^k-1}), B_1^k(\overline{a}_0, \ldots, \overline{a}_{2^k-1}), \ldots, B_{2^k-1}^k(\overline{a}_0, \ldots, \overline{a}_{2^k-1})\big) \tag{5.35}$$

where each $B_i^k(\overline{a}_0, \ldots, \overline{a}_{2^k-1})$ is a $\{0,1\}$-linear combination of the vectors $\overline{a}_0, \overline{a}_1, \ldots, \overline{a}_{2^k-1}$ and it is given inductively as

$$B_i^k(\overline{a}_0, \ldots, \overline{a}_{2^k-1}) = B_i^{k-1}(\overline{a}_0, \ldots, \overline{a}_{2^{k-1}-1}) + B_i^{k-1}(\overline{a}_{2^{k-1}}, \ldots, \overline{a}_{2^k-1}) \tag{5.36}$$

for all $i < 2^{k-1}$, and

$$B_i^k(\overline{a}_0, \ldots, \overline{a}_{2^k-1}) = B_{i-2^{k-1}}^{k-1}(\overline{a}_{2^{k-1}}, \ldots, \overline{a}_{2^k-1}) \tag{5.37}$$

for all $i \geq 2^{k-1}$.

Using (5.35)–(5.37) and induction together with Pascal's identity one can prove that exactly $\binom{k}{i}$ of the B_j^k's have 2^{k-i} terms in their linear combinations. Our first observation

will be the following quick lemma:

Lemma 5.36.

$$B_0^k(\overline{a}_0, \ldots, \overline{a}_{2^k-1}) = \overline{a}_0 + \overline{a}_1 + \cdots + \overline{a}_{2^k-1}$$

and

$$B_{2^k-1}^k(\overline{a}_0, \overline{a}_1, \ldots, \overline{a}_{2^k-1}) = \overline{a}_{2^k-1}$$

for all k.

Proof. This follows easily from the fact that these statements are true for $k = 1$ and $k = 2$ and by induction, using the identities (5.35)–(5.37), which basically is the construction of ϕ_k. □

A main tool in understanding ϕ_k will be the following lemma:

Lemma 5.37. *For $\overline{a} \in S_k^n$ and τ the generator of the permutation group $\mathbb{Z}_{2^k}$, which basically is the cyclic shift of the n-vectors, we have the following:*

$$\phi_k\big((1+u)\overline{a}\big) = \tau\big(\phi_k(\overline{a})\big).$$

Proof. We will use induction. This statement is certainly true for $k = 1$ and $k = 2$. Suppose it is true for $k - 1$. We first note that

$$\begin{aligned}(1+u)\overline{a} &= \overline{a}_0 + u(\overline{a}_0 + \overline{a}_1) + \cdots + u^{2^k-2}(\overline{a}_{2^k-3} + \overline{a}_{2^k-2}) + u^{2^k-1}(\overline{a}_{2^k-2} + \overline{a}_{2^k-1}) \\ &= \Big(\overline{a}_0 + u(\overline{a}_0 + \overline{a}_1) + \cdots + u^{2^{k-1}-1}(\overline{a}_{2^{k-1}-2} + \overline{a}_{2^{k-1}-1})\Big) \\ &\quad + u^{2^{k-1}}\Big(\overline{a}_{2^{k-1}-1} + \overline{a}_{2^{k-1}} + u(\overline{a}_{2^{k-1}} + \overline{a}_{2^{k-1}+1}) + \cdots + u^{2^{k-1}-1}(\overline{a}_{2^k-2} + \overline{a}_{2^k-1})\Big).\end{aligned}$$

But this means that

$$A_0\big((1+u)\overline{a}\big) = (1+u)A_0(\overline{a}) \tag{5.38}$$

and

$$A_1\big((1+u)\overline{a}\big) = \overline{a}_{2^{k-1}-1} + (1+u)A_1(\overline{a}). \tag{5.39}$$

Now suppose that

$$\phi_{k-1}(A_0(\overline{a})) = (\overline{x}_0, \overline{x}_1, \ldots, \overline{x}_{2^{k-1}-1})$$

and

$$\phi_{k-1}(A_1(\overline{a})) = (\overline{y}_0, \overline{y}_1, \ldots, \overline{y}_{2^{k-1}-1})$$

so that we would have

$$\phi_k(\overline{a}) = (\overline{x}_0 + \overline{y}_0, \ldots, \overline{x}_{2^{k-1}-1} + \overline{y}_{2^{k-1}-1}, \overline{y}_0, \overline{y}_1, \ldots, \overline{y}_{2^{k-1}-1}). \tag{5.40}$$

By using (5.38) and (5.39), we see that

$$\begin{aligned}\phi_k((1+u)\overline{a}) = \Big(&\phi_{k-1}((1+u)A_0(\overline{a})) + \phi_{k-1}(\overline{a}_{2^{k-1}-1}) + \phi_{k-1}((1+u)A_1(\overline{a})),\\ &\phi_{k-1}(\overline{a}_{2^{k-1}-1}) + \phi_{k-1}((1+u)A_1(\overline{a}))\Big).\end{aligned} \tag{5.41}$$

We now use induction hypothesis to note that

$$\phi_{k-1}((1+u)A_0(\overline{a})) = (\overline{x}_{2^{k-1}-1}, \overline{x}_0, \ldots, \overline{x}_{2^{k-1}-2}) \tag{5.42}$$

and

$$\phi_{k-1}((1+u)A_1(\overline{a})) = (\overline{y}_{2^{k-1}-1}, \overline{y}_0, \ldots, \overline{y}_{2^{k-1}-2}) \tag{5.43}$$

and we also note that

$$\phi_{k-1}(\overline{a}_{2^{k-1}-1}) = (\overline{a}_{2^{k-1}-1}, \overline{0}, \ldots, \overline{0}) = (\overline{x}_{2^{k-1}-1}, \overline{0}, \overline{0}, \ldots, \overline{0}) \tag{5.44}$$

because by Lemma 5.36, $\overline{x}_{2^{k-1}-1} = \overline{a}_{2^{k-1}-1}$. Now, combining (5.40)–(5.44) we get

$$\begin{aligned}\phi_k\big((1+u)\overline{a}\big) &= (\overline{x}_{2^{k-1}-1} + \overline{y}_{2^{k-1}-1} + \overline{x}_{2^{k-1}-1}, \overline{x}_0 + \overline{y}_0, \ldots, \overline{x}_{2^{k-1}-2} + \overline{y}_{2^{k-1}-2},\\ &\quad \overline{x}_{2^{k-1}-1} + \overline{y}_{2^{k-1}-1}, \overline{y}_0, \overline{y}_1, \ldots, \overline{y}_{2^{k-1}-2})\\ &= (\overline{y}_{2^{k-1}-1}, \overline{x}_0 + \overline{y}_0, \ldots, \overline{x}_{2^{k-1}-1} + \overline{y}_{2^{k-1}-1}, \overline{y}_0, \ldots, \overline{y}_{2^{k-1}-2})\\ &= \tau\big(\phi_k(\overline{a})\big).\end{aligned}$$

□

Remark 5.38. An easy induction shows that ϕ_k is an $\mathbb{F}_2$-linear and injective map from S_k^n to $\mathbb{F}_2^{2^k n}$.

We are finally ready to state and prove the analogous result to the ones that we obtained in Section 5.2:

Theorem 5.39. *Suppose that C is a linear binary code of length $2^k n$. Then C is invariant under the permutation group $\mathbb{Z}_{2^k}$ if and only if C is the image under ϕ_k of some linear code over S_k of length n.*

Proof. Suppose that C is a binary linear code of length $2^k n$ and suppose it is the Gray image under ϕ_k of a linear code over S_k of length n, say $C = \phi_k(D)$. Let $\overline{c} = (\overline{x}_0, \ldots, \overline{x}_{2^k-1})$ be any codeword in C, and suppose that $\overline{c} = \phi_k(\overline{a})$ for some $\overline{a} \in D$. Then since D is linear over S_k, we see that $(1+u)\overline{a} \in D$, and so by the hypothesis, we see that $\phi_k\big((1+u)\overline{a}\big) \in C$, but then by Lemma 5.37, we see that

$$\tau(\overline{c}) = (\overline{x}_{2^k-1}, \overline{x}_0, \ldots, \overline{x}_{2^k-2}) = \phi_k\big((1+u)\overline{a}\big) \in C$$

for all $\overline{c} \in C$. This means that C is invariant under τ, which means that it is invariant under τ^i for all $i = 0, 1, \ldots, 2^k - 1$, which means that C is invariant under the action of the permutation group $\mathbb{Z}_{2^k}$.

Conversely, suppose that C is a binary linear code of length $2^k n$ that is invariant under the action of the permutation group $\mathbb{Z}_{2^k}$. Since ϕ_k is one-to-one and $\mathbb{F}_2$-linear, we can define $\phi_k^{-1} : C \to S_k^n$. Let $D = \phi_k^{-1}(C)$. Since ϕ_k is additive, we see that D is an additive subgroup of S_k^n. All we need to prove now is that D is an S_k-module. For this, all we need to show is that D is invariant under the multiplication from the left by powers of u. We observe, by repeated use of Lemma 5.37 and induction, that

$$\phi_k\big((1+u)^i\overline{a}\big) = \tau^i\big(\phi_k(\overline{a})\big) \tag{5.45}$$

for all $\overline{a} \in S_k^n$ and for all $i = 0, 1, \ldots, 2^k - 1$. So, suppose that $\overline{c} \in C$ and let $\overline{d} = \phi_k^{-1}(\overline{c}) \in D$.

This means that $\phi_k(\overline{d}) = \overline{c}$, and, by (5.45) as well as by the hypothesis, we know that

$$\phi_k\big((1+u)^i\overline{d}\big) = \tau^i(\overline{c}) \in C,$$

which means that by the definition of D that

$$(1+u)^i\overline{d} \in D, \qquad i = 0, 1, \ldots, 2^k - 1.$$

This means that D is invariant under multiplication from the left by $(1+u)^i$ for $i = 0, 1, \ldots, 2^k - 1$. But then, the fact that D is additive and an easy induction leads us to conclude that D is invariant under multiplication from the left by u^i, $\;i = 0, 1, \ldots, 2^k - 1$ and so D is an S_k-module, which means that D is linear over S_k. □

Remark 5.40. Note that if we make the transformation $v = 1 + u$ in S_k we will get an equivalent ring

$$T_k = \mathbb{F}_2 + v\mathbb{F}_2 + \ldots v^{2^k-1}\mathbb{F}_2 \simeq \mathbb{F}_2[X]/(X^{2^k} - 1).$$

In this case, the Gray map that we defined above simplifies quite considerably because one can easily show in that case that

$$\phi_k(\overline{a}_0 + v\overline{a}_1 + \cdots + v^{2^k-1}\overline{a}_{2^k-1}) = (\overline{a}_0, \overline{a}_1, \ldots, \overline{a}_{2^k-1}). \tag{5.46}$$

Of course in that case, Theorem 5.39 becomes quite trivial to prove. Unfortunately I realized this simplification much later than I considered all the cases above.

Bibliography

[1] R.M. Wilson, *A lemma on polynomials modulo p^m and applications to coding theory*, Proc. of Int. Workshop on Comb., Linear Algebra and Graph Coloring, 2003.

[2] A.R. Hammons, V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory, **40** (1994), 301–319.

[3] V. Pless, *Constraints on weights in binary codes*, Applicable Algebra in Engineering, Communication and Computing, **8** (1997), 411–414.

[4] J. Simonis, *Restrictions on the weight distributions of binary linear codes imposed by the structure of Reed-Muller codes*, IEEE Trans. Inform. Theory, **40** (1994), 194–196.

[5] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Phillips Res. Rep. Suppl., **10** (1973)

[6] J.H. van Lint and R.M. Wilson, *A Course in Combinatorics*, Cambridge University Press, (2001)

[7] P.V. Kumar, T. Helleseth, and A.R. Calderbank, *An Upper Bound for Weil Exponential Sums over Galois Rings and Applications*, IEEE Trans. Inform. Theory, **41** (1995), 456–468.

[8] C. Carlet, *$\mathbb{Z}_{2^k}$-linear Codes*, IEEE Trans. Inform. Theory, **44** (1998), 1543–1547.

[9] T.A. Gulliver, and M. Harada, *Codes over $\mathbb{F}_3 + u\mathbb{F}_3$ and Improvements to the Bounds on Ternary Linear Codes*, Des. Cod. Crypt, **22** 2001, 89–96.

[10] S. Ling and J.T. Blackford, *$\mathbb{Z}_{p^{k+1}}$-linear codes*, IEEE Trans. Inform. Theory, **48** (2002), 2592–2605.

[11] K. Betsumiya and S. Ling, F.R. Nemenzo, *Type II Codes over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$*, Discrete Math., **275** (2004), 43–65.

[12] S.T. Dougherty, P. Gaborit, M. Harada, A. Munemasa and P. Solé, *Type IV self-dual codes over rings*, IEEE Trans. Inform. Theory, **45** (1999), 2345–2360.

[13] S.T. Dougherty, P. Gaborit, M. Harada and P. Solé, *Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$*, IEEE Trans. Infrom. Theory, **45** (1999), 32–45.

[14] J.T. Blackford and D.K. Ray-Chaudhuri, *A Transform Approach to Permutation Groups of Cyclic Codes Over Galois Rings*, IEEE Trans. Inform. Theory, **46** (2000), 2350–2358.

[15] P.V. Kumar, T. Helleseth and A.R. Calderbank, *An Upper Bound for Weil Exponential Sums over Galois Rings and Applications*, IEEE Trans. Inform. Theory, **41** (1995), 456–468.

[16] B.K. Dey and B.S. Rajan, *Affine Invariant Extended Cyclic Codes Over Galois Rings*, IEEE Trans. Inform. Theory, **50** (2004), 691–698.

[17] W.C. Huffman, *Decompositions and extremal Type II codes over $\mathbb{Z}_4$*, IEEE Trans. Inform. Theory, **44** (1998), 800–809.

[18] J.F. Voloch and J.L. Walker, *Homogeneous weights and exponential sums*, Finite Fields and Their Applications, (2003), 310–321.

[19] S. Ling and F. Ozbudak, *An Improvement on the Bounds of Weil Exponential Sums over Galois Rings with some Applications*, IEEE Trans. Inform. Theory, **50** (2004), 2529–2539.

[20] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, (1978).

[21] T.W. Hungerford, *Algebra*, Springer, (1974).

[22] M. Grefrath and S.E. Schmidt, *Gray Isometries for finite chain rings and a nonlinear ternary* $(36, 3^{12}, 15)$ *code*, IEEE Trans. Inform. Theory, **45** (1999), 2522–2524.

[23] D. Jungnickel, *Finite Fields: Sturcture and Arithmetics*, Wissenschaftsverlag, Mannheim, (1993).

[24] B.R. MacDonald, *Finite Rings with Identity*, New York: Marcel Dekker (1974).

[25] M. Gerefrath, G. McGuire and M.E. O'Sullivan, *On Plotkin-Optimal Codes over Finite Frobenius Rings*, **submitted to** Journal of Algebra and its Applications, (2005).