2012

Equivalence Theorems and the Local-Global Property

Aleams Barra
University of Kentucky, aleamsbarra@gmail.com

STUDENT AGREEMENT:

I represent that my thesis or dissertation and abstract are my original work. Proper attribution has been given to all outside sources. I understand that I am solely responsible for obtaining any needed copyright permissions. I have obtained and attached hereto needed written permission statements(s) from the owner(s) of each third-party copyrighted matter to be included in my work, allowing electronic distribution (if such use is not permitted by the fair use doctrine).

I hereby grant to The University of Kentucky and its agents the non-exclusive license to archive and make accessible my work in whole or in part in all forms of media, now or hereafter known. I agree that the document mentioned above may be made available immediately for worldwide access unless a preapproved embargo applies.

I retain all other ownership rights to the copyright of my work. I also retain the right to use in future works (such as articles or books) all or part of my work. I understand that I am free to register the copyright to my work.

REVIEW, APPROVAL AND ACCEPTANCE

The document mentioned above has been reviewed and accepted by the student's advisor, on behalf of the advisory committee, and by the Director of Graduate Studies (DGS), on behalf of the program; we verify that this is the final, approved version of the student's dissertation including all changes required by the advisory committee. The undersigned agree to abide by the statements above.

Aleams Barra, Student

Dr. Heide Gluesing-Luerssen, Major Professor

Dr. Peter A. Perry, Director of Graduate Studies

Equivalence Theorems and the Local-Global Property

DISSERTATION

A dissertation submitted in partial
fulfillment of the requirements for
the degree of Doctor of Philosophy
in the College of Arts and Sciences
at the University of Kentucky

By
Aleams Barra
Lexington, Kentucky

Director: Dr. Heide Gluesing-Luerssen, Professor of Mathematics
Lexington, Kentucky 2012

ABSTRACT OF DISSERTATION

Equivalence Theorems and the Local-Global Property

In this thesis we revisit some classical results about the MacWilliams equivalence theorems for codes over fields and rings. These theorems deal with the question whether, for a given weight function, weight-preserving isomorphisms between codes can be described explicitly. We will show that a condition, which was already known to be sufficient for the MacWilliams equivalence theorem, is also necessary. Furthermore we will study a local-global property that naturally generalizes the MacWilliams equivalence theorems. Making use of F-partitions, we will prove that for various subgroups of the group of invertible matrices the local-global extension principle is valid.

KEYWORDS: Codes, Frobenius rings, weight-preserving isomorphisms, MacWilliams equivalence theorem, F-partition

Author's signature: Aleams Barra

Date: April 30, 2012

Equivalence Theorems and the Local-Global Property

By
Aleams Barra

Director of Dissertation: Heide Gluesing-Luerssen

Director of Graduate Studies: Peter A. Perry

Date: April 30, 2012

ACKNOWLEDGMENTS

I am sincerely and heartily grateful to my advisor, Dr. Heide Gluessing-Luerssen, for her constant support and guidance throughout the writing of my dissertation. I am sure it would have not been possible without her help. In addition, I would like to thank other members of my Dissertation Committee, Dr. Uwe Nagel, Dr. Alberto Corso and Dr. Andy Klapper, for their time and valuable comments. I am indebted to Dr. Jay A. Wood, his work on extension theorems lead to many results in this dissertation. My wife, Lia, and my sons, Raka, Hanif and Ilman, support me with their patience and love during my studies, and I could not have gotten this far without them.

Dedicated to my wife, Lia
and
my father, Syahbuddin Mansoer

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1 Introduction

In this thesis we consider isometries between codes. Codes will be submodules of some R^n for a suitable finite, commutative ring R, and isometries are R-isomorphisms between such codes that preserve certain weight functions. Our goal is to describe, for various instances, such isometries explicitly. These considerations are motivated by a fundamental result of MacWilliams from 1962, which has enjoyed various generalizations and has led to many activities at the interface of coding theory and ring theory.

Let us briefly report these results and developments. Let $\mathbb{F}$ be a finite field. In her thesis [29], MacWilliams showed that every Hamming-weight-preserving linear isomorphism f between codes (subspaces) in $\mathbb{F}^n$ is a monomial map; that is, f is given by a permutation and a rescaling of the codeword coordinates. We refer to this result as the MacWilliams equivalence theorem. By translating the Hamming-weight-preserving property into character-theoretic language, an alternative proof for the same result was given by Ward and Wood [38].

In [12], Goldberg generalized the MacWilliams equivalence theorem in the following direction. Let U be a multiplicative subgroup of $\mathbb{F}^*$, the group of units of $\mathbb{F}$, and denote the cosets of U in $\mathbb{F}^*$ by $U_1, U_2, \ldots, U_s$. Then the U-coset weight of $x \in \mathbb{F}^n$ is defined as $W_U(x) := (w_1(x), w_2(x), \ldots, w_s(x))$, where $w_j(x)$ counts the number of components of x that belong to the coset U_j. In the same paper [12], Goldberg showed that every W_U-preserving linear isomorphism f between codes in $\mathbb{F}^n$ extends to a U-monomial map $f : \mathbb{F}^n \to \mathbb{F}^n$; that is, f is a permutation and a rescaling of the coordinates by units from U. This result is a generalization of the MacWilliams equivalence theorem since for $U = \mathbb{F}^*$ the U-coset weight is exactly the Hamming weight. Goldberg also noticed that his result is an analogue to Witt's extension theorem (see [1]).

In the early 1990's, Hammons et. al. [15] proved the groundbreaking result that the binary nonlinear Kerdock and Preparata codes can be considered as linear codes over $\mathbb{Z}_4$ via the Gray map. This initiated the research area of codes over $\mathbb{Z}_4$ and even over more general finite rings, which eventually became an integral part of coding theory. Furthermore, motivated by the particular role of the Lee weight on $\mathbb{Z}_4$, more general weight functions than just the Hamming weight were taken into consideration.

In 1997, Wood [42] generalized the above-mentioned result of Goldberg to codes over finite Frobenius rings. Two years later, in [43] he also extended the MacWilliams equivalence theorem to finite Frobenius rings. The two generalizations were proven using the same character-theoretic techniques that he used with Ward in their proof of the MacWilliams equivalence theorem over fields. A few months after Wood published this result, Greferath and Schmidt [13] gave a combinatorial proof of the MacWilliams equivalence theorem over finite Frobenius rings. Finally, following a strategy of Dinh and López-Permouth [9], Wood [46] showed that the result cannot be extended to more general rings by proving that finite rings for which the MacWilliams equivalence theorem holds true must necessarily be Frobenius rings.

Another direction to generalize the equivalence theorem is to consider weights other than the Hamming weight. In his 1997 paper [42], Wood considered subgroups U of the group of units $\mathcal{U}(R)$ and introduced the notion of a U-weight for weight functions that are constant on the U-orbits. In the same paper, he gave a sufficient condition for a U-weight, extended additively to R^n, to satisfy the equivalence theorem. Using this condition, he showed that all $\mathcal{U}(R)$-weights on chain rings R satisfy the equivalence theorem if the weight function is positive on its domain. Wood claimed in [40] and proved in [41] that the Lee weight and the Euclidean weight satisfy the equivalence theorem for the residue rings $\mathbb{Z}_N$ if N is of the form 2^k or 3^k or if N is a prime number of the form $N = 2p + 1$, where p is also prime.

Before we describe our contributions to this research area, we would like to highlight a question raised by Goldberg in [12]. Goldberg observed that the MacWilliams equivalence theorem and Witt's extension theorem are similar in the sense that any linear isomorphism between two subspaces that preserves a certain metric (Hamming metric in the first case and a quadratic form for the second) can be extended to a matrix multiplication map (in the first case the matrix is a monomial matrix and in the second case the matrix is an orthogonal matrix). Goldberg then asked if one can find subgroups G of $\mathrm{GL}(n, R)$ together with some metric such that every linear isomorphism between two subspaces that preserves this metric can be extended to a G-map.

The main contribution of this thesis is to provide some answers to Goldberg's question. We first reformulate Goldberg's problem as an existence problem of subgroups G of $\mathrm{GL}(n, R)$ that satisfy the local-global property in the sense that every map that is a pointwise G-map is a global G-map. We then show that the group of U-monomial matrices satisfies the local-global property. This result not only gives a more natural proof of Wood's result in [42], but also serves as a model of how to prove the local-global property for other subgroups G of $\mathrm{GL}(n, R)$. We show that the groups of invertible diagonal and invertible lower triangular matrices satisfy the local-global property. This puts us in the position to derive the following results for codes over finite Frobenius rings; they have the same flavor as Witt's extension theorem over fields. We show that every support-preserving linear isomorphism between codes can be extended to a diagonal map. We also prove that every Rosenbloom-Tsfasman-weight-preserving linear isomorphism between codes can be extended to a lower triangular map. Finally, we establish a certain class of subrings of the ring of $n \times n$-matrices, whose group of units is guaranteed to satisfy the local-global property.

Another contribution is in the following area. As we mentioned earlier, Wood [42] provided a sufficient condition, in terms of the invertibility of a certain matrix A, for a weight function on R^n to satisfy the equivalence theorem. We will show that this condition is in fact necessary for weight functions attaining rational values. For certain classes of rings and certain weight functions, namely finite chain rings and finite fields, we reveal the structure of the matrix A and take advantage of this additional information to establish the invertibility of A. More precisely, for a $\mathcal{U}(R)$-weight function on R^n, where R is a finite chain ring, we show that up to row and column permutations, the matrix A is a triangular matrix. This leads us to recover some of Wood's result in [42]. Furthermore, for a U-weight over finite fields, the

matrix A is circulant. By exploiting this circulant structure, we reprove Wood's result that the Lee weight satisfies the equivalence theorem over the rings $\mathbb{Z}_N$, where N is a prime of the form $2p+1$ with p being prime itself, and we also show the new result that the same is true for prime numbers $N = 4p+1$ where p is prime.

Summarizing, the following results in this thesis are new: Theorem 5.6 and consequences, Theorem 5.28, and all results in Chapter 6 without Theorem 6.2 and Lemma 6.32.

The thesis is organized as follows. In Chapter 2 we introduce some basic notions of coding theory over rings. We also discuss some basic properties of characters over additive abelian groups that will be needed in the following chapters.

In Chapter 3 we reprove the classical result of MacWilliams' equivalence theorem in two ways. The first leads to a general condition for weight functions over fields to satisfy the equivalence theorem. The second one familiarizes us with the character-theoretic technique that we will employ often later.

In Chapter 4 we present Wood's proof for the generalization of MacWilliams' and Goldberg's result over admissible rings (Frobenius rings). We present the proof in such away that admissible rings appear naturally as those that make the proofs over fields work again.

In Chapter 5 we first observe that in order for the equivalence theorem between any two modules to be valid it is enough to show the validity for cyclic modules. This helps us to immediately obtain a sufficient condition, in terms of the invertibility of a certain matrix A, for a weight function to satisfy the equivalence theorem. For rational-valued weight functions, we show that this condition is necessary and show that – although the condition is much simpler than the one in Chapter 3 – the two conditions are actually equivalent. Furthermore, we will show that over finite fields, the matrix A has the nice structure of a circulant. By exploiting this structure, we prove the equivalence theorem for the Lee weight over the residue rings $\mathbb{Z}_N$, where N takes the particular values mentioned above.

In Chapter 6 we start with a motivation that Witt's extension theorem and Goldberg's result can be formulated in terms of the local-global property. Then we introduce and discuss some properties of F-partitions. These partitions form a close link to characters and will be a main tool for establishing that certain subgroups satisfy the local-global property. They will allow us to derive the results we discussed on the previous page.

Finally, in the last chapter we give a broad overview that connects the results of the two previous chapters and offers some directions of how to further the research.

Chapter 2 General Notions and Basic Results

Before we start with the formal notation, let use give a brief motivation.

Linear block codes are the main tool for ensuring the integrity of data transmission over a channel. Messages are assumed to be vectors over a certain finite field. Before being sent, they are encoded in such a way the receiver has a chance to reconstruct the original message from the received, and generally erroneous, message. Algebraically, encoding is simply a linear map from the domain of all possible messages. The image, a certain vector space, is called the associated code. In order to deal with transmission errors, one needs a tool for measuring such errors. Traditionally, this is achieved by the Hamming metric, which simply counts the number of distinct entries in two vectors. Decoding, that is recovering the original message, amounts to finding the codeword that most likely has been sent. Under certain assumptions on the transmission channel, this is equivalent to applying the minimum distance decoding rule: if a word y is received, this rule will decode y to x_y so that the Hamming distance between x_y and y is minimal among all possible codewords. A code is called ε-error-correcting if this procedure is able to correct up to ε errors.

One main theme of coding theory is to find codes with large error-correcting capability. Furthermore, mathematically one is interested in understanding as to when two codes can be regarded the same with respect to their error-correcting capability. Taken the above into account, this translates into when two codes are isomorphic as vector spaces and such that the isomorphism preserves the Hamming metric. In other words, when are two codes isometric? The classical MacWilliams equivalence theorem, discussed in Chapter 3, gives an explicit description of isometric codes.

Around 1970 several binary non-linear codes having at least twice as many codewords as any linear code with the same error-correcting capability have been constructed. Among them are the Preparata codes and the Kerdock codes. Mysteriously, the transform of the weight enumerator of the Preparata is that of the Kerdock code of the same length, while they are not dual to each other. In 1994 Hammons et. al. ([15]) made a breakthrough in explaining this problem. They showed that the Kerdock code can be viewed as a cyclic linear code over $\mathbb{Z}_4$ and the dual of its binary image under the Gray map can be considered as a variant of the Preparata code. The Gray map gives a weight preserving map from $\mathbb{Z}_4^n$ with the Lee weight to $\mathbb{Z}_2$ with the Hamming weight. This result has led to active research of codes over $\mathbb{Z}_4$ and over finite rings in general and also triggered interest in codes with different weights.

For application, the Gray map is also used in data transmission with the QPSK modulation. It is implemented to assign 2 information bits into four possible phases. The advantage of this assignment is that only a single bit error occurs in the 2-bit sequence when noise causes the incorrect selection of an adjacent phase to the transmitted phase. Some of the popular applications of QPSK include CDMA systems, digital video broadcasting satellite (DVB-S) and cable modems.

In this chapter we will introduce the basic notions for codes over rings as needed for this thesis. After introducing the general concept of a weight function, we will

discuss weight preserving maps (called isometries) and various forms of monomial maps. Finally we will present some basic concepts of character theory.

Throughout this chapter, let R be a finite commutative ring with identity. We will denote the group of units of R by $\mathcal{U}(R)$.

2.1 Linear Codes Over Rings

Definition 2.1. Let R^n be the R-module of all n-tuples over the ring R. Elements of R^n will be written as row vectors. A *linear code* $\mathcal{C}$ over R is an R-submodule of R^n. The members of $\mathcal{C}$ are called *codewords*. A *generator matrix* G for $\mathcal{C}$ is a matrix whose rows generates $\mathcal{C}$, i.e., every codeword in $\mathcal{C}$ can be written as a linear combination of the row vectors of G.

We need here to emphasize the difference between linear codes over rings and linear codes over fields. If R is a field, then $\mathcal{C}$ is a subspace of R^n. If $\mathcal{C}$ has dimension k then we say that $\mathcal{C}$ is an $[n, k]$ linear code and in this case we also require the rows of the generator matrix for $\mathcal{C}$ to be linearly independent. So all the generator matrices are of the size $k \times n$.

When R is just a ring, $\mathcal{C}$ is not necessary a free module, hence we cannot talk about dimension and there is no specific size of the generator matrix for $\mathcal{C}$.

2.2 Weight Functions

When a codeword $x \in \mathcal{C}$ is sent trough a channel, the noise in the form of an error vector e distorts the codeword and produces the vector $y = x + e$ at the other end of the channel. To measure this distortion, Hamming [14] introduced the distance function $D(x, y)$ which measures in how many positions x and y differ, that is

$$D(x, y) = |\{i \mid x_i \neq y_i\}| \text{ for } x,\, y \in R^n.$$

This distance function satisfies the distance axiom for a metric space as we can see from the following proposition.

Proposition 2.2. *The distance function $D(x, y)$ satisfies the distance properties:*

1. $D(x, y) \geq 0$ *for all* $x, y \in R^n$.
2. $D(x, y) = 0$ *if and only if* $x = y$.
3. $D(x, y) = D(y, x)$ *for all* x, y *in* R^n.
4. $D(x, z) \leq D(x, y) + D(y, z)$ *for every* $x, y, z \in R^n$.

Properties (i),(ii) and (iii) are obvious; (iv) is a simply exercise [18] pp.8 or [30] pp.13.

Another metric that is commonly used for error correcting purposes is the Lee distance. It was first introduced by Lee [27] in 1958 and measures the distance

between two points on a circle. Suppose there are N points on the circle and that we label them with $0, 1, ..., N-1$. The distance between two points x and y is the minimum number of arcs (clockwise or counter-clock wise) to go from x to y. Because of this reason, originally Lee called this distance the *circular* distance. We will formally define this metric on the integer residue ring $\mathbb{Z}_N$ as follows. First we denote the elements of $\mathbb{Z}_N$ by $0, 1, \ldots, N-1$. Then the Lee distance on $\mathbb{Z}_N$ is defined as

$$\rho(x, y) = \min\{x - y \bmod N, y - x \bmod N\}.$$

For example in $\mathbb{Z}_8$, we have $\rho(7, 2) = 3$ since $7 - 2 = 5$ and $2 - 7 = -5 = 3$ in $\mathbb{Z}_8$. One can also see that $\rho(7, 2) = 3$ from the picture below.

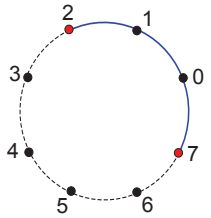


Figure 2.1: The Lee distance between 2 and 7

We can extend this distance to the module $\mathbb{Z}_N^n$ by defining

$$\rho(x, y) = \sum_{i=1}^{n} \rho(x_i, y_i).$$

It is easy to see that the Lee distance satisfies the properties of Proposition 2.2.

In this thesis we will consider very general weight functions. In the following definition note that we do not require a weight to satisfy the properties of a metric given in Proposition 2.2.

Definition 2.3. A *weight* w on the ring R is a function $w : R \to \mathbb{C}$ such that $w(0) = 0$. Let U be a multiplicative subgroup of $\mathcal{U}(R)$. We say that the weight w is a *U-weight* if $w(\alpha x) = w(x)$ for all $x \in R$ and $\alpha \in U$. The biggest subgroup U for which w is a U-weight is called the *symmetry group of the weight* w and we denote it by $\mathrm{Sym}(w)$.
Each weight function on R can naturally be extended to R^n. The resulting function on R^n will be denoted by w as well, thus,

$$w(x) = \sum_{i=1}^{n} w(x_i) \text{ for all } x \in R^n. \tag{2.1}$$

If w is a U-weight, then $w(\alpha x) = w(x)$ for all $x \in R^n$ and $\alpha \in U$.

Obviously, every weight function on R is a $\{1\}$-weight. To present non-trivial examples of U-weights, we first give the following definition.

Definition 2.4. The *Hamming weight* w_H on any ring R is defined by

$$w_H(x) = \begin{cases} 1 & , \text{ if } x \neq 0 \\ 0 & , \text{ if } x = 0 \end{cases}.$$

The *Lee weight* w_L on the ring $\mathbb{Z}_N$ is defined as

$$w_L(m) = \min\{m \bmod N, (N-m) \bmod N\} \text{ for all } m \in \mathbb{Z}_N$$

(where, as usual, mod N refers to the remainder in the set $\{0, \ldots, N-1\}$).

From the definition above we can see that the Hamming weight is a $\mathcal{U}(R)$-weight and the Lee weight is a $\{\pm 1\}$-weight. In fact $\mathrm{Sym}(w_H) = \mathcal{U}(R)$ and $\mathrm{Sym}(w_L) = \{\pm 1\}$. We can view the Hamming weight and the Lee weight on R^n in terms of the Hamming distance D and the Lee distance ρ. Using the extension in Equation (2.1) we have

$$\begin{aligned} w_H(x) &= D(x, 0) = |\{i \mid x_i \neq 0\}| \\ w_L(x) &= \rho(x, 0). \end{aligned}$$

2.3 Isometries and Monomial Maps

We would like to have a notion to say that two codes, $\mathcal{C}$ and $\mathcal{C}'$ are "essentially the same". As a first attempt, we can say that $\mathcal{C}$ and $\mathcal{C}'$ are the same if every codeword in $\mathcal{C}'$ is just a rearrangement of some codeword in $\mathcal{C}$, that is, if there is a permutation $\sigma \in S_n$ such that the assignment $(x_1, \ldots, x_n) \mapsto (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ gives a one-to-one correspondence between $\mathcal{C}$ and $\mathcal{C}'$. In this case we say that $\mathcal{C}$ and $\mathcal{C}'$ are *permutation equivalent*.

If we also take the Hamming weight into account, we can allow some scaling to take place and still consider the two codes as being the same. This is because the scaling process does not change the Hamming weight of a vector. We say that $\mathcal{C}$ and $\mathcal{C}'$ are *monomially equivalent* if there is some permutation σ in S_n and scalars $\alpha_1, \ldots, \alpha_n \in \mathcal{U}(R)$ such that the map from $\mathcal{C}$ to $\mathcal{C}'$ given by

$$(x_1, \ldots, x_n) \mapsto (\alpha_1 x_{\sigma(1)}, \ldots, \alpha_n x_{\sigma(n)})$$

is a one-to-one correspondence.

To make these two notions of equivalence more compact we will write them in matrix form. To do so we need the following definition.

Definition 2.5. Denote the set of $n \times n$ permutation matrices over the ring R by $\mathcal{P}(n, R)$. A *monomial matrix* over R is a matrix M that can be written as $M = PD$ where P is in $\mathcal{P}(n, R)$ and D is a diagonal matrix where the diagonal entries are elements of $\mathcal{U}(R)$. If the diagonal entries in D are elements of a subgroup U of $\mathcal{U}(R)$, we say that M is a *U-monomial matrix*. We denote the set of all monomial and U-monomial $n \times n$ matrices over R respectively by $\mathcal{M}(n, R)$ and $\mathcal{M}_U(n, R)$.

Let $\mathrm{GL}(n, R)$ be the group of all $n \times n$ invertible matrices with entries from R. It is not difficult to see that $\mathcal{P}(n, R), \mathcal{M}(n, R)$ and $\mathcal{M}_U(n, R)$ are subgroups of $\mathrm{GL}(n, R)$. Now we are ready to give the definition of permutation equivalence and monomial equivalence in terms of permutation and monomial matrices.

Definition 2.6. Two codes $\mathcal{C}$ and $\mathcal{C}'$ in R^n are *permutation equivalent* (respectively *monomially equivalent*) if there are generator matrices G for $\mathcal{C}$ and G' for $\mathcal{C}'$ such that $G' = GP$ for some $P \in \mathcal{P}(n, R)$ (respectively $G' = GM$ for some $M \in \mathcal{M}(n, R)$). If M is in $\mathcal{M}_U(n, R)$ then we say that $\mathcal{C}$ and $\mathcal{C}'$ are *U-monomially equivalent*. We also write $\mathcal{C}' = \mathcal{C}P$ or $\mathcal{C}' = \mathcal{C}M$ to indicate that $\mathcal{C}$ and $\mathcal{C}'$ are permutation or monomially equivalent without explicitly mentioning specific generator matrices.

Another key concept is that of a monomial map. A map $f : R^n \to R^n$ is said to be a monomial map if there is a monomial matrix M that represents f. More generally we define the following.

Definition 2.7. A linear map $f : R^n \to R^n$ is called a *U-monomial map* if there is an $M \in \mathcal{M}_U(n, R)$ such that $f(x) = xM$ for all $x \in R^n$ or, equivalently, if there are $\alpha_1, \ldots, \alpha_n \in U$ and $\sigma \in S_n$ such that

$$f(x) = (\alpha_1 x_{\sigma(1)}, \ldots, \alpha_n x_{\sigma(n)})$$

for all $x \in R^n$. If $U = \mathcal{U}(R)$ we simply call f a *monomial map*.

Notice that every $M \in \mathcal{M}(n, R)$ preserves the Hamming weight in the sense that $w_H(x) = w_H(xM)$ for every $x \in R^n$. In this case we say that a monomial map is a Hamming weight isometry in the sense of the following definition.

Definition 2.8. Let w be a U-weight and $\mathcal{C}$, $\mathcal{C}'$ be codes in R^n. We say that a map $f : \mathcal{C} \to \mathcal{C}'$ is a *w-isometry* (and $\mathcal{C}$ and $\mathcal{C}'$ are *w-isometric*) if f is a linear isomorphism and f preserves w, that is, for every $x \in \mathcal{C}$ we have

$$w(x) = w(f(x)).$$

Obviously, if $f : \mathcal{C} \to \mathcal{C}'$ is the restriction of a U-monomial map on R^n, then f is a w-isometry for every U-weight w. In this thesis we will be concerned with the converse, that is, whether a given w-isometry $f : \mathcal{C} \to \mathcal{C}'$, where w is a U-weight, is the restriction of a U-monomial map on R^n.

The most classical case is that of a Hamming weight isometry, and the question amounts to whether a w_H-isometry $f : \mathcal{C} \to \mathcal{C}'$ is the restriction of some monomial map M on $\mathcal{C}$. It was first proved by MacWilliams [29] that this is indeed true when R is a field. Since then there have been many generalizations of that result to more general rings and weights. We will discuss these results in the next chapters.

2.4 Basic Notions of Character Theory

In this section G will always be a finite abelian group, written additively. A *character* χ on G is a group homomorphism $\chi : G \to \mathbb{C}^*$, where $\mathbb{C}^*$ is the multiplicative group of nonzero complex numbers.

While all the results in this section are well known (see for example [36] and [19]), they do not always appear in the form needed for our purposes. Therefore, we choose to devote this section to deriving the necessary character theory in a self-contained form.

If G is of order n and χ is a character on G, we have

$$\chi(g)^n = \chi(ng) = \chi(0) = 1$$

for all $g \in G$. Hence $\chi(g)$ is an nth root of unity. Since

$$1 = \chi(0) = \chi(g + (-g)) = \chi(g)\chi(-g),$$

we also have

$$\chi(-g) = \chi(g)^{-1} = \overline{\chi(g)}$$

where the bar indicates the complex conjugation. We call the character χ_0 defined by $\chi_0(g) = 1$ for every $g \in G$ the *principal character*.

Let $\widehat{G}$ be the set of all characters on G. By defining $(\chi \cdot \psi)(g) = \chi(g)\psi(g)$ for all $g \in G$, the set $\widehat{G}$ is an abelian group, and $\overline{\chi}$ defined by $\overline{\chi}(g) := \overline{\chi(g)}$ is the inverse of χ in $\widehat{G}$. We call $\widehat{G}$ the *character group* of G.

Below we will show that the character group $\widehat{G}$ is isomorphic to G. In order to do so we will use the fundamental theorem of finite abelian groups which says that G is isomorphic to a direct sum $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ for some $n_1, \ldots, n_k$. Then to prove that $G \cong \widehat{G}$, it is enough to show that the result is true for $G = \mathbb{Z}_n$ and to show that $\widehat{H_1 \oplus H_2} \cong \widehat{H_1} \oplus \widehat{H_2}$. We will prove this in the following lemmas.

Lemma 2.9. $\widehat{\mathbb{Z}_n} \cong \mathbb{Z}_n$

Proof. Let $\omega \in \mathbb{C}$ be a primitive nth root of unity. For any $j \in \{0, 1, \ldots, n-1\}$, the map χ_j defined by

$$\chi_j(g) := \omega^{jg}$$

for $g \in \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is well-defined and in fact a character on $\mathbb{Z}_n$. Let χ be any character. Then $\chi(1)$ is a nth root of unity and hence $\chi(1) = \omega^j$ for some j. It follows that $\chi = \chi_j$. Thus $\widehat{\mathbb{Z}_n} = \{\chi_0, \chi_1, \ldots, \chi_{n-1}\}$. By definition of χ_j, we have $\chi_j = (\chi_1)^j$ for all $j = 0, \ldots, n-1$. Hence $\widehat{\mathbb{Z}_n}$ is a cyclic group of order n and isomorphic to $\mathbb{Z}_n$. □

Lemma 2.10. *If $G = H_1 \oplus H_2$ then $\widehat{G} \cong \widehat{H_1} \oplus \widehat{H_2}$.*

Proof. Let $\chi_1 \in \widehat{H_1}$ and $\chi_2 \in \widehat{H_2}$. Define $\chi = \chi_1 \oplus \chi_2$ by

$$\chi(h_1, h_2) := \chi_1(h_1)\chi_2(h_2)$$

for all $(h_1, h_2) \in H_1 \oplus H_2$. One can check that $\chi \in \widehat{G}$. The map $\widehat{H_1} \oplus \widehat{H_2} \to \widehat{G}$ given by $(\chi_1, \chi_2) \mapsto \chi_1 \oplus \chi_2$ is clearly a homomorphism. If $1 = (\chi_1 \oplus \chi_2)(h_1, h_2) = \chi_1(h_1)\chi_2(h_2)$ for all (h_1, h_2) then $\chi_1(h_1) = 1$ and $\chi_2(h_2) = 1$ for all $h_1 \in H_1$ and $h_2 \in H_2$. Hence χ_1, χ_2 are principal characters and hence the map $(\chi_1, \chi_2) \mapsto \chi_1 \oplus \chi_2$ is injective. Conversely, if $\chi \in \widehat{G}$, then the restriction $\chi_i := \chi \mid_{H_i}$ is a character on H_i and $\chi = \chi_1 \oplus \chi_2$. □

As a consequence of the above, G and $\widehat{G}$ are isomorphic.

Proposition 2.11. $G \cong \widehat{G}$

Proof. By the fundamental theorem of abelian groups we have $G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$. It follows that

$$G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k} \cong \widehat{\mathbb{Z}_{n_1}} \oplus \cdots \oplus \widehat{\mathbb{Z}_{n_k}} \cong \widehat{G}.$$

□

Remark 2.12. Let g be a non-zero element in $\mathbb{Z}_n$. Let χ_j be the character on $\mathbb{Z}_n$ as defined in the proof of Lemma 2.9. Choose j such that $\gcd(j, n) = 1$. Suppose that $\chi_j(g) = 1$. Then $\omega^{jg} = 1$ and hence $n \mid gj$. But since $\gcd(j, n) = 1$, then $n \mid g$. But this is impossible because $g \in \{1, \ldots, n-1\}$. Therefore there exists a character $\chi \in \widehat{\mathbb{Z}_n}$ for which $\chi(g) \neq 1$. We will show in the following lemma that this result is true for a general group G.

Lemma 2.13. *Let $g \neq 0 \in G$. Then there exist a $\chi \in \widehat{G}$ such that $\chi(g) \neq 1$.*

Proof. By the fundamental theorem of finite abelian groups we may assume that $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$. Let $g \neq 0 \in G$. Write $g = (g_1, g_2, \ldots, g_k) \in \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$. Since $g \neq 0$, then $g_i \neq 0$ for some i. Without loss of generality let $g_1 \neq 0$. By Remark 2.12, there is a character χ_1 on $\mathbb{Z}_{n_1}$ such that $\chi_1(g_1) \neq 1$. Let $\chi_2, \ldots, \chi_k$ be the principal characters on $\mathbb{Z}_{n_2}, \ldots, \mathbb{Z}_{n_k}$. Then $\chi := \chi_1 \oplus \chi_2 \oplus \cdots \oplus \chi_k$ is a character on G and

$$\chi(g) = \chi_1(g_1)\chi_2(g_2) \cdots \chi_k(g_k) = \chi_1(g_1) \neq 1.$$

□

The following results will be important in translating weight preserving properties in character theory language.

Proposition 2.14.

$$\sum_{g \in G} \chi(g) = \begin{cases} |G|, & \text{if } \chi \text{ is principal} \\ 0, & \text{otherwise} \end{cases}$$

Proof. The case where χ is principal is obvious since $\chi(g) = 1$ for all $g \in G$. If χ is not principal, there is an $a \in G$ such that $\chi(a) \neq 1$. Then

$$\sum_{g \in G} \chi(a + g) = \sum_{g \in G} \chi(a)\chi(g) = \chi(a) \sum_{g \in G} \chi(g)$$

On the other hand

$$\sum_{g\in G}\chi(a+g)=\sum_{h\in G}\chi(h)=\sum_{g\in G}\chi(g).$$

Therefore

$$(\chi(a)-1)\sum_{g\in G}\chi(g)=0.$$

Since $\chi(a)\neq 1$, the conclusion follows. □

Corollary 2.15. *Let χ and ψ be two characters on G. Then*

$$\sum_{g\in G}\chi(g)\overline{\psi(g)}=\begin{cases}|G|, & \text{if } \chi=\psi\\ 0, & \text{if } \chi\neq\psi\end{cases}.$$

Proof. If $\chi=\psi$, then $\chi(g)\overline{\psi(g)}=1$ and the conclusion follows. If $\chi\neq\psi$, then $\chi\overline{\psi}$ is a non principal character and hence $\sum_g\chi(g)\overline{\psi(g)}=0$. □

Consider the $\mathbb{C}$-vector space $\mathbb{C}^G$ consisting of all functions $\phi: G\to\mathbb{C}$. One can check that

$$\langle\phi,\psi\rangle:=\frac{1}{|G|}\sum_{g\in G}\phi(g)\overline{\psi(g)}$$

defines an inner product on $\mathbb{C}^G$. By Corollary 2.15, the set of all characters on G forms an orthonormal set. But every orthonormal set is linearly independent. Therefore we have the following proposition (often attributed to Dedekind) that we will use often.

Proposition 2.16. *Let $n\in\mathbb{N}$. If $\chi_1,\ldots,\chi_n$ are distinct characters on G, then they are linearly independent as elements of $\mathbb{C}^G$.*

Corollary 2.17. *Let χ_i, $i=1,\ldots,n$, and ψ_j, $j=1,\ldots,m$, be characters on G. If*

$$\chi_1+\cdots+\chi_n=\psi_1+\cdots+\psi_m, \tag{2.2}$$

then $\{\chi_1,\ldots,\chi_n\}=\{\psi_1,\ldots,\psi_m\}$ as multisets.

Proof. Let $\phi_1,\ldots,\phi_s$ be all distinct characters among $\chi_1,\ldots,\chi_n,\psi_1,\ldots,\psi_m$. For $i=1,\ldots,s$, let a_i (respectively b_i) be the number of characters on the left-side (respectively right-side) of the Equation (2.2) that are equal to ϕ_i. Then Equation (2.2) can be written as

$$\sum_{i=1}^{s}a_i\phi_i=\sum_{i=1}^{s}b_i\phi_i$$

which is equivalent to

$$\sum_{i=1}^{s}(a_i-b_i)\phi_i=0.$$

By Proposition 2.16, $a_i=b_i$ for all $i=1,\ldots,s$. Then obviously $\{\chi_1,\ldots,\chi_n\}=\{\psi_1,\ldots,\psi_m\}$ as multisets. □

Notice that since $G \cong \widehat{G}$, clearly $G \cong \widehat{\widehat{G}}$. In fact we can identify G with $\widehat{\widehat{G}}$ via the map $g \mapsto \theta_g$, where θ_g is defined by $\theta_g(\chi) := \chi(g)$ for all $\chi \in \widehat{G}$. By Lemma 2.13 the map $g \mapsto \theta_g$ is a group isomorphism. As a consequence, G and $\widehat{\widehat{G}}$ are canonically isomorphic (whereas there is in general no canonical isomorphism between G and $\widehat{G}$). Applying Proposition 2.14 to the characters on $\widehat{G}$, we have

$$\sum_{\chi \in \widehat{G}} \theta_g(\chi) = \begin{cases} |\widehat{\widehat{G}}|, & \theta_g \text{ is principal in } \widehat{\widehat{G}} \\ 0, & \text{otherwise.} \end{cases}$$

Now since $\theta_g(\chi) = \chi(g)$ and $G \cong \widehat{\widehat{G}}$ and θ_g is principal iff $g = 0$ (by Lemma 2.13), we have the following.

Proposition 2.18.

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G|, & g = 0, \\ 0, & g \neq 0. \end{cases}$$

Chapter 3 Equivalence Theorems for Codes over Fields

In this chapter let R be a finite field.

We will begin with revisiting the classical MacWilliams Equivalence Theorem which states that every Hamming weight preserving map between codes over fields is a monomial map ([29]). We first reproduce an elementary proof and next, in Section 3.2, a character theoretic proof. Both are from the literature, but will be presented in a way that will allow us to use the central ideas for later generalizations. In Section 3.3 we derive a sufficient criterion for the MacWilliams Equivalence Theorem to hold true for general U-weights, where U is a multiplicative subgroup of R. Thereafter, a result from the literature will be derived that establishes the MacWilliams equivalence theorem for certain partition preserving isomorphisms. Finally, in the last section the equivalence theorem will be rephrased as an extension theorem, which then will motivate our approach in Chapter 6.

3.1 MacWilliams Equivalence Theorem for the Hamming Weight

We consider the following situation. Let $\mathcal{C}$ and $\mathcal{C}'$ be two $[n,k]$ codes in R^n and suppose $f : \mathcal{C} \to \mathcal{C}'$ is a Hamming weight isometry (see Definition 2.8). The MacWilliams Equivalence Theorem states that $\mathcal{C}$ and $\mathcal{C}'$ are monomially equivalent, i.e., there is an $M \in \mathcal{M}(n,R)$ such that $\mathcal{C}' = \mathcal{C}M$. We will present a proof similar to that in [18]. It will allow us later on to adopt the idea for more general U-weights. In the next section we will also reproduce a character theoretic proof as found by Ward and Wood in [38].

Before stating and proving the result, let us first discuss the main idea and concepts. We need two $k \times n$ generator matrices G and G' of $\mathcal{C}$ and $\mathcal{C}'$ respectively such that $G' = GM$. This means that the two generator matrices are the same up to column permutation and column scaling by units in R. Since the column vectors of $G \in R^{k\times n}$ are vectors in R^k, the following notation will be crucial.

Let $V_1, \ldots, V_r$ be all one-dimensional subspaces of the vector space R^k, and let v_i be a fixed basis vector of V_i. It is known that if $|R| = q$, then the number of such subspaces is $r = \dfrac{q^k - 1}{q - 1}$. For $G \in R^{k\times n}$ denote by $n_i(G)$ the number of nonzero columns of G that belong to V_i (of course we allow $n_i(G)$ to be zero here). We slightly abuse the notation since technically vectors in V_i are row vectors. Now it is clear that two codes $\mathcal{C}$ and $\mathcal{C}'$ are monomially equivalent if there exist generator matrices G and G' of $\mathcal{C}$ and $\mathcal{C}'$ such that $n_i(G) = n_i(G')$ for all $i = 1, \ldots, r$.

Recall the Hamming weight w_H on R from Definition 2.4 and its extension $w_H(x) = \sum_{i=1}^{n} w_H(x_i)$ to R^n from Definition 2.3.

Theorem 3.1 (MacWilliams Equivalence Theorem [29])**.** *Let $\mathcal{C}$ and $\mathcal{C}'$ be two $[n,k]$ codes over R. Then $\mathcal{C}$ and $\mathcal{C}'$ are w_H-isometric if and only if $\mathcal{C}$ and $\mathcal{C}'$ are monomially equivalent.*

Proof. (see also [18]) ($\Leftarrow$) If $\mathcal{C}' = \mathcal{C}M$ for some $M \in \mathcal{M}(n, R)$, then the map $x \mapsto xM$ defines a w_H-isometry.

($\Rightarrow$) Let $f : \mathcal{C} \to \mathcal{C}'$ be a w_H-isometry. Moreover, let G be a $k \times n$ generator matrix for $\mathcal{C}$ and let r_i be the ith row of G. Define G' to be the matrix whose ith row is $f(r_i)$. Then it is clear that $G' \in R^{k\times n}$ is a generator matrix of $\mathcal{C}'$. As we discussed earlier, it is enough to show that $n_i(G) = n_i(G')$ for every i.

Note that $f(xG) = xG'$ for all $x \in R^k$. Since f is a w_H-isometry, we have $w_H(xG) = w_H(xG')$ for every $x \in R^k$. Let c_i and c'_i, $i = 1, \ldots, n$, be the columns of G and G'. Then

$$w_H(xc_1, \ldots, xc_n) = w_H(xc'_1, \ldots, xc'_n),$$

thus

$$\sum_{i=1}^{n} w_H(xc_i) = \sum_{i=1}^{n} w_H(xc'_i).$$

Each of the $n_j(G)$ columns in G which are in V_j contributes $w_H(x \cdot v_j)$ to the total weight on the left-side. Here $x \cdot v_j$ is the usual dot product on R^k (recall that vectors in R^k are row vectors). It follows that

$$\sum_{j=1}^{r} w_H(x \cdot v_j) n_j(G) = \sum_{j=1}^{r} w_H(x \cdot v_j) n_j(G').$$

By choosing $x = v_i$ for $i = 1, \ldots, r$ we obtain r equations that can be written in the form

$$A \begin{pmatrix} n_1(G) \\ n_2(G) \\ \vdots \\ n_r(G) \end{pmatrix} = A \begin{pmatrix} n_1(G') \\ n_2(G') \\ \vdots \\ n_r(G') \end{pmatrix},$$

where

$$A = \begin{pmatrix} w_H(v_1 \cdot v_1) & w_H(v_1 \cdot v_2) & \cdots & w_H(v_1 \cdot v_r) \\ w_H(v_2 \cdot v_1) & w_H(v_2 \cdot v_2) & \cdots & w_H(v_2 \cdot v_r) \\ \vdots & \vdots & & \vdots \\ w_H(v_r \cdot v_1) & w_H(v_r \cdot v_2) & \cdots & w_H(v_r \cdot v_r) \end{pmatrix} \in \mathbb{Q}^{r\times r}. \tag{3.1}$$

If we can show that A is invertible, then all this implies $n_j(G) = n_j(G')$ for all j and thus $\mathcal{C}$ and $\mathcal{C}'$ are monomially equivalent, as desired. The invertibility of A follows from the next two lemmas. □

Lemma 3.2. *Let W be a subspace of R^k and $v \notin W^\perp$. Then*

$$\sum_{w\in W} w_H(w \cdot v)$$

does not depend on the choice of $v \notin W^\perp$.

Proof. Let $v \notin W^\perp$. The linear map

$$\begin{aligned} \alpha_v : W &\to R \\ w &\mapsto w \cdot v \end{aligned}$$

has rank 1, and hence $\ker \alpha_v$ is of co-dimension 1. Therefore $\ker \alpha_v := \{w \in W \mid v \cdot w = 0\}$ is isomorphic to $R^{\dim W - 1}$. So the cardinality of $\ker \alpha_v$ does not depend on the choice of $v \notin W^\perp$. Now since

$$\sum_{w \in W} w_H(w \cdot v) = |W| - |\ker \alpha_v|$$

then $\sum_{w \in W} w_H(w \cdot v)$ is also independent of the choice of $v \notin W^\perp$. □

Lemma 3.3. *The matrix $A = (w_H(v_i \cdot v_j)) \in \mathbb{Q}^{r \times r}$ is invertible.*

Proof. First we want to show that if we add all the rows of A, the resulting vector x is of the form $x = (\alpha, \cdots, \alpha)$ for some $\alpha \neq 0$. The jth entry of x is given by

$$\begin{aligned} \sum_{i=1}^{r} w_H(v_i \cdot v_j) &= \frac{1}{|R| - 1} \sum_{i=1}^{r} \sum_{w \in V_i} w_H(w \cdot v_j) \\ &= \frac{1}{|R| - 1} \sum_{w \in R^k} w_H(w \cdot v_j). \end{aligned} \tag{3.2}$$

The first equality is true since for each i there are $|R| - 1$ non-zero multiples of v_i in V_i. By Lemma 3.2, the sum on the right-hand side of Equation (3.2) is independent of the choice of j. Hence $x = (\alpha, \ldots, \alpha)$, where α is the right-side of (3.2). It follows that $(1, 1, \ldots, 1)$ is in the row space of A.

Next fix some $t \in \{1, \ldots, r\}$ and consider all rows of A for which v_i is orthogonal to v_t. Add all these rows and call the resulting vector y. Then for $j \neq t$ the jth component of y is

$$\begin{aligned} \sum_{i : v_i \perp v_t} w_H(v_i \cdot v_j) &= \frac{1}{|R| - 1} \sum_{i : v_i \perp v_t} \sum_{v \in V_i} w_H(v \cdot v_j) \\ &= \frac{1}{|R| - 1} \sum_{v \in \langle v_t \rangle^\perp} w_H(v \cdot v_j). \end{aligned} \tag{3.3}$$

For any $j \neq t$, the vector v_j is not a multiple of v_t, that is $v_j \notin \langle v_t \rangle = \langle v_t \rangle^{\perp\perp}$. So by Lemma 3.2 we have that $y = (\beta, \ldots, \beta, \overset{t\text{th}}{0}, \beta, \cdots, \beta)$, where β is the right-side of (3.3). It follows that for every t the vector $(1, \ldots, 1, \overset{t\text{th}}{0}, 1, \ldots, 1)$ is in the row space of A. As a consequence, for every $t = 1, \ldots, r$

$$e_t = (1, \ldots, 1) - (1, \ldots, 1, \overset{t\text{th}}{0}, 1, \ldots, 1)$$

is in the row space of A, and therefore A is invertible over $\mathbb{Q}$. □

All of this concludes the proof of Theorem 3.1.

3.2 Character Theoretic Proof of the MacWilliams Equivalence Theorem

In this section we will present a character theoretic proof of the MacWillams equivalence theorem as given by Ward and Wood in [38]. Before we start with the proof we need some preparation.

Throughout, let χ be a fixed non principal character on R (considered as an additive group).

Let V be an R-vector space. Then every linear map $g : V \to R$, that is $g \in \mathrm{Hom}_R(V, R)$, gives rise to a character $\chi \circ g$ on V. We will show that this assignment is injective.

Lemma 3.4. *Consider $Hom_R(V, R)$ as an additive group. Then the map $g \mapsto \chi \circ g$ from $Hom_R(V, R)$ to $\widehat{V}$ is an injective group homomorphism.*

Proof. If g is in the kernel of the map, then $\chi \circ g(v) = 1$ for all $v \in V$. Notice that since R is a field, the range of $g : V \to R$ is either R or $\{0\}$, since these are the only subspaces of R. But if the range of g is R, then $\chi(x) = 1$ for all $x \in R$, that is χ is the principal character; contradiction. Hence $\{0\}$ must be the range of g, i.e., g is the zero map in $\mathrm{Hom}_R(V, R)$. □

Every linear endomorphism on R is a multiplication map $\mu_r : R \to R$ given by $\mu_r(x) = rx$ for some $r \in R$. Thus $|\mathrm{Hom}_R(R, R)| = |R|$. On the other hand, using Proposition 2.11, $|R| = |\widehat{R}|$. Therefore by Lemma 3.4 we have the following.

Lemma 3.5. *Every character ψ on R can be written as $\psi = \chi \circ \mu_r$ for some $r \in R$.*

We will now translate the Hamming weight into character theoretic language. Let n_0 be the function that counts the number of zero entries of a vector in R^n, that is $n_0(x) = \#\{x_i \mid x_i = 0\}$. Then two vectors $x, y \in R^n$ have the same Hamming weight if and only if $n_0(x) = n_0(y)$. Now notice that by using Proposition 2.18 we have

$$n_0(x) = \sum_{i=1}^{n} \frac{1}{|R|} \sum_{\psi \in \widehat{R}} \psi(x_i)$$

Thus we have

Lemma 3.6. *Let $x, y \in R^n$. Then $w_H(x) = w_H(y)$ if and only if*

$$\sum_{i=1}^{n} \sum_{\psi \in \widehat{R}} \psi(x_i) = \sum_{i=1}^{n} \sum_{\psi \in \widehat{R}} \psi(y_i)$$

Now we are ready to prove the MacWilliams equivalence theorem using character theory.

Proof of Theorem 3.1, following Wood and Ward [38]. We will only prove "⇒". Let $f : \mathcal{C} \to \mathcal{C}'$ be a w_H-isometry between the $[n, k]$ codes $\mathcal{C}, \mathcal{C}'$ over R. Denote by π_i the projection of R^n onto the ith coordinate. Then every $x \in \mathcal{C}$ can be written as

$x = (\pi_1(x), \ldots, \pi_n(x))$. Similarly, $f(x) = (f_1(x), \ldots, f_n(x))$, where $f_i = \pi_i \circ f$. Since f preserves the Hamming weight, Lemma 3.6 implies

$$\sum_{i=1}^{n} \sum_{\psi \in \widehat{R}} \psi(\pi_i(x)) = \sum_{i=1}^{n} \sum_{\psi \in \widehat{R}} \psi(f_i(x)) \text{ for all } x \in \mathcal{C}.$$

By Lemma 3.5, we have

$$\sum_{i=1}^{n} \sum_{r \in R} \chi \circ \mu_r \circ \pi_i = \sum_{i=1}^{n} \sum_{r \in R} \chi \circ \mu_r \circ f_i. \tag{3.4}$$

Notice that for each i the maps $\chi \circ \mu_r \circ \pi_i$ and $\chi \circ \mu_r \circ f_i$ are characters on $\mathcal{C}$. Hence the Equation (3.4) is an equation of characters on $\mathcal{C}$. If $r = 0$ notice that $\chi \circ \mu_r \circ \pi_i$ and $\chi \circ \mu_r \circ f_i$ are principal characters for all $i = 1, \ldots, n$. Hence the case $r = 0$ can be removed from the summation to get

$$\sum_{i=1}^{n} \sum_{r \in R - \{0\}} \chi \circ \mu_r \circ \pi_i = \sum_{i=1}^{n} \sum_{r \in R - \{0\}} \chi \circ \mu_r \circ f_i. \tag{3.5}$$

Consider the character $\chi \circ \mu_1 \circ f_1$ on the right hand side, that is where $i = 1$ and $r = 1$. By Corollary 2.17, there is $j \in \{1, \ldots, n\}$ and $s \in R - \{0\}$ such that

$$\chi \circ \mu_s \circ \pi_j = \chi \circ \mu_1 \circ f_1 = \chi \circ f_1.$$

Now by Lemma 3.4

$$f_1 = \mu_s \circ \pi_j. \tag{3.6}$$

By using this result we have

$$\begin{aligned} \sum_{r \in R - \{0\}} \chi \circ \mu_r \circ f_1 &= \sum_{r \in R - \{0\}} \chi \circ \mu_r \circ \mu_s \circ \pi_j \\ &= \sum_{r \in R - \{0\}} \chi \circ \mu_{rs} \circ \pi_j \\ &= \sum_{t \in R - \{0\}} \chi \circ \mu_t \circ \pi_j. \end{aligned}$$

Therefore we can remove the summands in Equation (3.5) corresponding to $i = j$ on the left and $i = 1$ on the right, reducing the index of the outer sum by 1. Then by induction there exist $\sigma \in S_n$ and $s_i \in R - \{0\}$ such that

$$f_i = \mu_{s_i} \circ \pi_{\sigma(i)} \tag{3.7}$$

for all $i = 1, \ldots, n$. Therefore for every $x \in \mathcal{C}$ we have

$$f(x) = (s_i x_{\sigma(1)}, \ldots, s_n x_{\sigma(n)})$$

as we desired. □

3.3 General Weight Functions

It is natural to ask if the equivalence theorem for the Hamming weight holds true for general U-weights where U is any subgroup of $\mathcal{U}(R)$ (see Definition 2.3). In other words, is each w-isometry between codes in R^n a U-monomial equivalence provided that w is a U-weight? Recall from Equation (2.1) that we extend a weight w on R to the vector space R^n via $w(x) = \sum_{i=1}^{n} w(x_i)$. Unfortunately the above is not true in general. The following two examples illustrate this fact.

Example 3.7. First, let $R = \mathbb{Z}_5$ and consider the zero function $w : \mathbb{Z}_5 \to \mathbb{C}$; it defines a $\{\pm 1\}$-weight. If the equivalence theorem is true, any w-isometry $f : R \to R$ will be of the form $f(x) = ux$ where $u = \pm 1$. But this is not always the case because $f(x) = 2x$ is a w-isometry and not of that form. However, one should notice that the symmetry group of w, see Definition 2.3, is given by $\mathrm{Sym}(w) = \mathcal{U}(R)$, and the map f is indeed $\mathcal{U}(R)$-monomial. This indicates already that one should, for a given weight w, consider w as a $\mathrm{Sym}(w)$-weight.

Example 3.8. A more compelling example has been given by Wood in [44, Ex. 8.3]: choose again the field $\mathbb{Z}_5$ and consider the weight $w(i) = i$, $i = 0, \ldots, 4$. Then w is a $\{1\}$-weight and in fact $\mathrm{Sym}(w) = \{1\}$. Consider the one-dimensional codes $\mathcal{C}$ and $\mathcal{C}'$ in $\mathbb{Z}_5^2$ generated by the vectors $(1, 4)$ and $(2, 3)$, respectively. It is easy to see that the linear map $f : \mathcal{C} \to \mathcal{C}'$ defined by $f(1, 4) = (2, 3)$ is a w-isometry. However, f is not $\{1\}$-monomial. Obviously, f is the restriction of the map $x \mapsto 2x$ on $\mathbb{Z}_5^2$, which is not a w-isometry on $\mathbb{Z}_5^2$. We will come back to this example in Example 5.9 at the end of Section 5.1.

In light of these counterexamples, we may ask the following question. For what U-weights w is every w-isometry $f : \mathcal{C} \to \mathcal{C}'$ a U-monomial equivalence? Before we study this question we will first argue that the question can have an affirmative answer only in the case where $U = \mathrm{Sym}(w)$. Indeed, let $\mathcal{C} = \mathcal{C}' = R$ and let U be a proper subgroup of $\mathrm{Sym}(w)$. If $\alpha \in \mathrm{Sym}(w) \backslash U$, then the map $g : \mathcal{C} \to \mathcal{C}'$ given by $g(x) = \alpha x$ is clearly a w-isometry. But this map is not a U-monomial map: if g is a U-map then $g(x) = \beta x$ for some $\beta \in U$ and it follows that $\alpha = g(1) = \beta \in U$, which contradicts the fact that α is not in U. So from this point on we assume that $U = \mathrm{Sym}(w)$ and we phrase our question as follows.

Question 3.9. For which weights w is every w-isometry $f : \mathcal{C} \to \mathcal{C}'$ a U-monomial equivalence, where $U = \mathrm{Sym}(w)$?

Now to answer the above question, we try to mimic the line of thought of the first proof of the equivalence theorem for the Hamming weight. Let w be a weight on R, which we then extend to R^n as in Equation (2.1) via $w(x) = \sum_{i=1}^{n} w(x_i)$. Let $f : \mathcal{C} \to \mathcal{C}'$ be a w-isometry and $U = \mathrm{Sym}(w)$. Hence w is a U-weight. To show that $\mathcal{C}$ and $\mathcal{C}'$ are U-monomially equivalent, we need to show that there are generator matrices G and G' for $\mathcal{C}$ and $\mathcal{C}'$ respectively and a U-monomial matrix M such that $G' = GM$.

In the discussion prior to the proof of Theorem 3.1, we considered the one dimensional subspaces $V_1, \ldots, V_r$ with basis vectors $v_1, \ldots, v_r$. For a U-weight the analogue for these subspaces are the U-orbits of the multiplication action of U on R^k. Notice that $\{0\}$ is one orbit of this action. We will call the nonzero orbits $V_1, \ldots, V_r$ and choose representatives $v_1, \ldots, v_r$ for them. Notice that each nonzero orbit consists of $|U|$ elements and thus there are $r = \frac{|R|^k - 1}{|U|}$ orbits. In particular, $r = \frac{|R|^k - 1}{|R| - 1}$ only when $U = \mathcal{U}(R)$. Moreover, V_i are not vector spaces and, more importantly, distinct v_i and v_j may be linearly dependent.

Again, we use $n_i(G)$ to denote the number of (nonzero) columns of G that belong to V_i. To prove that $G' = GM$ for some U-monomial matrix M it is enough to show that $n_i(G) = n_i(G')$ for all $i = 1, \ldots, r$.

From here the line of reasoning is almost verbatim as in the proof of Theorem 3.1. Let G and G' be as in that proof given in Section 3.1. Since f preserves w, we have $w(xG) = w(xG')$ for any $x \in R^k$. If c_i and c'_i are the ith columns of G and G', then

$$w(xc_1, \ldots, xc_n) = w(xc'_1, \ldots, xc'_n),$$

and thus

$$\sum_{i=1}^{n} w(xc_i) = \sum_{i=1}^{n} w(xc'_i).$$

As we can see, these equations are identical to Equation (3.1). Hence following the same argument we have the matrix equation

$$A \begin{pmatrix} n_1(G) \\ n_2(G) \\ \vdots \\ n_r(G) \end{pmatrix} = A \begin{pmatrix} n_1(G') \\ n_2(G') \\ \vdots \\ n_r(G') \end{pmatrix} \tag{3.8}$$

where

$$A = \begin{pmatrix} w(v_1 \cdot v_1) & w(v_1 \cdot v_2) & \cdots & w(v_1 \cdot v_r) \\ w(v_2 \cdot v_1) & w(v_2 \cdot v_2) & \cdots & w(v_2 \cdot v_r) \\ \vdots & \vdots & & \vdots \\ w(v_r \cdot v_1) & w(v_r \cdot v_2) & \cdots & w(v_r \cdot v_r) \end{pmatrix}.$$

Observe that the matrix A does not depend on the choice of the representatives v_i for the U-orbits in R^k. It is thus an invariant of the weight w and the parameter k.

Now an answer for Question 3.9 can be formulated as follows.

Proposition 3.10. *Let w be a weight on R with $U = \mathrm{Sym}(w)$, and let $v_1, \ldots, v_r$ be representatives of the nonzero U-orbits in R^k. If $A = (w(v_i \cdot v_j)) \in \mathbb{C}^{r \times r}$ is invertible, then every w-isometry $f : \mathcal{C} \to \mathcal{C}'$ between $[n, k]$ codes $\mathcal{C}$ and $\mathcal{C}'$ is a U-monomial equivalence.*

Note that if w is a nonzero $\mathcal{U}(R)$-weight, then w is just some scaling of the Hamming weight (recall that R is a field), i.e., $w = \alpha w_H$ for some $\alpha \in \mathbb{C} \backslash \{0\}$. Therefore in this case, obviously the matrix A above is invertible.

Let $U \neq \mathcal{U}(R)$. In this case, invertibility of A is not known in general. We will briefly report on problems arising in proving this. One key ingredient for the invertibility of $(w_H(v_i \cdot v_j))$ in Lemma 3.3 is Lemma 3.2. It turns out that Lemma 3.2 holds true for any weight function w on R.

Lemma 3.11. *Let w be a weight function on R. Let W be a subspace of R^k and $v \notin W^\perp$. Then*

$$\sum_{x \in W} w(x \cdot v)$$

does not depend on the choice of $v \notin W^\perp$.

Proof. As we have seen in the proof of Lemma 3.2, the cardinality of

$$X_0(v) := \{x \in W \mid x \cdot v = 0\}$$

is independent of the choice of $v \notin W^\perp$. Consider now, for any $r \in R$, the set $X_r(v) := \{x \in W \mid x \cdot v = r\}$. Evidently, this is a translation of $X_0(v)$, that is $X_r(v) = X_0(v) + y$ for any y in $X_r(v)$. Thus the cardinality of $X_r(v)$ equals that of $X_0(v)$. Now

$$\begin{aligned}
\sum_{x \in W} w(x \cdot v) &= \sum_{r \in R} \sum_{x \in X_r(v)} w(x \cdot v) \\
&= \sum_{r \in R} |X_r(v)| w(r) \\
&= |X_0(v)| \sum_{r \in R} w(r) \qquad (\text{since } |X_r(v)| = |X_0(v)| \text{ for all } r\ ).
\end{aligned}$$

Since $|X_0(v)|$ is independent of $v \notin W^\perp$, then $\sum_{x \in W} w(x \cdot v)$ is independent of the choice of $v \notin W^\perp$ as well. □

Using Lemma 3.11, one can see as in the proof of Lemma 3.3 that if we add all rows of matrix A, the resulting vector is of the form $(\alpha, \alpha, \cdots, \alpha)$ for some non-zero α. Hence again we can obtain the vector $(1, 1, \ldots, 1)$ in the row space of A. Unfortunately, the method in that lemma does not apply when we try to obtain the vector $(1, \cdots, 1, \overset{j\text{th}}{0}, 1, \cdots, 1)$ in the row space of A. Indeed, if $U \neq \mathcal{U}(R)$, the orbit representatives $v_1, \ldots, v_r$ are not necessary pairwise linearly independent. In fact for any index j there is an index k such that $v_j = \alpha v_k$ for some $\alpha \in \mathcal{U}(R) - U$. So if we add all rows of A that are perpendicular to v_j, all these rows are perpendicular to v_k as well. Thus the resulting vector has more than one zero entry and we cannot receive $(1, \cdots, 1, \overset{j\text{th}}{0}, 1, \cdots, 1)$ in this way. Therefore, a general proof of the invertibility of A is not known.

For example it is not known whether the matrix A is invertible in the case of the Lee weight on general residue rings $\mathbb{Z}_N$. The MacWilliams equivalence theorem for the Lee weight has been established only for a few cases. Even the case $\mathbb{Z}_p$ for general prime numbers p is still unsolved. Yet, empirical evidence suggests that the matrix

is invertible for all primes p. We will discuss this in more depth in Chapter 5 after reducing the problem to cyclic modules, that is, to the case where $k = 1$.

Considering the size of matrix A, in most cases it is not practical to use this criterion to check whether the MacWilliams Equivalence Theorem is true for general U-weights. Nevertheless, we will see some applications of Proposition 3.10. In the next section, we will present a result of Goldberg that generalizes the MacWilliams equivalence theorem via this matrix A. Also, in Chapter 5 we will use Proposition 3.10 to obtain a better and more useful sufficient condition for Question 3.9.

3.4 Weight Compositions

In this section we will discuss a result of Goldberg [12] that generalizes the MacWilliams equivalence theorem in a certain direction. Fixing a subgroup U of $\mathcal{U}(R)$ we will investigate whether isomorphisms that preserve the U-orbits in R in a symmetrized manner are U-monomial maps.

Observe that the Hamming weight w_H partitions R into the two sets $P_0 := \{0\}$ and $P_1 := R\backslash\{0\}$ so that w_H is constant on each of them (with value zero and one, respectively). We call this partition the *Hamming partition* of R.

Let now $\mathcal{P} = P_0, \cdots, P_t$ be any partition on R with the property that $P_0 = \{0\}$. For $i = 0, 1 \ldots, t$ let δ_i be the indicator function for the set P_i, thus

$$\delta_i(x) := \begin{cases} 1, & \text{if } x \in P_i \\ 0, & \text{if } x \notin P_i \end{cases}.$$

Notice that all functions δ_i except δ_0 are weight functions on R. We can extend the functions δ_i to R^n by

$$\delta_i(x) = \sum_{j=1}^{n} \delta_i(x_j) = \big|\{j \mid x_j \in P_i\}\big|$$

for every $x \in R^n$. Define the *composition of* x with respect to $\mathcal{P}$ by

$$\mathrm{comp}_{\mathcal{P}}(x) = (\delta_1(x), \ldots, \delta_t(x)). \tag{3.9}$$

Thus, $\mathrm{comp}_{\mathcal{P}}(x)$ keeps track of how many entries of x are contained in each partition set. Notice that $\sum_{i=0}^{t} \delta_i(x) = n$ for all $x \in R^n$.

Definition 3.12. Let $\mathcal{P}$ be a partition of R. Let $\mathcal{C}$ be a code of length n over R. A linear map $f : \mathcal{C} \to R^n$ is called a *$\mathcal{P}$-preserving map* if $\mathrm{comp}_{\mathcal{P}}(x) = \mathrm{comp}_{\mathcal{P}}(f(x))$ for all $x \in \mathcal{C}$. If $f : \mathcal{C} \to \mathcal{C}'$ is a $\mathcal{P}$-preserving isomorphism, we say that f is a *$\mathcal{P}$-isometry.*

Using this notion, a map $f : \mathcal{C} \to \mathcal{C}'$ is a Hamming weight preserving map if and only if f preserves the Hamming partition.

The Hamming partition can obviously be realized as the orbits of the action of the group $\mathcal{U}(R)$ on R by multiplication (recall that R is a field). Goldberg [12] considered the partition $\mathcal{P}$ induced by the multiplication action of a general subgroup U of $\mathcal{U}(R)$ on R and proved an equivalence theorem for this situation. We first fix the following terminology.

Definition 3.13. Let U be a subgroup of $\mathcal{U}(R)$. The orbits of the multiplication action of U on R form a partition of R, denoted by $\mathcal{P}_U$. We will always write this partition as $\mathcal{P}_U = P_0, P_1, \ldots, P_t$ (for some t), where the set P_0 is the singleton set $\{0\}$ and P_1 is the set that contains 1, i.e., $P_1 = U$.

Note that the indicator functions $\delta_1, \ldots, \delta_t$ of the sets $P_1, \ldots, P_t$ in the partition $\mathcal{P}_U$ are U-weights. Even more, by construction $\mathrm{Sym}(\delta_i) = U$ for all i. In this regard, the $\mathcal{P}_U$-preserving maps are the maps that preserves the family $\delta_1, \ldots, \delta_t$ of U-weights.

Remark 3.14. We even have that if a linear map f preserves δ_1 then f is $\mathcal{P}_U$-preserving. To see this, let r_i be a representative of P_i for $i = 1, \ldots, t$. Then for $r \in R$ we have $r \in P_i$ if and only if $r_i^{-1} r \in U = P_1$. It follows that for $x \in R^n$ we have $\delta_i(x) = \delta_1(r_i^{-1} x)$. By linearity of f, if f preserves δ_1 then f preserves δ_i for all $i = 1, \ldots, t$. Hence f is a $\mathcal{P}_U$-preserving map.

Now we can formulate an answer to the analogue of Question 3.9 in the context of partition-preserving maps. The proof combines the ideas in [12] with our previous results.

Theorem 3.15 (Goldberg [12])**.** *Let U be a subgroup of $\mathcal{U}(R)$. If $f : \mathcal{C} \to \mathcal{C}'$ is a $\mathcal{P}_U$-isometry, then $\mathcal{C}$ and $\mathcal{C}'$ are U-monomially equivalent.*

Note that the converse is trivially true: a U-monomial map $f : \mathcal{C} \to \mathcal{C}'$ is a $\mathcal{P}_U$-isometry.

Proof. We know that f preserves the U-weight δ_1 and $\mathrm{Sym}(\delta_1) = U$. By Proposition 3.10, the proof is complete if we can show that $A = (\delta_1(v_i \cdot v_j))$ is invertible. We will show this in the next proposition. □

Proposition 3.16. *Let U be a subgroup of $\mathcal{U}(R)$ and let $V_1, \ldots, V_r$ be the nonzero orbits of the multiplication action of U on R^k. For $i = 1, \ldots, r$ let v_i be a fixed representative of V_i. Define the matrices $A = (\delta_1(v_i \cdot v_j))$ and $B = (\delta_0(v_i \cdot v_j))$ in $\mathbb{C}^{r \times r}$. Then*

$$A^{-1} = \frac{1}{q^{k-1}}(A - hB),$$

where $|R| = q$ and $|U| = h$.

Proof. We will show that $A^2 - hAB = q^{k-1} I$ by considering the (i, j) entries of A^2 and $h \cdot AB$ in the three cases: (i) the diagonal entries, (ii) when $v_i = \alpha v_j$ for some $\alpha \in \mathcal{U}(R) - U$, and (iii) when v_i and v_j are linearly independent.

Define $W(i) := \{u \in R^k \mid u \cdot v_i \in U\}$. One can view this set as the union $\bigcup_{\alpha \in U} \{u \in R^k \mid u \cdot v_i = \alpha\}$. Hence $W(i)$ is a union of h parallel affine subspaces of dimension $k - 1$. Since $P_1 = U$, the (i, j) entry of A^2 is given by

$$\begin{aligned} \sum_{t=1}^{r} \delta_1(v_i \cdot v_t)\delta_1(v_t \cdot v_j) &= \frac{1}{|U|} \sum_{u \in R^k} \delta_1(v_i \cdot u)\delta_1(u \cdot v_j) \\ &= \frac{1}{h} \big| \{u \in R^k \mid u \cdot v_i \in U \text{ and } u \cdot v_j \in U\} \big|. \end{aligned}$$

Thus $(A^2)_{ij} = \frac{1}{h} \cdot |W(i) \cap W(j)|$.

In (i) we have $(A^2)_{ii} = \frac{1}{h}.|W(i)|$. Hence $(A^2)_{ii} = q^{k-1}$. In case (ii), since $\alpha \notin U$ we cannot have $u \cdot v_i \in U$ and $u \cdot \alpha v_i \in U$ at the same time. Hence in this case $(A^2)_{ij} = 0$. For case (iii) since v_i and v_j are not parallel to each other, each affine subspace in $W(i)$ intersects with each affine subspace in $W(j)$ resulting in h^2 affine subspaces of dimension $k-2$. Therefore $(A^2)_{ij} = \frac{1}{h} \cdot h^2 q^{k-2} = hq^{k-2}$. In summary

$$(A^2)_{ij} = \begin{cases} q^{k-1}, & i = j \\ 0, & v_i = \alpha v_j \text{ for some } \alpha \notin U \\ hq^{k-2}, & v_i \text{ and } v_j \text{ are linearly independent} \end{cases}.$$

Now, the (i, j) entry of AB is

$$\sum_{t=1}^{r} \delta_1(v_i \cdot v_t)\delta_0(v_t \cdot v_j) = \frac{1}{|U|} \sum_{u \in R^k} \delta_1(v_i \cdot u)\delta_0(u \cdot v_j)$$

Therefore $(AB)_{ij} = \frac{1}{h}|W(i) \cap \langle v_j \rangle^{\perp}|$.

In case (i) and (ii) v_i and v_j are multiples of each other. Hence we cannot have $u \cdot v_j = 0$ while $u \cdot v_i$ is nonzero. Therefore in these cases $(AB)_{ij} = 0$. For case (iii) notice that $W(i) \cap \langle v_j \rangle^{\perp}$ is a union of h affine subspaces of dimension $k-2$. Hence $(AB)_{ij} = q^{k-2}$. Therefore

$$(AB)_{ij} = \begin{cases} 0, & i = j, \\ 0, & v_i = \alpha v_j \text{ for some } \alpha \notin U, \\ q^{k-2}, & v_i, v_j \text{ are linearly independent.} \end{cases}$$

It follows that $A^2 - h(AB) = q^{k-1}I$, as desired. □

Note that Theorem 3.15 implies the classical MacWilliams Equivalence case by simply choosing $U = \mathcal{U}(R)$. It is also worth pointing out the case where $U = \{1\}$. In this situation, a map $f : \mathcal{C} \to \mathcal{C}'$ is a $\mathcal{P}_U$-isometry if and only if for each $x \in \mathcal{C}$ there exists a permutation $\sigma_x \in S_n$ such that $f(x) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. Thus, f "is locally a permutation". Theorem 3.15 shows that f is indeed a global permutation, meaning that there exists a uniform permutation $\sigma \in S_n$ such that $f(x) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ for all $x \in \mathcal{C}$. We will come back to the local-global extension principle in Chapter 6, where we study codes over rings and also present further examples. At this point one may have in mind already that the linearity of f is crucial in Theorem 3.15. One can easily give two binary codes with the same Hamming weight enumerator (thus, with a Hamming weight preserving bijection between them) that are not permutation equivalent; see for instance [18], p. 20.

3.5 Reformulation as an Extension Theorem

It was Goldberg, who first recognized the resemblance between the MacWilliams equivalence theorem and the Witt extension theorem. He even named his result

(Theorem 3.15) the Witt-MacWilliams extension theorem. To see the similarities between the two results, we will formulate the Witt extension theorem and then restate Theorem 3.15 accordingly.

For the following we refer to Lang [26] Theorem 10.2 in Chapter 15 or Roman [33] Theorem 11.15.

Theorem 3.17 (Witt)**.** *Let Q be a nonsingular quadratic form on a finite-dimensional vector space V over a not necessarily finite field of characteristic $\neq 2$. Let*

$$\Omega = \Omega(V, Q) = \{M \in Aut(V, V) : Q(xM) = Q(x) \text{ for all } x \in V\}$$

be the Q-orthogonal group. If $f : W_1 \to W_2$ is a Q-isometry of subspaces W_1 and W_2 of V, then f can be extended to an element of Ω.

In Theorem 3.15, $\text{comp}_{\mathcal{P}}$ (or equivalently δ_1) plays the role of Q and the U-monomial maps (given by the matrices in $\mathcal{M}_U(n, R)$) take the place of Ω. Indeed, the theorem can obviously be reformulated as

Theorem 3.18 (Goldberg [12])**.** *If $f : \mathcal{C} \to \mathcal{C}'$ is a $\mathcal{P}_U$-isometry, then f can be extended to an element of $\mathcal{M}_U(n, R)$.*

At the end of his paper, Goldberg [12] asks the following question:

Question 3.19. For which subgroups G of $\text{GL}(n, R)$ and modules S do there exist maps $v : R^n \to S$ (taking the place of weight functions) such that

(i) v is constant on the G-orbits in R^n, and

(ii) every linear isomorphism $f : \mathcal{C} \to \mathcal{C}'$ preserving v extends to an element of G?

We will see in Chapter 6, that some of our results provide answers to this question. We give a solution for the groups $\text{GL}(n, R)$, $\Delta(n, R)$, and $\text{LT}(n, R)$ where $\Delta(n, R)$ and $\text{LT}(n, R)$ are the groups of non-singular diagonal and lower triangular matrices, respectively.

Chapter 4 Equivalence Theorem for the Hamming Weight and Compositions on Rings

Throughout this chapter let R be a finite commutative ring with identity.

We will first derive the class of rings for which we can study the equivalence theorem. These are the rings that allow a generating character, called admissible rings. This way we will be able to use character theory again in a way similar to the situation over fields. We will demonstrate this by showing the MacWilliams equivalence theorem for the Hamming weight over admissible rings, which was proven first by Wood in [43]. In the second section we will turn to isomorphisms that preserve partitions induced by the action of a multiplicative group.

4.1 MacWilliams Equivalence Theorem for Rings

In this section we would like to extend the result of Theorem 3.1 to codes over rings. For that purpose, we first investigate the possibility of applying the character theoretic proof of Section 3.2.

The key element that made the proof work is Lemma 3.4. Recall that in that lemma we showed that the map from $\mathrm{Hom}_R(V,R)$ to $\widehat{V}$ given by $g \mapsto \chi \circ g$ is injective for any non principal character χ. A closer look at the proof of Theorem 3.1 in Section 3.2 shows that we do not need that much generality. We just need a single non principal character χ that satisfies Lemma 3.4.

Lemma 3.4 is true if R is a field because for any $g \in \mathrm{Hom}_R(V,R)$ we have either $g(V) = R$ or $g(V) = 0$. If R is not a field then we do not have this property in general. If R is just a ring and V is an R-module, then $g(V)$ is an ideal in R. In order to force the map $g \mapsto \chi \circ g$ to be injective we will require that the kernel of χ does not contain any non-zero ideal. In the following proposition we show the interconnection between the proposed condition and Lemma 3.4 and Lemma 3.5.

Proposition 4.1 ([4] and [43])**.** *Let χ be a character on R (considered as additive group). Then the following are equivalent:*

(1) If I is an ideal of R and $I \subset \ker\chi := \{r \in R \mid \chi(r) = 1\}$, then $I = 0$.

(2) For each R-module V the map from $Hom_R(V,R)$ to $\widehat{V}$ given by $g \mapsto \chi \circ g$ is an injective group homomorphism.

(3) The map from $Hom_R(R,R)$ to $\widehat{R}$ given by $g \mapsto \chi \circ g$ is an injective group homomorphism.

(4) Every element ψ in $\widehat{R}$ can be written as $\psi = \chi \circ \mu_r$ for some $r \in R$.

Proof. $(1 \Rightarrow 2)$ is obvious because $g(V)$ is an ideal. $(2 \Rightarrow 3)$ obvious. $(3 \Rightarrow 4)$ follows in the same way as Lemma 3.5. $(4 \Rightarrow 1)$ Suppose $I \subset \ker\chi$. Then for any $r \in R$ we

have $1 = \chi(rI) = \chi \circ \mu_r(I)$. Since all characters on R are of the form $\chi \circ \mu_r$ for some r, we obtain $\psi(I) = 1$ for all $\psi \in \widehat{R}$. By Lemma 2.13, $I = 0$. □

Following Claasen and Goldbach [4], we give the following definition.

Definition 4.2. A character $\chi \in \widehat{R}$ is called an *admissible* character if every $\psi \in \widehat{R}$ can be written as $\chi \circ \mu_r$ for some $r \in R$. We say that R is an *admissible ring* if R has an admissible character.

Thus an admissible character on R satisfies the conditions (1)–(4) of Proposition 4.1. Sometimes admissible characters are called *generating characters* in the literature, see for instance [43], [17] and [3]. This originates from the fact that one may regard $\widehat{R}$ as an R-module in a natural way. Admissibility of R simply means that $\widehat{R}$ is a cyclic R-module generated by any admissible character.

Here are some examples of admissible rings.

Example 4.3.

1. Each field is admissible and each non principal character is admissible. This has been dealt with in Lemma 3.5.
2. $\mathbb{Z}_n$ is admissible since for every $\chi_j \in \widehat{\mathbb{Z}}_n$ we have $\chi_j = \chi_1 \circ \mu_j$ (see proof of Lemma 2.9).
3. It is easy to see that the finite direct sum $\bigoplus_{i=1}^{j} R_i$ of admissible rings $R_1, \ldots, R_j$ with admissible characters $\chi_1, \cdots, \chi_j$ is admissible with admissible character $\oplus_{i=1}^{j} \chi_i$ (see proof of Lemma 2.10).

Hirano [16] was the first to show that a finite ring R is admissible if only if R is Frobenius. For finite commutative rings, being Frobenius is equivalent to being self-injective (see [43, Theorem 1.2 and Remark 1.3]). Since Frobenius rings have been extensively studied, identifying admissible rings with Frobenius rings provides us with many additional examples of admissible rings. Besides the examples mentioned above, Frobenius rings includes the ring of $n \times n$ matrix over a Frobenius ring R, Galois rings and group rings $R[G]$ where R is Frobenius and G is a finite group (see [43]).

The following is an example of a non-admissible ring given in [4].

Example 4.4. Consider the ring $R = \mathbb{Z}_2[x, y]/(x^2, y^2, xy)$. This ring has four non-trivial ideals. They are $\{0, x\}, \{0, y\}, \{0, x+y\}$ and $\{0, x, y, x+y\}$ (the last one being non-principal). Since every element in the additive group of R is of order 2, for any $\chi \in \widehat{R}$ and $r \in R$ we have $\chi(r) = \pm 1$. Suppose on the contrary that R has an admissible character χ. Then $\chi(x) = \chi(y) = \chi(x + y) = -1$ (because otherwise $\chi(I) = 1$ for some non zero ideal I). But this is impossible since this implies that $\chi(x + y) = \chi(x)\chi(y) = 1$.

Notice that all the steps of the proof in Section 3.2 on Page 17 work flawlessly up to Equation (3.6) in the case where R is an admissible ring. In that equation we have $f_1 = \mu_s \circ \pi_j$ where $s \in R - \{0\}$. To carry out the next step of the argument, we need s to be a unit, which is not always the case if R is not a field. So we need a tool

to force s to be a unit of R. For this purpose we introduce the following concepts. We do this even for non-commutative rings because that will be needed in a later chapter.

A (potentially non-commutative) ring R is called *semilocal* if $R/\mathrm{rad}(R)$ is a left artinian ring (see for example [24] Section 20). If R is finite, then so is $R/\mathrm{rad}(R)$. Moreover every finite ring is artinian. Hence every finite ring R is semilocal.

Lemma 4.5 (Bass, [2]). *Let R be a semilocal ring, $a \in R$, and I be a left ideal of R. If $Ra + I = R$, then the coset $a + I$ contains a unit of R.*

Proof. See [24] Proposition 20.8. □

This result has the following nice consequence due to Wood [43].

Lemma 4.6 (Wood). *Let M be a left module over a finite ring R (not necessarily commutative). If $x, y \in M$ satisfy $Rx = Ry$, then $x = \alpha y$ for some unit α in R.*

Proof. Since $Rx = Ry$, there are $a, b \in R$ such that $ax = y$ and $x = by$. It follows that $(1 - ab)y = 0$. Now

$$R = Rab + R(1 - ab) \subseteq Rb + R(1 - ab).$$

Thus $R = Rb+R(1-ab)$, and by Lemma 4.5 there is a unit of the form $\alpha = b+r(1-ab)$ for some $r \in R$. It follows that

$$\alpha y = by + r(1 - ab)y = by = x.$$

□

Now we are ready to give the full statement and proof of the MacWilliams extension theorem for the Hamming weight on admissible rings.

Theorem 4.7 (Wood [43]). *Let R be admissible. Let $\mathcal{C}$ and $\mathcal{C}'$ be two codes over R. Then $\mathcal{C}$ and $\mathcal{C}'$ are w_H-isometric if and only if $\mathcal{C}$ and $\mathcal{C}'$ are monomially equivalent.*

Proof. As in the proof of Theorem 3.1 in Section 3.2 we arrive at Equation (3.5). Here we have to use an admissible character χ on R; then admissibility of the ring and Proposition 4.1 replace Lemma 3.5 and Lemma 3.4. Next we need to show that there is a unit α such that Equation (3.6) is true, that is

$$f_1 = \mu_\alpha \circ \pi_j.$$

In order to do so, we may assume that the cyclic module Rf_1 is maximal in the set $\{Rf_1, \ldots, Rf_n, R\pi_1, \ldots, R\pi_n\}$ (that is Rf_1 is not properly contained in any of these modules). Note that the situation is symmetric with respect to f_i and π_i. Now we may argue as in the proof on page 17 that $f_1 = \mu_s \circ \pi_k$ for some $s \neq 0$. It follows that $Rf_1 = R(\mu_s \circ \pi_k) \subseteq R\pi_k$. By maximality of f_1, we conclude that $Rf_1 = R\pi_k$. Now Lemma 4.6 implies $f_1 = \alpha\pi_k = \mu_\alpha \circ \pi_k$ for some unit α. The rest of the proof is identical to that of Theorem 3.1 in Section 3.2. □

We wish to remark that being admissible is equivalent to the MacWilliams equivalence theorem being true for the Hamming weight. Precisely, a finite commutative ring R is admissible if and only if every w_H-isometry between codes in R^n is a monomial equivalence; see [43], [8],[46].

4.2 $\mathcal{P}_U$-isometries are U-monomial Maps

In this section we are going to generalize the result of Goldberg in Theorem 3.15 to more general rings. Recall that the Hamming weight is a $\mathcal{U}(R)$-weight. Moreover, in the previous section we have seen that in order that the equivalence theorem works for the Hamming weight on a ring, the ring needs to be admissible. Then it would be natural to ask if Theorem 3.15 holds true for admissible rings. A positive answer was given by Wood [42]. He proved the result using the character theoretic technique that he developed with Ward in [38]; it is the same technique he used for the proof of Theorem 4.7.

We will again look at the character theoretic proof of Section 3.2. By doing so we are able to obtain a shorter proof of Theorem 3.15 for admissible rings than the one originally given by Wood. Our proof is more elementary, and we manage to avoid the averaging character argument that Wood used in his proof.

Before we formulate and prove Theorem 3.15 for admissible rings, let us first collect the concepts from Section 3.4 that carry over straightforwardly from fields to admissible rings.

Remark 4.8. First of all, for any partition $\mathcal{P}$ on a ring R we introduce the indicator functions δ_i as in Section 3.4; they in turn give rise to the composition vector $\mathrm{comp}_{\mathcal{P}}(x)$ as in (3.9). Next, the notions of $\mathcal{P}$-preserving maps and $\mathcal{P}$-isometries will be used for codes over admissible rings exactly as in Definition 3.12, and the notation $\mathcal{P}_U$ stands as in Definition 3.13 for the partition of R given by the U-orbits, where U is a subgroup of $\mathcal{U}(R)$. For U-monomial maps, matrices, and U-monomially equivalent codes we refer to the definitions in Section 2.3.

Now we can reformulate Theorem 3.15 for admissible rings. A proof will be derived further down.

Theorem 4.9 (Wood, [42])**.** *Let R be an admissible ring and U a subgroup of $\mathcal{U}(R)$. If $f : \mathcal{C} \to \mathcal{C}'$ is a $\mathcal{P}_U$-isometry, then f is a U-monomial map and thus $\mathcal{C}$ and $\mathcal{C}'$ are U-monomially equivalent.*

Again, the converse is trivially true.

Let us look at the character theoretic proof of Theorem 3.1 in Section 3.2 to get some inspiration of how to prove the above theorem. In order for $\mathcal{C}$ and $\mathcal{C}'$ to be U-monomially equivalent we want to show there is some $\sigma \in S_n$ and some $\alpha_1, \ldots, \alpha_n$ such that for all $x \in \mathcal{C}$

$$f(x) = (\alpha_1 x_{\sigma(1)}, \ldots, \alpha_n x_{\sigma(n)}).$$

So now if we look at proof on page 17, we are hoping to have an equation as Equation (3.5). But we need the inner summation to run through all elements of U, that is we

want to have

$$\sum_{i=1}^{n}\sum_{r\in U}\chi\circ\mu_r\circ\pi_i=\sum_{i=1}^{n}\sum_{r\in U}\chi\circ\mu_r\circ f_i. \tag{4.1}$$

Once we have this equation, all the arguments on page 17 carry over since Lemma 3.4 is replaced by Definition 4.2 if we choose χ to be an admissible character. Then we have Equation (3.7)

$$f(x)=(s_1x_{\sigma(1)},\ldots,s_nx_{\sigma(n)}),$$

for some $\sigma\in S_n$ and $s_1,\ldots,s_n\in U$.

Therefore the proof of Theorem 4.9 is complete if we can show that Equation (4.1) is true. We are going to establish that using the following argument.

Proof of Theorem 4.9. Recall that $\mathcal{P}_U=P_0,P_1,\ldots,P_t$ is the partition induced by the (multiplication) action of U on R. We write $x\sim_U y$ if $x=\alpha y$ for some $\alpha\in U$. In this notation, $x,y\in P_i$ for some i if and only if $x\sim_U y$. As before we use the notation $\pi_i:R^n\to R$ for the projection map onto the ith component and $f_i:=\pi_i\circ f$.

Now since f is a $\mathrm{comp}_{\mathcal{P}_U}$-isometry, for every x there is a σ (depending on x) such that $x_i\sim_U f_{\sigma(i)}(x)$ for all $i=1,\ldots,n$. It follows that

$$\sum_{\alpha\in U}\chi(\alpha x_i)=\sum_{\alpha\in U}\chi(\alpha f_{\sigma(i)}(x))$$

for all $i=1,\ldots,n$. Adding the above identities for all $i=1,\ldots,n$, we have

$$\begin{aligned}\sum_{i=1}^{n}\sum_{\alpha\in U}\chi(\alpha x_i)&=\sum_{i=1}^{n}\sum_{\alpha\in U}\chi(\alpha f_{\sigma(i)}(x))\\&=\sum_{i=1}^{n}\sum_{\alpha\in U}\chi(\alpha f_i(x)),\end{aligned} \tag{4.2}$$

where the second identity is true since $\{\sigma(1),\ldots,\sigma(n)\}=\{1,\ldots,n\}$. Writing αx_i as $\mu_\alpha\circ\pi_i(x)$ and $\alpha f_i(x)$ as $\mu_\alpha\circ f_i(x)$, we have

$$\sum_{i=1}^{n}\sum_{\alpha\in U}\chi\circ\mu_\alpha\circ\pi_i(x)=\sum_{i=1}^{n}\sum_{\alpha\in U}\chi\circ\mu_\alpha\circ f_i(x).$$

Since this identity is independent of σ, it holds true for all $x\in\mathcal{C}$. Therefore we have Equation (4.1) as we desired. □

Example 4.10. Recall the Lee weight on $\mathbb{Z}_N$ from Definition 2.4. Its symmetry group is given by $U=\{1,-1\}$. Moreover, two elements have the same Lee weight if and only if they are in the same U-orbit. Theorem 4.9 tells us that every isomorphism between codes over $\mathbb{Z}_N$ that preserves the number of entries in each codeword with the same Lee weight is a U-monomial map. This fact is well-known as the MacWilliams equivalence theorem for the symmetrized Lee weight composition; see also [42].

Chapter 5 Equivalence Theorem for General Weights On Rings

In this chapter we will generalize the equivalence theorem for the Hamming weight in Chapter 4 to more general weight functions on admissible rings. By reducing to the case of cyclic modules we reprove a result of Wood [44] which gives a criterion for a weight function w to satisfy the equivalence theorem. This condition is an improvement of Proposition 3.10 because, firstly, the new condition involves a matrix A whose size is much smaller than in Proposition 3.10 and, secondly, the condition applies to isometries between codes of any size. Specializing the ring to a field, we observe that the A matrix is a circulant matrix – up to row and column reordering. This additional structure allows us to prove a new result: the Lee weight on any field $\mathbb{Z}_N$, where $N = 4p + 1$ and N and p are both prime, satisfies the equivalence theorem. We will also recover a result of Wood's which shows that the Lee weight satisfies the equivalence theorem on fields $\mathbb{Z}_N$, when $N = 2p + 1$ and N and p are both prime.

We will also show that the same reduction technique yields a more direct proof of the fact that the homogeneous weight satisfies the equivalence theorem which was originally proven by Greferath and Schmidt [13].

Throughout this chapter let R be a finite commutative admissible ring.

5.1 Reduction to Cyclic Modules

In Proposition 3.10 we gave a sufficient criterion for a w-isometry on a field R to be a $\mathrm{Sym}(w)$-monomial map. In this section we will present a more powerful criterion by showing that we can reduce the situation to cyclic modules. Let us first reformulate Question 3.9 for admissible rings.

Question 5.1. Let R be admissible and let $\mathcal{C}$ and $\mathcal{C}'$ be two codes in R^n. For which weights w is every w-isometry $f : \mathcal{C} \to \mathcal{C}'$ a $\mathrm{Sym}(w)$-monomial equivalence?

In Section 4.2 we showed that if $f : \mathcal{C} \to \mathcal{C}'$ is a $\mathcal{P}_U$-isometry, then f is a U-monomial equivalence. For a U-weight w, the two notions w-isometry and $\mathcal{P}_U$-isometry both involve the subgroup U, yet we have not clarified the connection between these two maps.

Let $f : \mathcal{C} \to \mathcal{C}'$ be a linear isomorphism and let $U = \mathrm{Sym}(w)$. Consider the following types of isomorphisms between $\mathcal{C}$ and $\mathcal{C}'$:

(1) f is a U-monomial map.

(2) f is a $\mathcal{P}_U$-isometry.

(3) f is a w-isometry.

By Theorem 4.9 property (1) is equivalent to (2). It is also clear that (1) $\Rightarrow$ (3). Answering Question 5.1 is the same as finding a sufficient condition for the implication (3) $\Rightarrow$ (1). Since (1) $\Leftrightarrow$ (2), it is enough to find a sufficient condition for the implication (3) $\Rightarrow$ (2). Before we do so we need to following related concept.

Definition 5.2. Let $\mathcal{C}$ be a code in R^n and let U be a subgroup of $\mathcal{U}(R)$. A map $f : \mathcal{C} \to R^n$ is called a *local U-monomial* map if for every $x \in \mathcal{C}$ there is a U-monomial matrix M (depending on x) such that $f(x) = xM$.

Notice that, even without using Theorem 4.9, it is easy to see that being a $\mathcal{P}_U$-isometry is equivalent to being a local U-monomial isomorphism. Now we claim that in order to have (3) $\Rightarrow$ (1) it is enough to consider the case where f is an isometry between cyclic modules.

Proposition 5.3. *If every w-isometry $f' : \mathcal{D} \to \mathcal{D}'$ of cyclic modules $\mathcal{D}$ and $\mathcal{D}'$ is a U-monomial map, then every w-isometry $f : \mathcal{C} \to \mathcal{C}'$ of any codes $\mathcal{C}, \mathcal{C}'$ is a U-monomial map.*

Proof. Let x be a fixed element in $\mathcal{C}$. Notice that f is also a w-isometry from the cyclic module Rx to $Rf(x)$. By the hypothesis, f is a U-monomial map on Rx. Then $f(x) = xM$ for some U-monomial matrix M that depends on x. But this means that f is a local U-monomial map, and hence a $\mathcal{P}_U$-isometry. Now by Theorem 4.9, f is a U-monomial map. □

Notice that Proposition 3.10 remains valid for rings. In the ring case codes $\mathcal{C}$ and $\mathcal{C}'$ that have generator matrices of size $k \times n$ replace the $[n, k]$ codes $\mathcal{C}$ and $\mathcal{C}'$. The size of the matrix $A = (w(v_i \cdot v_j))$ depends on the number of non-zero of U-multiplication orbits in R^k. By Proposition 5.3 it is enough to consider the case where $k = 1$. Therefore we arrive at the following theorem which answers Question 5.1.

Theorem 5.4 ([44])**.** *Let w be a U-weight on R and let $a_1, \ldots, a_r$ be representatives of the nonzero U-orbits in R. If $A = (w(a_i \cdot a_j)) \in \mathbb{C}^{r \times r}$ is invertible, then every w-isometry $f : \mathcal{C} \to \mathcal{C}'$ between two codes $\mathcal{C}$ and $\mathcal{C}'$ is a U-monomial equivalence.*

The above criterion first appeared in the paper [44] of Wood ; however, he did not make the reduction to cyclic modules explicit. One should note that if U is not the symmetry group of w, then A is not invertible. Indeed, in this case we may pick the representatives $a_1, \ldots, a_r$ of the nonzero U-orbits in such a way that $a_1 = 1$ and $a_2 \in \mathrm{Sym}(w) \backslash U$. But then the first two rows of A are identical. As a consequence, the criterion is interesting only for $U = \mathrm{Sym}(w)$.

We remark that compared to the size of A in Proposition 3.10 the matrix A in the above theorem is significantly smaller. Even more, it does not depend on the size of generator matrices for $\mathcal{C}$ and $\mathcal{C}'$ and therefore provides a sufficient criterion for codes of all sizes.

We give the following example of how to apply the above theorem.

Example 5.5. (1) Let w_H be the Hamming weight on a finite field $\mathbb{F}$. Clearly w_H is a $\mathcal{U}(\mathbb{F})$-weight. There is only one non-zero $\mathcal{U}(\mathbb{F})$-orbit of $\mathbb{F}$ namely $\mathbb{F}\backslash\{0\}$. Take 1 as the representative of this orbit. The 1×1 matrix $A = (1)$ is obviously invertible. Hence by Theorem 5.4, every w_H-isometry between codes in $\mathbb{F}^n$ is a U-monomial map. One should notice the difference to the criterion via the matrix in Equation (3.1) used in Theorem 3.1. If $\mathbb{F} = q$, then there are $\frac{q^k-1}{q-1}$ non-zero orbits in $\mathbb{F}^k$, and this is the size of the A matrix in (3.1).

(2) Let w_L be the Lee weight on $\mathbb{Z}_4$ (see Definition 2.4). Thus $w_L(1) = w_L(3) = 1$ and $w_L(2) = 2$, and w_L is a $\{\pm 1\}$-weight. The non-zero $\{\pm 1\}$-orbits are $\{1, 3\}$ and $\{2\}$. Take 1 and 2 respectively as the representative of these orbits. Then we have

$$A = \begin{pmatrix} w_L(1 \cdot 1) & w_L(1 \cdot 2) \\ w_L(2 \cdot 1) & w_L(2 \cdot 2) \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}.$$

Since $\det(A) \neq 0$, every w_L-isometry between codes in $\mathbb{Z}_4^n$ is a $\{\pm 1\}$-monomial map.

We will see more applications of Theorem 5.4 in the next sections. At this point we want to deal with the natural question whether the converse of Theorem 5.4 also true: if the matrix A corresponding to a U-weight w on R is not invertible, is it then true that we do not have the equivalence theorem for the weight w? We will show in the next theorem that if w takes only rational values, then this is indeed the case.

Theorem 5.6. *Let w be a U-weight with rational values on a finite admissible ring R. Let $A = w(a_i \cdot a_j)$ be the matrix as in Theorem 5.4. If A is not invertible, then there exist two one-dimensional codes $\mathcal{C}$ and $\mathcal{C}'$ and a w-isometry $f : \mathcal{C} \to \mathcal{C}'$ which is not a U-monomial map.*

Proof. Notice that $A \in \mathbb{Q}^{r \times r}$ for some r. If A is not invertible, then there exists a non-zero column vector $q = (q_1\, q_2\, \cdots\, q_r)^T \in \mathbb{Q}^r$ such that $Aq = 0$. By multiplying q with a suitable integer α we can make all components of αq to be integers. Hence without loss of generality we can assume that q is a column vector in $\mathbb{Z}^r$. Since $Aq = 0$, we have for every $i = 1, \ldots, r$

$$\sum_{j=1}^{r} w(a_i a_j) q_j = 0. \tag{5.1}$$

For each $i = 1, \ldots, r$ define two constant vectors $x^{(i)} = (\underbrace{\alpha_i, \ldots, \alpha_i}_{|q_i|})$ and $y^{(i)} = (\underbrace{\beta_i, \ldots, \beta_i}_{|q_i|})$ where α_i and β_i are defined as follows

$$\alpha_i = \begin{cases} a_i & \text{if } q_i > 0 \\ 0 & \text{if } q_i \leq 0 \end{cases} \qquad \beta_i = \begin{cases} a_i & \text{if } q_i < 0 \\ 0 & \text{if } q_i \geq 0 \end{cases}.$$

Now let $x = (1, x^{(1)}, \ldots, x^{(r)})$ (respectively $y = (1, y^{(1)}, \ldots, y^{(r)})$) be the vector that is obtained by concatenating 1 and $x^{(i)}$ (respectively 1 and $y^{(i)}$) for $i = 1, \ldots, r$. Then $x, y \in R^N$ where $N = 1 + \sum_{i=1}^{r} |q_i|$. Consider the cyclic modules Rx and Ry and define a map $f : Rx \to Ry$ by $f(\gamma x) = \gamma y$ for all $\gamma \in R$. The first entry, 1, of x and y ensures that both Rx and Ry are one-dimensional free submodules of R^N and, as a consequence, the map f is clearly a well-defined isomorphism.

We want to show that f is a w-isometry. Let $\gamma \in R$. Then $\gamma \sim_U a_i$ for some i. It follows that $w(\gamma x) = w(a_i x)$ and $w(\gamma y) = w(a_i y)$. By definition of $x^{(j)}$ and $y^{(j)}$ we have

$$\begin{aligned} w(a_i x^{(j)}) - w(a_i y^{(j)}) &= \begin{cases} w(a_i a_j)|q_j| - 0 & \text{if } q_j > 0 \\ 0 & \text{if } q_j = 0 \\ 0 - w(a_i a_j)|q_j| & \text{if } q_j < 0 \end{cases} \\ &= w(a_i a_j) q_j \end{aligned}$$

It follows that

$$\begin{aligned} w(\gamma x) - w(\gamma y) &= w(a_i x) - w(a_i y) \\ &= \sum_{j=1}^{r} w(a_i x^{(j)}) - w(a_i y^{(j)}) \\ &= \sum_{j=1}^{r} w(a_i a_j) q_j \\ &= 0 \quad \text{(by Equation (5.1)).} \end{aligned}$$

Therefore f is a w-preserving map.

We have $f(x) = y$. But, by definition of x and y, for any non-zero entry a_s in x and a_t in y the elements a_s and a_t belong to different U-orbits. Therefore f cannot be a U-monomial map. □

Remark 5.7. One should notice that if one allows non-rational weights, then it is possible for A to be singular and yet have no nonzero rational vectors in its kernel (e.g., if the values of the weight are linearly independent over $\mathbb{Q}$). In this situation, the condition characterizing when the MacWilliams equivalence theorem is true is not the invertibility of A, but simply $\ker A \cap \mathbb{Q}^r = \{0\}$.

We want to illustrate Theorem 5.6 with an example that we have encountered before. Before doing so, we coin the following notion.

Definition 5.8. Let w be a weight on R. We say that w satisfies the equivalence theorem if every w-isometry $f : \mathcal{C} \to \mathcal{C}'$ is a $\mathrm{Sym}(w)$-monomial map.

Example 5.9. Consider the weight w on $\mathbb{Z}_5$ in Example 3.8, defined by $w(i) = i$ for all $i = 0, 1, \ldots, 4$. We will use Theorem 5.6 to show that w does not satisfy the

equivalence theorem. The matrix A corresponds to this weight is

$$A = \begin{pmatrix} w(1\cdot 1) & w(1\cdot 2) & w(1\cdot 3) & w(1\cdot 4) \\ w(2\cdot 1) & w(2\cdot 2) & w(2\cdot 3) & w(2\cdot 4) \\ w(3\cdot 1) & w(3\cdot 2) & w(3\cdot 3) & w(3\cdot 4) \\ w(4\cdot 1) & w(4\cdot 2) & w(4\cdot 3) & w(4\cdot 4) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

One can check that $\det(A) = 0$. Hence A is not invertible over $\mathbb{Q}$ and by Theorem 5.6 the weight w does not satisfy the equivalence theorem.

Let us apply the proof of Theorem 5.6 to construct two codes $\mathcal{C}$ and $\mathcal{C}'$ and an isometry $f : \mathcal{C} \to \mathcal{C}'$ that violates the equivalence theorem. Notice that $(1, -1, -1, 1)^T$ is in the kernel of A. According to the construction, we obtain $x = (1, 1, 0, 0, 4)$ and $y = (1, 0, 2, 3, 0)$. To have shorter codes we may remove any common entry in x and y. By doing so we obtain the shorter codes generated by $x' = (1, 4)$ and $y' = (2, 3)$, and by construction the w-isometry between $\langle x' \rangle$ and $\langle y' \rangle$ is the map f sending $\gamma(1, 4)$ to $\gamma(2, 3)$ for every $\gamma \in \mathbb{Z}_5$. But this is exactly the example given by Wood that we have seen in Example 3.8.

Remark 5.10. The proof of Theorem 5.6 can be adapted to show that also the invertibility of the bigger matrix $A = (w(v_i \cdot v_j))$ in Proposition 3.10 is necessary for the MacWilliams equivalence theorem to be true over admissible rings R (and whenever the weight has rational values). Remember that in this case the vectors $v_i \in R^k$ are representatives of the nonzero U-orbits in R^k, where again $U = \mathrm{Sym}(w)$. If A is not invertible then the above proof has to be modified by replacing $a_i \in R$ by $v_i \in R^k$. This way, we obtain $x^{(i)}$, $y^{(i)} \in R^{k \times |q_i|}$. Instead of appending an entry 1, we now have to add the $k \times k$-identity matrix. This way one can construct two generator matrices G, $G' \in R^{k \times N}$, where $N = k + \sum_{i=1}^{r} |q_i|$, in a similar fashion as we constructed x and y in the proof of Theorem 5.6. Then G and G' generate free modules of dimension k, and the map f defined by $f(xG) = xG'$ is a w-isometry but not a U-monomial map.

Remark 5.10 has the following interesting consequence.

Theorem 5.11. *Let $w : R \to \mathbb{Q}$ be a weight function and $U = \mathrm{Sym}(w)$. Let $a_1, \ldots, a_s$ be representatives of the nonzero U-orbits in R and let $v_1, \ldots, v_r$ be representatives of the nonzero U-orbits in R^k. Then $A := (w(a_i \cdot a_j)) \in \mathbb{Q}^{s \times s}$ is invertible if and only if $A' := (w(v_i \cdot v_j)) \in \mathbb{Q}^{r \times r}$ is invertible.*

Proof. If A is invertible, then the invertibility of A' follows from Theorem 5.4 and Remark 5.10. If A' is invertible, then the equivalence theorem is true for maps between codes that can be generated with k generators; see Proposition 3.10, which remains true for admissible rings. But then it is certainly also true for cyclic modules (add $k - 1$ zero codewords as generators) and thus the invertibility of A follows from Theorem 5.6. □

It is not clear at this point how one could derive this result by purely matrix theoretical arguments. The relationship between the matrices $(w(a_i \cdot a_j)) \in \mathbb{Q}^{s \times s}$ and $(w(v_i \cdot v_j)) \in \mathbb{Q}^{r \times r}$ is not trivial and cannot immediately be exploited.

5.2 Homogeneous Weights

In this section we will see another application of Proposition 5.3 and show that the homogeneous weight satisfies the equivalence theorem. Homogenous weights were first introduced by Constantinescu and Heise [6] on $\mathbb{Z}_N$ as a generalization of Lee weight on $\mathbb{Z}_4$ having a certain homogeneity properties. Thereafter, several others generalized this concept and defined homogenous weights on any finite ring and even on modules (see [13], [31]). This has led to the following definition. We recall that R is always a finite commutative admissible ring.

Definition 5.12. A weight w on R is called *homogeneous*, if $w(0) = 0$ and the following is true:

(H1) If $Rx = Ry$ then $w(x) = w(y)$ for all $x, y \in R$.

(H2) There exist a real number $\gamma \geq 0$ such that

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

In [13, Theorem 1.3] the authors show the existence and the uniqueness (up to a constant factor) of homogeneous weights with the aid of the Möbius function on the poset of principal ideals. Notice that the symmetry group of any homogeneous weight is $\mathcal{U}(R)$.

If R is not a field, R contains a zero divisor.In this case the Hamming weight on R is not homogeneous. Indeed, if $x \in R\backslash\{0\}$, then $\sum_{y \in Rx} w_H(x) = |Rx| - 1 = \frac{|Rx|-1}{|Rx|}|Rx|$. Thus the constant γ has to be $\frac{|Rx|-1}{|Rx|}$, but this is not independent of x if R is not a field (take x a unit and x a zero divisor). However, the Hamming weight is certainly homogeneous on a field R, and so is the Lee weight on $\mathbb{Z}_4$; see Example 5.13 below. Therefore, the homogeneous weight arises as a generalization of both the Hamming weight on fields and the Lee weight on $\mathbb{Z}_4$.

Example 5.13. Let us consider the ring $R := \mathbb{Z}_{p^r}$, where p is a prime number. Define

$$w(a) = \begin{cases} 0, & \text{if } a = 0, \\ p, & \text{if } a \in Rp^{r-1}\backslash\{0\}, \\ p-1, & \text{if } a \notin Rp^{r-1}. \end{cases}$$

It is straightforward to check that w is a homogeneous weight with $\gamma = p - 1$. In particular, on $\mathbb{Z}_4$ we obtain $w(0) = 0$, $w(1) = w(3) = 1$, $w(2) = 2$, which coincides with the Lee weight given in Definition 2.4. On the other hand, for any other residue ring $\mathbb{Z}_N$, where $N > 4$, the Lee weight differs from the homogeneous weight because for the latter all units have the same weight (see Definition 5.12(H1)), while this is not the case for the Lee weight if $N > 4$. One may also observe that on $\mathbb{Z}_3$ the Hamming, Lee and the above homogeneous weight coincide, while on fields $\mathbb{Z}_p$ the above homogeneous weight is exactly the Hamming weight.

The following two results are due to Greferath and Schmidt [13].

Proposition 5.14. *Let w_{hom} be a homogeneous weight on R with constant γ as in Definition 5.12(H2). Then we have*

(H2') $\sum_{y\in I} w_{\mathrm{hom}}(y) = \gamma|I|$ *for all nonzero ideals I in R.*

Proof. See [13, Theorem 1.3, Corollary 1.6]. □

Lemma 5.15. *Let w_{hom} be a homogeneous weight on R with constant γ and consider its extension to R^n as in (2.1). Let π_i denote the projection of R^n onto its ith coordinate. Then for every code $\mathcal{C}$ we have*

$$\sum_{x\in\mathcal{C}} w_{\mathrm{hom}}(x) = |\mathcal{C}| \cdot \gamma|\{i \mid \pi_i(\mathcal{C}) \neq 0\}|.$$

Proof. The linear map $\pi_i : \mathcal{C} \to \pi_i(\mathcal{C})$ is onto, and by the isomorphism theorem we have $|\mathcal{C}|/|\mathcal{C} \cap \ker \pi_i| = |\pi_i(C)|$. Note that $\pi_i(\mathcal{C})$ is an ideal in R. If $\pi_i(C) \neq 0$, then by Lemma 5.14 we have

$$\gamma|\mathcal{C}| = |\mathcal{C} \cap \ker \pi_i| \cdot \gamma|\pi_i(C)| = |\mathcal{C} \cap \ker \pi_i| \cdot \sum_{r\in\pi_i(\mathcal{C})} w_{\mathrm{hom}}(r). \tag{5.2}$$

If $\pi_i(x) = r$ for some $x \in \mathcal{C}$, then $\pi_i(x + y) = r$ for every $y \in \mathcal{C} \cap \ker \pi_i$. Hence r has exactly $|\mathcal{C} \cap \ker \pi_i|$ preimages in $\mathcal{C}$. It follows that

$$\begin{aligned}\sum_{x\in\mathcal{C}} w_{\mathrm{hom}}(x) &= \sum_{i=1}^{n} \sum_{x\in\mathcal{C}} w_{\mathrm{hom}}(\pi_i(x)) \\ &= \sum_{i=1}^{n} |\mathcal{C} \cap \ker \pi_i| \sum_{r\in\pi_i(\mathcal{C})} w_{\mathrm{hom}}(r) \\ &= |\{i \mid \pi_i(C) \neq 0\}| \cdot \gamma|\mathcal{C}|.\end{aligned}$$

□

The last lemma in combination with Proposition 5.3 allows us to derive the MacWilliams equivalence theorem for the homogeneous weight. This result has been shown before in [13, Theorem 2.5], but with different arguments and not via the reduction to cyclic modules.

Fix $x \neq 0 \in \mathcal{C}$. Applying Lemma 5.15 to the code generated by x we obtain

$$\sum_{y\in Rx} w_{\mathrm{hom}}(y) = |\{i \mid \pi_i(Rx) \neq 0\}| \cdot \gamma|Rx|.$$

But since $\pi_i(Rx) = 0$ if and only if $x_i = 0$, the cardinality $|\{i \mid \pi_i(Rx) \neq 0\}|$ is exactly the Hamming weight of x, i.e., $w_H(x)$. Therefore we have a direct relationship between the homogeneous weight and the Hamming weight given by

$$\gamma|Rx| \cdot w_H(x) = \sum_{y\in Rx} w_{\mathrm{hom}}(y).$$

If $\gamma > 0$, then

$$w_H(x) = \frac{1}{\gamma|Rx|} \sum_{y \in Rx} w_{\hom}(y).$$

Now we are ready to provide an alternative proof of the equivalence theorem for homogenous weights.

Theorem 5.16 ([13]). *Let $w_{\hom}$ be a homogeneous weight on R with $\gamma > 0$. Then $w_{\hom}$ satisfies the equivalence theorem. That is, every $w_{\hom}$-isometry between codes in R^n is a $\mathcal{U}(R)$-monomial map.*
As a consequence, an isomorphism between codes is a $w_{\hom}$-isometry if and only if it is a Hamming isometry.

Proof. Recall that $\mathrm{Sym}(w_{\hom}) = \mathcal{U}(R)$. In view of Proposition 5.3, it is enough to show that if $f : \mathcal{D} \to \mathcal{D}'$ is a $w_{\hom}$-isometry between two cyclic modules, then f is a $\mathcal{U}(R)$-monomial map. We can write $\mathcal{D} = Rx$ and $\mathcal{D}' = Rf(x)$ for some nonzero $x \in \mathcal{D}$. Since the Hamming weight satisfies the equivalence theorem, it is enough to show that f is a w_H-isometry on $\mathcal{D}$. For every $z \neq 0 \in \mathcal{D}$ the restriction of f to Rz gives a $w_{\hom}$-isometry between Rz and $Rf(z)$. Then clearly $|Rz| = |Rf(z)|$ and $w_{\hom}(\alpha z) = w_{\hom}(f(\alpha z)) = w_{\hom}(\alpha f(z))$ for every $\alpha \in R$. It follows that

$$w_H(z) = \frac{1}{\gamma|Rz|} \sum_{y \in Rz} w_{\hom}(y) = \frac{1}{\gamma|Rf(z)|} \sum_{y \in Rf(z)} w_{\hom}(y) = w_H(f(z)).$$

Therefore f is a w_H-isometry and the conclusion follows from the MacWilliams equivalence theorem 4.7 for the Hamming weight on R^n. This also shows the consequence. □

5.3 The Structure of A and Circulant Matrices

In this section we will investigate the structure of the matrix A in Theorem 5.4 for the following two case: (1) w is a $\mathcal{U}(R)$-weight on a chain ring R and (2) w is a U-weight on a finite field, where U is any multiplicative group. We will start with the definition of chain rings and some properties.

Definition 5.17. Let R be a finite commutative ring. We say that R is a *finite chain ring* if its lattice of ideals forms a chain with respect to inclusion.

The following proposition gives several characterizations of finite chain rings. Let $\mathrm{Rad}R$ denote the radical of R, that is, $\mathrm{Rad}R$ is the intersection of the maximal ideals of R,

Proposition 5.18. *Let R be a finite commutative ring and $N = \mathrm{Rad}R \neq 0$. Then the following are equivalent.*

(1) R is a chain ring;

(2) the principal ideals of R form a chain;

(3) R is a local ring, and $N = R\theta$ for some (any) θ in N which is not in N^2.

Moreover, if R satisfies the above conditions, then every proper ideal has the form $N^i = R\theta^i$ for some positive integer i.

Proof. See [5, Lemma 1] □

Examples of finite chain rings include finite fields, the rings $\mathbb{Z}_{p^r}$ (where p is prime), and Galois rings.

Here are some basic properties of chain rings which are not hard to prove. The reader interested in the proof may consult [44].

Proposition 5.19. *Let R be a chain ring with $N = R\theta$ being the unique maximal ideal in R. Then we have the following:*

(1) There is a smallest positive integer s for which $N^s = 0$. In this case we call s the nilpotency index of R.

(2) R is admissible.

(3) The nonzero $\mathcal{U}(R)$-orbits in R are given by $\mathcal{O}_{\theta^i} = \{\alpha\theta^i \mid \alpha \in \mathcal{U}(R)\}$ for $i = 0, \ldots, s-1$.

Let now R be as in Proposition 5.19 and let w be a weight on R with $\mathrm{Sym}(w) = \mathcal{U}(R)$. Choose the elements $1, \theta, \theta^2, \ldots, \theta^{s-1}$ as the representatives of the $\mathcal{U}(R)$-orbits. Then the weight matrix A as in Theorem 5.4 corresponding to w is given by $A = w(\theta^{i-1} \cdot \theta^{j-1})$. Using the fact that $\theta^i = 0$ for all $i \geq s$, the entries of A are as in the inner part of the following table.

	1	θ	θ^2	$\cdots$	θ^{s-2}	θ^{s-1}
1	$w(1)$	$w(\theta)$	$w(\theta^2)$	$\cdots$	$w(\theta^{s-2})$	$w(\theta^{s-1})$
θ	$w(\theta)$	$w(\theta^2)$	$w(\theta^3)$	$\cdots$	$w(\theta^{s-1})$	0
θ^2	$w(\theta^2)$	$w(\theta^3)$	$\cdots$	$\iddots$	0	0
$\vdots$	$\vdots$	$\vdots$	$\iddots$		$\vdots$	$\vdots$
θ^{s-2}	$w(\theta^{s-2})$	$w(\theta^{s-1})$	0	$\cdots$	0	0
θ^{s-1}	$w(\theta^{s-1})$	0	0	$\cdots$	0	0

It is easy to see that if $w(\theta^{s-1}) \neq 0$, then $\det A \neq 0$. Thus with the aid of Theorem 5.4 we arrive at the following theorem.

Theorem 5.20. *Let w be a weight on the finite commutative chain ring R with $\mathrm{Sym}(w) = \mathcal{U}(R)$ and such that $w(\theta^{s-1}) \neq 0$. Then w satisfies the equivalence theorem.*

The above theorem is a special case of a result by Wood [44, Theorem 16]. For his more general result, Wood considered a weight with symmetry group U which is not necessarily equal to $\mathcal{U}(R)$. He showed if $\sum_{a \in \mathcal{O}_{\theta^{s-1}}} w(a) \neq 0$, then every w-isometry $f : \mathcal{C} \to \mathcal{C}'$ extends to a $\mathcal{U}(R)$-monomial map. We need to emphasize here that his proof does not guarantee that f is a U-monomial map.

Now, we turn our focus to finite fields $\mathbb{F}_q$ and investigate the structure of the matrix A from Theorem 5.4. Recall that the non zero elements $\mathbb{F}_q^*$, the units in $\mathbb{F}_q$, form a cyclic group. Let w be a U-weight on $\mathbb{F}_q$, where U is any subgroup of $\mathbb{F}_q^*$. The U-orbits are the elements of the quotient group $\mathbb{F}_q^*/U$, which has order $s := \frac{q-1}{|U|}$. Notice that the quotient group $\mathbb{F}_q^*/U$ is also cyclic.

Let β be an element of $\mathbb{F}_q$ such that βU is a generator of the cyclic group $\mathbb{F}_q^*/U$. Relabel the partition $\mathcal{P}$ formed by the U-orbits as follows: $P_0 = \{0\}$ and $P_j = \beta^{j-1}U$ for $j = 1, \ldots, s$. In particular, for every $j = 1, \ldots, s$ we can take β^{j-1} as a representative of P_j. It follows that the matrix A in Theorem 5.4 is given by $A = (w(\beta^{i-1} \cdot \beta^{j-1})) = (w(\beta^{i+j-2}))$. Since the invertibility of A is invariant under row operation, we may reorder the rows of A as follows:

	1	β	β^2	$\cdots$	β^{s-2}	β^{s-1}
1	$w(1)$	$w(\beta)$	$w(\beta^2)$	$\cdots$	$w(\beta^{s-2})$	$w(\beta^{s-1})$
β^{s-1}	$w(\beta^{s-1})$	$w(1)$	$w(\beta)$	$\cdots$	$w(\beta^{s-3})$	$w(\beta^{s-2})$
β^{s-2}	$w(\beta^{s-2})$	$w(\beta^{s-1})$	$w(1)$	$\cdots$	$w(\beta^{s-4})$	$w(\beta^{s-3})$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
β^2	$w(\beta^2)$	$w(\beta^3)$	$w(\beta^4)$	$\cdots$	$w(1)$	$w(\beta)$
β	$w(\beta)$	$w(\beta^2)$	$w(\beta^3)$	$\cdots$	$w(\beta^{s-1})$	$w(1)$

(5.3)

Here the first column gives the new labels for the rows of A and the entries in the inner table are the entries of the reordered matrix A.

As one can see, the matrix A now has the special structure that each row is a cyclic shift of the row above it. This is called a circulant matrix. We give the precise definition and discuss some properties.

Definition 5.21. A complex *circulant* matrix is a matrix of the form

$$C := \begin{pmatrix} c_0 & c_1 & \cdots & c_{s-1} \\ c_{s-1} & c_0 & \cdots & c_{s-2} \\ \vdots & \vdots & & \vdots \\ c_1 & c_2 & \cdots & c_0 \end{pmatrix} \in \mathbb{C}^{s \times s}.$$

Thus each row is obtained from the previous row by a cyclic shift to the right. For abbreviation, we write the above circulant matrix as $C := \mathrm{Circ}(c_0, c_1, \ldots, c_{n-1})$, where $(c_0, c_1, \ldots, c_{n-1})$ is the first row of C.

In the following we give some properties of complex circulant matrices. All the results are taken from Kra and Simanca [22].

Definition 5.22. Let $C = \mathrm{Circ}(c_0, \ldots, c_{s-1})$. The polynomial P_C (in the indeterminate z) defined by

$$P_C(z) = c_0 + c_1 z + \cdots c_{s-1} z^{s-1}$$

is called the *representer* of C.

Let ϵ be an sth primitive root of unity in $\mathbb{C}$. For $l = 0, 1, \ldots, s-1$ define a column vector $x_l := \frac{1}{\sqrt{s}}(1, \epsilon^l, \epsilon^{2l}, \ldots, \epsilon^{(s-1)l})$. One can show that x_l is an eigenvector of C with eigenvalue $P_C(\epsilon^l)$ for every l. The set $\{x_l\}_l$ is linearly independent since x_l^T are the rows of a Vandermonde matrix. It follows that C can be diagonalized and the determinant of C is given by the product of all eigenvalues of C. Therefore we have the following proposition.

Proposition 5.23. *If $C = \mathrm{Circ}(c_0, \ldots, c_{s-1})$, then*

$$\det C = \prod_{l=0}^{s-1} P_C(\epsilon^l),$$

where ϵ is any sth primitive root of unity in $\mathbb{C}$.

The following equivalent conditions characterizing the singularity of circulant matrices are obvious consequences of the determinant formula above. These conditions will be useful for us to determine the non-singularity of the circulant matrix as in (5.3).

Proposition 5.24. *Let $C \in \mathbb{C}^{s\times s}$ be a circulant matrix with a representer P_C. The following are equivalent:*

(1) The matrix C is singular.

(2) $P_C(\eta) = 0$ for some sth root of unity η in $\mathbb{C}$.

(3) The polynomials $P_C(z)$ and $z^s - 1$ are not relatively prime.

We also have several special cases where a circulant matrix is invertible.

Theorem 5.25 ([22])**.** *Let $C = \mathrm{Circ}(c_0, \ldots, c_{s-1})$. Then C is non-singular in the following cases:*

(1) If s is prime, $(c_0, \ldots, c_{s-1})$ is in $\mathbb{Q}^s$ and not a multiple of $(1, 1, \ldots, 1)$, and $\sum_{i=0}^{s-1} c_i \neq 0$.

(2) If $(c_0, \ldots, c_{s-1}) \in \mathbb{C}^s$ and there is an index j such that $|c_j| > \sum_{i\neq j} |c_i|$.

(3) If $(c_0, \ldots, c_{s-1}) \in \mathbb{R}^s$ and $c_0, c_1, \ldots, c_{s-1}$ is a strictly monotone sequence and either all entries are nonpositive or all entries are nonnegative.

Proof. See [22, Proposition 18, 23, 24]. □

Here is a first example of how we can apply the above results to our question about the equivalence theorem.

Example 5.26. Let $\mathbb{F} := \{0, \alpha_1, \ldots, \alpha_s\}$ be a finite field. Define a weight function w on $\mathbb{F}$ as follows: $w(0) = 0$ and

$$w(\alpha_i) = 2^{1-i} \quad \text{if } i = 1, \ldots, s$$

Clearly $\mathrm{Sym}(w) = \{1\}$. We will show that w satisfies the equivalence theorem. After some reordering, the matrix A corresponding to the weight w is a circulant matrix. More precisely, $A = \mathrm{Circ}(c_1, \ldots, c_s)$ where $\{c_1, \ldots, c_s\}$ is a permutation of $\{2^{1-i}\}_{1 \le i \le s}$. Let j be the index such that $c_j = 2^0 = 1$. Notice that

$$\sum_{i \neq j} c_i < \sum_{i=1}^{\infty} 2^{-i} = 1 = c_j.$$

Therefore by Theorem 5.25 we conclude that A is non-singular and hence w satisfies the equivalence theorem due to Theorem 5.4. Since $\mathrm{Sym}(w) = \{1\}$, this means that any w-isometry is a permutation equivalence.

5.4 Equivalence Theorem for the Lee Weight on Certain Fields

Recall the Lee weight w_L on $\mathbb{Z}_N$ given in Definition 2.4. It is still an open problem whether the Lee weight satisfies the equivalence theorem for a general residue ring $\mathbb{Z}_N$. Wood claimed in [40] and proved in [41] that this is true for N of the form 2^k, 3^k for any k, and for prime numbers N of the form $N = 2p + 1$, where p itself is prime. His proof for all these cases relies on the factorization of semigroup determinants that he developed in [45].

In this section we will reproduce the result of Wood for the case $N = 2p + 1$, where N and p are prime, by exploiting the structure of A that we have learned in the previous section. By realizing that A is a circulant matrix and using Proposition 5.23, our approach also gives a factorization of the determinant of A. The advantage of our approach to Wood's is that, modulo N we know explicitly the coefficients of the representer polynomial P_A that appear in the factorization of $\det(A)$. We will exploit this advantage to show that the equivalence theorem for the Lee weight is also true for the case $N = 4p + 1$, where N and p are prime.

First we reprove the result of Wood.

Theorem 5.27 ([41])**.** *The Lee weight w_L on $\mathbb{Z}_N$ satisfies the equivalence theorem for $N = 2p + 1$, where N and p are prime.*

Recall that a prime number p is called a *Sophie Germain prime* if $2p + 1$ is also prime. In this case the prime number $2p + 1$ is also known as a *safe prime*. It is not known but strongly believed that there are infinitely many such primes.

Proof. Notice that $U = \{\pm 1\}$ is the symmetry group of the Lee weight. Let β be a generator of the cyclic group $\mathbb{Z}_N^*$. Then clearly βU is a generator of $\mathbb{Z}_N^*/U$ and from (5.3) we have that $A = \mathrm{Circ}(v)$, where $v = (w_L(1), w_L(\beta), \ldots, w_L(\beta^{p-1}))$. Obviously, the vector v is in $\mathbb{Q}^p$ where p is prime. The components of v are all possible distinct values of the Lee weight on $\mathbb{Z}_{2p+1}$, and these are the values $1, 2, \ldots, p$. Hence v is a permutation of $(1, 2, \ldots, p)$. It follows that v is not a multiple of $(1, 1, \ldots, 1)$ and clearly

$$\sum_{i=0}^{p-1} w_L(\beta^i) = \sum_{j=1}^{p} j = \frac{p(p+1)}{2} > 0.$$

Now Theorem 5.25 implies that A is non-singular and hence by Theorem 5.4, the Lee weight satisfies the equivalence theorem. □

Now we can generalize this result to the following case.

Theorem 5.28. *The Lee weight w_L on $\mathbb{Z}_N$ satisfies the equivalence theorem for $N = 4p + 1$, where N and p are prime.*

The infinitude of Sophie Germain primes and prime numbers p such that $4p + 1$ is also prime are special cases of a well known conjecture in number theory called Dickson's Conjecture (see [7] and [20, Problem 16.5]). A link to the first 5000 prime numbers p where $4p + 1$ is also prime can be found in [39].

Proof. It is well-known (see for example [21, pp. 514]) that 2 is a generator of the cyclic group $\mathbb{Z}_N^*$. Then as in the proof of Theorem 5.27, we have

$$A = \mathrm{Circ}(w_L(1), w_L(2), \ldots, w_L(2^{2p-1})).$$

The representer $P(x)$ of A is given by

$$P(x) = \sum_{k=0}^{2p-1} w_L(2^k)x^k.$$

By Proposition 5.24 we have to show that $P(\eta) \neq 0$ for each $2p$th root of unity η. Thus, fix such an η. Then $\mathrm{ord}(\eta) \in \{1, 2, p, 2p\}$. Now we will consider each case separately to show that $P(\eta) \neq 0$. For the rest of the proof we will simply write w for the Lee weight w_L. Notice also that $w(1), w(2), \ldots, w(2^{2p-1})$ are, up to ordering, the numbers $1, 2, \ldots, 2p$.

Case 1. $\mathrm{ord}(\eta) = 1$.
Then $\eta = 1$ and we have

$$P(1) = \sum_{k=0}^{2p-1} w(2^k) > 0 \qquad (\text{since } w(2^k) \in \mathbb{N})$$

Case 2. $\mathrm{ord}(\eta) = 2$.
Then $\eta = -1$. Suppose $P(\eta) = 0$. Then

$$0 = P(-1) = \sum_{k=0}^{p-1} w(2^{2k}) - \sum_{k=0}^{p-1} w(2^{2k+1}).$$

It follows that

$$2\sum_{k=0}^{p-1} w(2^{2k}) = \sum_{k=0}^{2p-1} w(2^k) = \sum_{k=1}^{2p} k = p(2p+1). \tag{5.4}$$

Hence the left hand side is even but the right hand side is odd. Thus $P(\eta) \neq 0$.

Case 3. $\operatorname{ord}(\eta) = p$.

Then $\eta^{p+k} = \eta^k$ for $k = 0, 1, \ldots, p-1$. Suppose $P(\eta) = 0$. Then

$$0 = P(\eta) = \sum_{k=0}^{p-1} \left(w(2^k) + w(2^{p+k})\right) \eta^k.$$

Recall that $1+x+\cdots+x^{p-1}$ is the minimal polynomial of η over $\mathbb{Q}$. Thus we conclude that $1 + x + \cdots + x^{p-1}$ divides $q(x) = \sum_{k=0}^{p-1} \left(w(2^k) + w(2^{p+k})\right) x^k$. Since $q(x)$ has degree $p-1$, this implies that the coefficients of $q(x)$ are all equal, and thus equal to $w(1) + w(2^p)$. By adding all these coefficients we obtain

$$p\left(w(1) + w(2^p)\right) = \sum_{k=0}^{p-1} \left(w(2^k) + w(2^{p+k})\right) = \sum_{k=0}^{2p-1} w(2^k).$$

Thus

$$p\left(1 + w(2^p)\right) = \sum_{k=1}^{2p} k = p(2p+1).$$

It follows that

$$w(2^p) = 2p. \tag{5.5}$$

Recall that $w(\alpha) \equiv \pm\alpha \pmod N$ for $\alpha \in \mathbb{Z}_N$, where one of the two identities must be true. Reducing (5.5) modulo N and multiplying both sides by 2, we arrive at

$$2\left(\pm 2^p\right) = 4p \equiv -1 \pmod{4p+1}.$$

Squaring both sides we have

$$2^{2p+2} \equiv 1 \pmod{4p+1}.$$

But 2 has order $4p$. So $4p \leq 2p+2$, which implies $p \leq 1$, a contradiction.

Case 4. $\operatorname{ord}(\eta) = 2p$

Then $\eta^p = -1$ and we have $\eta^{p+k} = -\eta^k$ for $k = 0, 1, \ldots, p-1$. Suppose $P(\eta) = 0$. Then

$$0 = P(\eta) = \sum_{k=0}^{p-1} \left(w(2^k) - w(2^{p+k})\right) \eta^k$$

Denote by $\Phi_m(x)$ the mth cyclotomic polynomial. It is known that $\Phi_m(x)$ is the minimal polynomial over $\mathbb{Q}$ of every mth primitive root in $\mathbb{C}$. This implies that for odd primes p we have $\Phi_{2p}(x) = \Phi_p(-x)$ (see also [11, pp. 555]). Observe also that since $N = 4p+1$ is prime, our prime p is certainly odd. It follows that $\sum_{k=0}^{p-1} \left(w(2^k) - w(2^{p+k})\right) x^k$ is a scalar multiple of $\Phi_p(-x) = 1 - x + x^2 - x^3 + \cdots + x^{p-1}$. Considering the constant coefficient and the coefficient of x, we conclude

$$w(1) - w(2^p) = w(2^{p+1}) - w(2)$$

It follows that

$$w(2^p) + w(2^{p+1}) = 3$$

Reducing the equation modulo N we have

$$\pm 2^p \pm 2^{p+1} \equiv 3 \pmod{4p+1}.$$

Squaring both sides we obtain

$$2^{2p} + 2^{2p+2} \pm 2 \cdot 2^{2p+1} \equiv 9 \pmod{4p+1}.$$

Recalling that $2^{2p} = -1$ we have

$$\begin{aligned} -1 - 4 \pm 4 &\equiv 9 \pmod{4p+1} \\ \pm 4 &\equiv 14 \pmod{4p+1}. \end{aligned}$$

Then $N = 4p+1$ divides 18 or $N \mid 10$. Since N is prime, then $N = 2, N = 3$, or $N = 5$. But then N is not of the form $4p+1$, where p is prime. Thus $P(\eta) \neq 0$.

All of this shows that we may apply Proposition 5.24 and conclude that A is nonsingular. Again, by Theorem 5.4 this means that the Lee weight on $\mathbb{Z}_N$ for this choice of N satisfies the equivalence theorem. □

It is known that for primes N of the form $N = 8p+1$, where p is prime (except $N = 41$), the element 3 is a primitive root modulo N (see [32, Theorem 1.6]. Thus, one may try to apply the above method to establish the equivalence theorem for the Lee weight in this particular case. Unfortunately the method fails, even in the case $\mathrm{ord}(\eta) = 2$. Assuming $P(\eta) = 0$, one derives a similar equation as in Equation (5.4), namely

$$2\sum_{k=0}^{2p-1} w(3^{2k}) = \sum_{k=0}^{4p-1} k = 2p(4p-1).$$

But now we can not easily derive a contradiction from this identity as we did earlier.

Nevertheless, realizing the A matrix as a circulant matrix helps us to check the validity of the equivalence theorem for the Lee weight for many cases. Wood [40, p. 1012] checked that the equivalence theorem holds true for all numbers $N \leq 256$. Meanwhile, we have checked the validity of the equivalence theorem for the Lee weight for all prime numbers N up to the 2012th prime, simply by verifying that the representer $P_A(z)$ of A is relatively prime to $z^s - 1$ (see 5.24). With this abundance of evidence, we strongly believe that the equivalence theorem holds true for the Lee weight on $\mathbb{Z}_N$ for any prime N.

Although we did not succeed in proving the general equivalence theorem for the Lee weight, we offer another perspective to solve the general situation. Recall that in Section 2.2 we define the Lee weight on $\mathbb{Z}_N$ via arc lengths on a circle. In that situation, we assume that we place the elements of $\mathbb{Z}_N$ on the circle using the order $0, 1, 2, \ldots, N-1$. In the following example, we will show that for N prime, a different choice of the ordering on the circle leads to a new circular weight that satisfies the equivalence theorem.

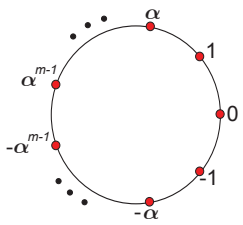


Figure 5.1: Reordering the points on the circle

Example 5.29. Let N be prime. The set of units $\mathbb{Z}_N^*$ is a cyclic group, say generated by some α. For $N = 2$ there is a unique ordering on the circle so we will not consider this case and assume that N is odd. Write $N = 2m + 1$. Then $\alpha^m = -1$. Now label the points on the circle in the ordering $0, 1, \alpha, \ldots, \alpha^{m-1}, -\alpha^{m-1}, \ldots, -\alpha, -1$.

Define the α-Lee weight w_L^α similar to the Lee weight but by using the above new ordering. So we have

$$w_L^\alpha(x) = \begin{cases} 0 & \text{if } x = 0 \\ i + 1 & \text{if } x = \pm\alpha^i \text{ for } i = 0, \ldots, m-1 \end{cases}$$

Notice that the α-Lee weight preserves many properties of the Lee weight. Among them we observe that the α-Lee weight partitions $\mathbb{Z}_N$ the same way as the Lee weight, $\mathrm{Sym}(w_L^\alpha) = \{\pm 1\}$, and the values of the α-Lee weight are still $0, 1, \ldots, m$.

Now we will show that the α-Lee weight satisfies the equivalence theorem.

Theorem 5.30. *Let $N = 2m + 1$ be a prime number and let α be a generator of the cyclic group $\mathbb{Z}_N^*$. Then the α-Lee weight on $\mathbb{Z}_N$ satisfies the equivalence theorem.*

Proof. As in (5.3), the matrix A can be written as

$$A = \mathrm{Circ}(w(1), w(\alpha), \ldots, w(\alpha^{m-1})).$$

But now notice that the sequence $w(1), w(\alpha), \ldots, w(\alpha^{m-1}) = 1, 2, \ldots, m$ is strictly monotone. By Theorem 5.25, A is non-singular and this finishes the proof. □

Chapter 6 Local Global Properties

In this chapter we will give some answers to a question originally raised by Goldberg [12] and which we formulated in Question 3.19. We will again use character theoretic methods in our approach. We will use the character equations that arise naturally from the concept of F-partitions and proceed in a similar fashion as we did in Chapter 4.

In the first section we reformulate Goldberg's question in terms of a local-global property of a subgroup G of $\mathrm{GL}(n, R)$. As a motivation we show that Witt's extension theorem and the equivalence theorem for compositions fit into this new framework. Since F-partitions play a central role in our methods, we will devote a full section to discussing this concept. Among other things we will show how to create F-partitions on R^n from the orbits of the multiplication action of certain subgroups G of $\mathrm{GL}(n, R)$ on R^n. Then we present our main results which show that the local-global property holds true for various subgroups of $\mathrm{GL}(n, R)$, and we show their connection to certain weight functions that have been studied in the literature.

Throughout this chapter let R be a finite commutative admissible ring with admissible character χ.

6.1 Motivation

In Definition 5.2 we defined, for a subgroup U of $\mathcal{U}(R)$, a local U-monomial map $f : \mathcal{C} \to R$ as a map that acts like a monomial map on each $x \in \mathcal{C}$, that is for every $x \in \mathcal{C}$ there is an $M_x \in \mathcal{M}_U(n, R)$ such that $f(x) = xM_x$. Let $\mathcal{P}_U$ be the partition formed by the U-orbits in R^n (Definition 3.13). Being able to recognize a $\mathcal{P}_U$-isometry as a $\mathcal{M}_U(n, R)$-map has led us to some interesting results in the previous chapter. So first we generalize the concept of a local map to any subgroup G of $\mathrm{GL}(n, R)$.

Definition 6.1. Let $\mathcal{C}$ be a submodule of R^n. Let G be a subgroup of $\mathrm{GL}(n, R)$. A linear map $f : \mathcal{C} \to R^n$ is called a *local G-map* if for every $x \in \mathcal{C}$ there is an $M_x \in G$ such that $f(x) = xM_x$. We say that such f is a *global G-map* if there is an $M \in G$ such that $f(x) = xM$ for all $x \in \mathcal{C}$. As a consequence, a global G-map extends to a G-automorphism on R^n.

We need to emphasize that from the definition above, local G-maps are always linear. Let $f : \mathcal{C} \to R^n$ be a local G-map. Suppose $f(x) = 0$. Then $0 = f(x) = xM_x$ for some $M_x \in G$. Since M_x is invertible, $x = 0$. Therefore all local G-maps are injective.

Since a map is a $\mathcal{P}_U$-isometry if and only if it is a local $\mathcal{M}_U(n, R)$-map, Theorem 4.9 can be reformulated as follows.

Theorem 6.2 (Wood, [42])**.** *Every local $\mathcal{M}_U(n, R)$-map $f : \mathcal{C} \to \mathcal{C}'$ is a global $\mathcal{M}_U(n, R)$-map.*

Let us also reformulate Witt's extension theorem (Theorem 3.17) in terms of this local-global property. Let Q be a nonsingular quadratic form on a finite-dimensional vector space V over a field (not necessarily finite) of characteristic $\neq 2$. Let $\Omega = \{M \in \mathrm{Aut}(V,V) : Q(xM) = Q(x) \text{ for all } x \in V\}$ be the Q-orthogonal group. Suppose $f : W_1 \to W_2$ is a local Ω-map of subspaces W_1, W_2 of V. More precisely, for all $x \in W_1$ there exists an automorphism $M_x \in \Omega$ such that $f(x) = xM_x$. Then

$$Q(f(x)) = Q(xM_x) = Q(x).$$

Therefore f is a Q-isometry on W_1, and by Witt's extension theorem (Theorem 3.17) the following is true.

Theorem 6.3. *Every local Ω-map $f : W_1 \to W_2$ is a global Ω-map.*

For anisotropic spaces the converse is true as well: Witt's extension theorem follows from Theorem 6.3. This can be seen as follows. A quadratic space (V, Q) is called *anisotropic* if there is no $x \neq 0 \in V$ such that $Q(x) = 0$. If (V, Q) is anisotropic and $Q(x) = Q(y)$, then there exist $M \in \Omega$ such that $y = xM$ (see [25, Proposition 4.7]. Let (V, Q) be an anisotropic quadratic space. Let W_1, W_2 be subspaces of V and let $f : W_1 \to W_2$ be a Q-isometry. Note that for $x \in W_1$ we have $Q(x) = Q(f(x))$. It follows from the above that $f(x) = xM_x$ for some $M_x \in \Omega$. Thus f is a local Ω-map. Therefore for anisotropic space (V, Q), Theorem 6.3 is equivalent to Witt's extension theorem (Theorem 3.17). It is worth noting that no quadratic space of dimension at least 3 over a finite field is anisotropic, see [35, Section 1.7]

All of this gives rise to the following terminology.

Definition 6.4. Let G be a subgroup of $\mathrm{GL}(n, R)$. We say that G *satisfies the local-global property* if every local G-map $f : \mathcal{C} \to R^n$ is a global G-map.

From the above theorems it is natural to ask if we also have the local-global property for other subgroups G of $\mathrm{GL}(n, R)$.

Question 6.5. Which subgroups G of $\mathrm{GL}(n, R)$ satisfy the local-global property?

To show that the local-global property is not trivial, we give an example of a subgroup G of $\mathrm{GL}(n, R)$ which does not satisfy the local-global property.

Example 6.6. Let $\mathbb{F}_3$ be the field with three elements. Consider the following subgroup G of $\mathrm{GL}(n, \mathbb{F}_3)$

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{F}_3 \text{ and } ac = 1 \right\}.$$

Let $f : \mathbb{F}_3^2 \to \mathbb{F}_3^2$ be defined by $f(\alpha(1,0)+\beta(0,1)) = \alpha(2,1)+\beta(0,1)$ for any $\alpha, \beta \in \mathbb{F}^3$. Obviously, f is linear. There are four one-dimensional subspaces of $\mathbb{F}_3^2$. The following

are bases for those subspaces: $(1,0),(0,1),(1,1),(1,2)$. Notice that

$$f(1,0) = (2,1) = (1,0)\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$$
$$f(0,1) = (0,1) = (0,1)\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$
$$f(1,1) = (2,2) = (1,1)\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$
$$f(1,2) = (2,0) = (1,2)\begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix},$$

where the matrices on the very right are the unique matrices in G satisfying the identities, and where $*$ may be any element of $\mathbb{F}_3$. Hence f is a local G-map. But f is not a global G-map because $f(1,0)$ and $f(0,1)$ cannot be expressed with a common matrix $M \in G$. Even more, f is uniquely given by $x \mapsto x\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$. This is also shows that f is a local $\mathrm{SL}(2,\mathbb{F}_3)$-map, but not a global one. Thus, $\mathrm{SL}(n,R)$ does not satisfy the local-global property in general.

Before we explore the local-global property further we need to develop some tools in the next section.

6.2 F-Partitions

The notion of an F-partition was first introduced by Zinoviev and Ericson [47] to study the existence of some types of MacWilliams identities between abelian group codes and their duals.

Definition 6.7. Let A be a finite (additive) abelian group with character group $\widehat{A}$. Fix an isomorphism $\varphi : A \to \widehat{A}$ given by $a \mapsto \varphi_a$. Let $\mathcal{P} = P_0, P_1, \ldots, P_s$ be a partition of A. For $x, y \in A$ we write $x \sim_{\mathcal{P}} z$ to indicate that x and y belong to the same partition set P_i. We say that $\mathcal{P}$ is an *F-partition with respect to the isomorphism* $a \mapsto \varphi_a$, if for every $j = 0, \ldots, s$ the sum $\sum_{y \in P_j} \varphi_y(x)$ does not depend on the choice of x in its partition set P_i, that is

$$\sum_{y \in P_j} \varphi_y(x) = \sum_{y \in P_j} \varphi_y(z) \text{ for } j = 0, \ldots, s$$

whenever $x \sim_{\mathcal{P}} z$.

The notion of an F-partition of an abelian group A with respect to a certain isomorphism $\varphi : A \to \widehat{A}$ was originally defined via a Fourier transform with respect to that isomorphism. This explains the F in the terminology. We refer the interested reader to [47].

The property of being an F-partition depends on the choice of the isomorphism between A and $\widehat{A}$; an example will be given in Example 6.24. We will always make the underlying isomorphism explicit.

Most of the time the abelian group A that we are dealing with is $(R^n, +)$ where R is our admissible ring with admissible character χ. Recall that every character ψ on R can be written as $\chi \circ \mu_r$ (Definition 4.2). For short, we will write χ_r for $\chi \circ \mu_r$. One can easily check that the map $r \mapsto \chi_r$ gives a group isomorphism from $(R, +)$ to $(\widehat{R}, \cdot)$. Now we are ready to give several examples of F-partitions on R.

Example 6.8. Partition R into $P_0 = \{0\}$ and $P_1 = R\backslash\{0\}$. We call this partition the *Hamming* partition. Since $\chi_0 = \chi \circ \mu_0$ is the principal character, it is clear that $\chi_0(x) = \chi_0(y)$ for every $x, y \in P_1$. By the fact that χ is an admissible character and by Proposition 2.18, we have for any $x \in P_1$

$$\sum_{z \in P_1} \chi_z(x) = -1 + \sum_{z \in R} \chi_z(x) = -1 + \sum_{\psi \in \widehat{R}} \psi(x) = |R| - 1.$$

Therefore the Hamming partition is an F-partition with respect to the isomorphism $r \mapsto \chi_r$.

Example 6.9. Let U be a subgroup of $\mathcal{U}(R)$. Denote by $\mathcal{P}_U = P_0, P_1, \ldots, P_s$ the U-orbits in R. In this context we always use the convention that $P_0 = \{0\}$ and $P_1 = U$. It is known that $\mathcal{P}_U$ is an F-partition. This is a special case of a more general situation that we will prove later in Theorem 6.18. F-partitions on R that arise in this way are called *multiplicative*.

Before we discuss F-partitions on R^n we need to set several conventions.

Definition 6.10. Let $\odot$ be the component-wise multiplication on R^n defined by

$$x \odot y = (x_1 y_1, \ldots, x_n y_n).$$

With respect to the usual addition and $\odot$ multiplication, R^n is a ring. If we want to emphasize the ring structure of R^n, we will denote R^n by $R^n_{\odot}$.

Consider again the admissible character χ on R and let $\Phi := \overbrace{\chi \oplus \cdots \oplus \chi}^{n}$ be the character on R^n defined by $\Phi(x) = \prod_{i=1}^n \chi(x_i)$ (see Lemma 2.10). Let $x \in R^n$. Denote by $\mu_x^{\odot} : R^n \to R^n$ the $\odot$-multiplication map by x on $R^n_{\odot}$. Due to Lemma 2.10, every character on R^n is of the form $\chi_{x_1} \oplus \cdots \oplus \chi_{x_n}$, and this in turn can be written as $\Phi \circ \mu_x^{\odot}$ where $x = (x_1, \ldots, x_n)$. Hence $R^n_{\odot}$ is an admissible ring with admissible character Φ. Let $\Phi_x := \Phi \circ \mu_x^{\odot}$. Then $x \mapsto \Phi_x$ is an isomorphism of the additive groups of R^n and $\widehat{R^n}$.

Denote the usual dot product between two vectors $x, y \in R^n$ by $\langle x, y \rangle = x_1 y_1 + \ldots + x_n y_n$. By using the multiplicative structure of R we can express $\Phi_x(y)$ nicely as follows.

$$\Phi_x(y) = (\chi_{x_1} \oplus \ldots \oplus \chi_{x_n})(y_1, \ldots, y_n) = \prod_{i=1}^n \chi(x_i y_i) = \chi(\langle x, y \rangle).$$

Using the isomorphism $x \mapsto \Phi_x$, Definition 6.7 now amounts to the following for partitions in R^n.

Proposition 6.11. *A partition $\mathcal{P} = P_0, P_1, \ldots, P_s$ on R^n is an F-partition with respect to the isomorphism $x \mapsto \Phi_x$ if for any $j = 0, 1, \ldots, s$ the quantity*

$$\sum_{y \in P_j} \chi(\langle y, x \rangle)$$

only depends on the set P_i where x belongs to.

Zinoviev and Ericson gave the following construction.

Proposition 6.12 (Zinoviev and Ericson [47])**.** *Let $\mathcal{P}$ and $\mathcal{Q}$ be F-partitions of abelian groups A and B with respect to the isomorphisms $a \mapsto \chi_a$ and $b \mapsto \psi_b$, respectively.. Then the partition $\mathcal{P} \times \mathcal{Q}$ consisting of all $P \times Q$, where P and Q are sets in $\mathcal{P}$ and $\mathcal{Q}$, respectively, is an F-partition of $A \times B$ with respect to the isomorphism $(a, b) \mapsto \chi_a \oplus \psi_b$. In particular $\mathcal{P}^n := \underbrace{\mathcal{P} \times \cdots \times \mathcal{P}}_{n}$ is an F-partition of A^n with respect to the isomorphism $x \mapsto \Phi_x$.*

Another natural construction of F-partitions is as follows. For any permutation $\sigma \in S_n$ and any $x \in R^n$ define $x\sigma := (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. For any subset $S \subset R^n$ let $S\sigma := \{x\sigma \mid x \in S\}$. Let $\mathcal{P} = P_0, P_1, \ldots, P_s$ be a partition on R. Note that $(P_{i_1} \times \cdots \times P_{i_n})\sigma = P_{i_{\sigma(1)}} \times \cdots \times P_{i_{\sigma(n)}}$.

Definition 6.13. Define an equivalence relation $\sim_{\mathcal{P}^n_{sym}}$ on R^n by declaring that $x \sim_{\mathcal{P}^n_{sym}} y$ if there is a permutation $\sigma \in S_n$ such that $x \sim_{\mathcal{P}^n} y\sigma$. We call the partition formed by this equivalence relation $\mathcal{P}^n_{sym}$. Elements of $\mathcal{P}^n_{sym}$ are sets of the form $Q := \bigcup_{\sigma \in S_n} P\sigma$ for some $P \in \mathcal{P}^n$.

For instance, the Hamming partition on R^n is $\mathcal{P}^n_{sym}$, where $\mathcal{P}$ is as in Example 6.8. From the following proposition it follows that it is an F-partition on R^n.

Observe that $\mathcal{P}^n_{sym}$ may be regarded as a symmetrization of $\mathcal{P}^n$. From the above definition it is clear that $Q\tau = Q$ for every $\tau \in S_n$. Also for each $Q \in \mathcal{P}^n_{sym}$ one can find a subset $S_Q \subset S_n$ such that $Q = \biguplus_{\sigma \in S_Q} P\sigma$. For example for $P := P_0 \times P_0 \times P_0 \in \mathcal{P}^3$ we have $Q = \bigcup_{\sigma \in S_3} P\sigma = P = \biguplus_{\sigma \in \{\mathrm{id}\}} P\sigma$. Now we will show that $\mathcal{P}^n_{sym}$ is an F-partition.

Proposition 6.14. *If $\mathcal{P}$ is an F-partition on R with respect to the isomorphism $a \mapsto \chi_a$, then $\mathcal{P}^n_{sym}$ is an F-partition with respect to $x \mapsto \Phi_x$.*

Proof. Let $x \sim_{\mathcal{P}^n_{sym}} z$. Then there is a $\tau \in S_n$ such that $x \sim_{\mathcal{P}^n} z\tau$. For any $Q = \biguplus_{\sigma \in S_Q} P\sigma \in \mathcal{P}^n_{sym}$ we have

$$\sum_{y \in Q} \Phi_y(x) = \sum_{y \in Q} \chi(\langle y, x \rangle) = \sum_{\sigma \in S_Q} \sum_{y \in P\sigma} \chi(\langle y, x \rangle) = \sum_{\sigma \in S_Q} \sum_{y \in P\sigma} \chi(\langle y, z\tau \rangle),$$

where the last identity is true since $P\sigma$ is a set of the F-partition $\mathcal{P}^n$; see Proposition 6.12. Now the above is equal to

$$\sum_{y \in Q} \chi(\langle y, z\tau \rangle) = \sum_{y \in Q\tau^{-1}} \chi(\langle y\tau, z\tau \rangle) = \sum_{y \in Q} \chi(\langle y, z \rangle) = \sum_{y \in Q} \Phi_y(z),$$

since $Q\tau^{-1} = Q$ and $\langle y\tau, z\tau\rangle = \langle y, z\rangle$. □

Now we introduce partitions on R^n that arise as orbits of the multiplication action of some subgroup G of $\mathrm{GL}(n, R)$.

Definition 6.15. A partition $\mathcal{P}$ on R^n is called a *multiplicative partition* if the sets of $\mathcal{P}$ are the G-right multiplication orbits for some subgroup G of $\mathrm{GL}(n, R)$.

This definition generalizes the concept of a multiplicative partition that we introduced in Example 6.9.

We will recall some notation and introduce some new ones.

Definition 6.16. Let U be a subgroup of $\mathcal{U}(R)$. The set of all permutation, monomial and U-monomial $n \times n$ matrices are denoted by $\mathcal{P}(n, R)$, $\mathcal{M}(n, R)$, and $\mathcal{M}_U(n, R)$. We define some more standard subgroups of $\mathrm{GL}(n, R)$ as follows

$$\begin{aligned}
\Delta(n, R) &:= \{\text{diagonal matrices with the diagonal entries being units}\},\\
\Delta_U(n, R) &:= \{\text{diagonal matrices where the diagonal entries are in } U\},\\
\mathrm{LT}(n, R) &:= \{\text{lower triangular matrices where the diagonal entries are units}\},\\
\mathrm{LT}_U(n, R) &:= \{\text{lower triangular matrices where the diagonal entries are in } U\}.
\end{aligned}$$

We will also use $\mathrm{Mat}(n, R)$ for the ring of $n \times n$-matrices with entries in R.

We have seen in Proposition 6.12 and Proposition 6.14 that for any F-partition $\mathcal{P}$, the two partitions $\mathcal{P}^n$ and $\mathcal{P}^n_{sym}$ are F-partitions on R^n. If $\mathcal{P} = \mathcal{P}_U$ is the partition consisting of the U-orbits for some subgroup U of $\mathcal{U}(R)$, then the partitions $\mathcal{P}^n$ and $\mathcal{P}^n_{sym}$ are in fact multiplicative partitions as well.

Proposition 6.17. *Let U be a subgroup of $\mathcal{U}(R)$ and let $\mathcal{P}_U$ be the associated multiplicative partition on R. Then $\mathcal{P}^n$ and $\mathcal{P}^n_{sym}$ are the multiplicative partitions with respect to $\Delta_U(n, R)$ and $\mathcal{M}_U(n, R)$, respectively.*

Proof. If $x \sim_{\mathcal{P}^n} y$, then x and y belong to the same partition set $P_{i_1} \times \cdots \times P_{i_n} \in \mathcal{P}^n$. Since $\mathcal{P} = \mathcal{P}_U$, for each $j = 1, \ldots, n$ there is an $\alpha_j \in U$ such that $y_j = \alpha_j x_j$. Therefore $x = y \cdot \mathrm{diag}(\alpha_1, \ldots, \alpha_n)$. Similarly if $x \sim_{\mathcal{P}^n_{sym}} y$, then there is a $\sigma \in S_n$ such that $x\sigma, y$ belong to the same set P in $\mathcal{P}^n$. It follows that there are $\alpha_1, \ldots, \alpha_n$ such that $x\sigma = y \cdot \mathrm{diag}(\alpha_1, \ldots, \alpha_n)$. Thus $x = y \cdot \mathrm{diag}(\alpha_1, \ldots, \alpha_n)P_{\sigma^{-1}}$ where P_σ is the permutation matrix that is obtained by permuting the identity matrix I_n under σ. Since $\mathrm{diag}(\alpha_1, \ldots, \alpha_n)P_{\sigma^{-1}} \in \mathcal{M}_U(n, R)$, then x, y belong to the same $\mathcal{M}_U(n, R)$-orbit. The converse is obvious by simply reversing the arguments. □

Next we will show that under a certain condition on the subgroup G of $\mathrm{GL}(n, R)$, the multiplicative partition on R^n induced by G is an F-partition with respect to a suitable isomorphism between R^n and $\widehat{R^n}$. Recall that the map from R^n to $\widehat{R^n}$, defined by $x \mapsto \Phi_x$ where $\Phi_x(y) = \chi(\langle x, y\rangle)$, is a group isomorphism. Since right-multiplication by a matrix $M \in \mathrm{GL}(n, R)$ gives an isomorphism on R^n, it is easy to see that the map $x \mapsto \Phi_{xM}$ is also a group isomorphism from R^n to $\widehat{R^n}$.

For a subgroup G of $\mathrm{GL}(n, R)$ define $G^T := \{A^T \mid A \in G\}$.

Proposition 6.18. *Let G be a subgroup of $\mathrm{GL}(n,R)$ and let $M \in \mathrm{GL}(n,R)$ be such that $MG^TM^{-1} \subseteq G$. Then the multiplicative partition on R^n given by the G-orbits is an F-partition with respect to the isomorphism $x \mapsto \Phi_{xM}$.*

Proof. Let x, z belong to the same G-orbit. Hence $z = xA$ for some $A \in G$. Then $B := MA^TM^{-1} \in G$. Let $\mathcal{O}$ be a G-orbit. We have

$$\begin{aligned}
\sum_{y\in\mathcal{O}} \Phi_{yM}(z) &= \sum_{y\in\mathcal{O}} \chi(\langle yM, z\rangle) \\
&= \sum_{y\in\mathcal{O}} \chi\left(\langle yM, xA\rangle\right) \qquad (\text{since } z = xA) \\
&= \sum_{y\in\mathcal{O}} \chi\left(\langle yMA^T, x\rangle\right) \\
&= \sum_{y\in\mathcal{O}} \chi\left(\langle y(MA^TM^{-1})M, x\rangle\right) \\
&= \sum_{y\in\mathcal{O}} \Phi_{yBM}(x) \qquad (\text{since } B = MA^TM^{-1}) \\
&= \sum_{y\in\mathcal{O}} \Phi_{yM}(x) \qquad (\text{since } y \mapsto yB \text{ is bijective on } \mathcal{O}).
\end{aligned}$$

□

Remark 6.19. Since $A \mapsto A^T$ is a bijection from G to G^T, the condition $MG^TM^{-1} \subseteq G$ is equivalent to $MG^TM^{-1} = G$. It follows that $M^{-1}GM = G^T$. If $M = I_n$ is the identity matrix, the hypothesis that $MG^TM^{-1} \subseteq G$ is equivalent to G being closed under matrix transposition.

Corollary 6.20. *For each of the groups*

$$\mathrm{GL}(n,R),\ \mathcal{P}(n,R),\ \Delta(n,R),\ \Delta_U(n,R),\ \mathcal{M}(n,R),\ \mathcal{M}_U(n,R)$$

the multiplicative orbits form an F-partition with respect to the isomorphism $x \mapsto \Phi_x$.

Proof. All the subgroups above are closed under matrix transposition. □

We also have the following interesting result.

Corollary 6.21. *Let G be a Sylow subgroup of $\mathrm{GL}(n,R)$. Then there exists a matrix $M \in \mathrm{GL}(n,R)$ such that the G-orbits form an F-partition with respect to the isomorphism $x \mapsto \Phi_{xM}$.*

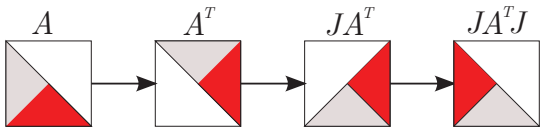
Proof. Since G^T is a subgroup of the same order, it is a Sylow subgroup as well (with respect to the same prime factor). But then G^T and G are conjugate, and thus $MG^TM^{-1} = G$ for some $M \in \mathrm{GL}(n,R)$. Now Proposition 6.18 applies. □

Definition 6.22. For a permutation $\sigma \in S_n$ and $A \in \mathrm{Mat}(n, R)$ we will denote by $A\sigma$ the matrix that is obtained by permuting the columns of A according to σ, that is if $(A)_i$ is the ith column of A then $(A)_{\sigma(i)}$ is the ith column of $A\sigma$. Similarly, we define σA the matrix that is obtained by permuting the rows of A according to σ. Let $\sigma := \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix}$. The matrix $J := I_n\sigma$ is called the *exchange matrix*. It is easy to see that $J = J^{-1} = J^T$.

Now we show that the orbits under the action of the group of all invertible $n \times n$ lower triangular matrices $\mathrm{LT}(n, R)$ is an F-partition with respect to a suitably chosen isomorphism between R^n and $\widehat{R^n}$.

Proposition 6.23. *Let U be any subgroup of $\mathcal{U}(R)$. Then the $\mathrm{LT}_U(n, R)$-orbits form an F-partition with respect to isomorphism $x \mapsto \Phi_{xJ}$. Thus in particular, the $\mathrm{LT}(n, R)$-orbits form an F-partition.*

Proof. In view of Proposition 6.18 we need to show that for every $A \in \mathrm{LT}_U(n, R)$ we have $JA^TJ^{-1} \in \mathrm{LT}_U(n, R)$. Notice that $\det(JA^TJ^{-1}) = \det(A)$. So, to show that $JA^TJ^{-1} = JA^TJ \in \mathrm{LT}_U(n, R)$ it is enough to show that JA^TJ is lower triangular with the diagonal elements being mapped to the diagonal. The following picture shows that JA^TJ is obtained by reflecting the entries of A about the anti-diagonal.



Therefore JA^TJ is in $\mathrm{LT}_U(n, R)$, as we desired. □

One may notice that if R is a field then $\mathrm{LT}_{\{1\}}(n, R)$ is a Sylow subgroup of $\mathrm{GL}(n, R)$ so that in this case the last result is already covered by Corollary 6.21.

Now one can easily give an example showing that the notion of an F-partition depends on the isomorphism between R^n and $\widehat{R^n}$.

Example 6.24. On $\mathbb{F}_2$ the map $\chi(a) := (-1)^a$ is an admissible character. For the subgroup $\mathrm{LT}(2, \mathbb{F}_2)$, the orbits containing $e_1 = (1, 0)$ and $e_2 = (0, 1)$ are given by $\mathcal{O}_1 := \{(1, 0)\}$ and $\mathcal{O}_2 := \{(0, 1), (1, 1)\}$, respectively. Consider $\sum_{y\in\mathcal{O}_1} \Phi_y(z)$ for $z \in \mathcal{O}_2$. Then $\Phi_{(1,0)}((0, 1)) = \chi(0) = 1$ while $\Phi_{(1,0)}((1, 1)) = \chi(1) = -1$. Therefore the $\mathrm{LT}(2, \mathbb{F}_2)$-orbits do not form an F-partition with respect to the isomorphism $x \mapsto \Phi_x$. But according to Proposition 6.23 they form an F-partition with respect to isomorphism $x \mapsto \Phi_{xJ}$.

6.3 Subgroups with the Local-Global Property

In this section we will show that the local-global property is satisfied by several subgroups G of $\mathrm{GL}(n, R)$.

We start with some technical lemma that we will use several times in the future.

Lemma 6.25. *Let G be a subgroup of $\mathrm{GL}(n,R)$ such that the G-orbits form an F-partition, say $\mathcal{Q}$, on R^n with respect to the isomorphism $x \mapsto \Phi_x$. Let $f : \mathcal{C} \to \mathcal{C}'$ be a local G-map between two codes $\mathcal{C}$ and $\mathcal{C}'$ in R^n. Then for any $Q \in \mathcal{Q}$ and any $x \in \mathcal{C}$*

$$\sum_{y \in Q} \chi(\langle y, f(x)\rangle) = \sum_{y \in Q} \chi(\langle y, x\rangle).$$

Moreover, for every $z \in R^n$ there is a matrix $A_z \in G$ such that

$$\langle z, f(x)\rangle = \langle x, zA_z\rangle$$

for all $x \in \mathcal{C}$.

Proof. Since f is a local G-map, clearly $x \sim_{\mathcal{Q}} f(x)$ for every $x \in \mathcal{C}$. It follows that for any $Q \in \mathcal{Q}$

$$\sum_{y \in Q} \chi(\langle y, f(x)\rangle) = \sum_{y \in Q} \chi(\langle y, x\rangle) \tag{6.1}$$

for all $x \in \mathcal{C}$. This proves the first part.

For a fixed $y \in \mathcal{C}$, the assignments $x \mapsto \langle y, x\rangle$ and $x \mapsto \langle y, f(x)\rangle$ are linear maps from $\mathcal{C}$ to R. It follows that $\chi(\langle y, -\rangle)$ and $\chi(\langle y, f(-)\rangle)$ are characters on $\mathcal{C}$. From (6.1) we have the identity

$$\sum_{y \in Q} \chi(\langle y, f(-)\rangle) = \sum_{y \in Q} \chi(\langle y, -\rangle)$$

of characters on $\mathcal{C}$.

Let $z \in R^n$. Then z is contained in some partition set Q in $\mathcal{Q}$. By choosing $y = z$ on the left hand side, Corollary 2.17 implies that there is a $zA_z \in Q$ for some $A_z \in G$, such that

$$\chi(\langle z, f(-)\rangle) = \chi(\langle zA_z, -\rangle) \in \widehat{\mathcal{C}}.$$

Since χ is an admissible character, we obtain from by Proposition 4.1(2)

$$\langle z, f(-)\rangle = \langle zA_z, -\rangle = \langle -, zA_z\rangle$$

as maps from $\mathcal{C}$ to R. Now the conclusion follows. □

Remark 6.26. If in the previous lemma, the G-multiplicative partition is an F-partition with respect to the isomorphism $x \mapsto \Phi_{xM}$ for some $M \in \mathrm{GL}(n,R)$, it is not difficult to adapt the proof to show that for every $z \in R^n$ there is an $A_z \in G$ such that

$$\langle zM, f(x)\rangle = \langle zA_zM, x\rangle$$

for all $x \in \mathcal{C}$.

Now we can show that $\mathcal{M}_U(n,R)$ has the local-global property, as we stated already in Theorem 6.2. This gives us a new proof of Theorem 4.9.

Proof of Theorem 6.2. Let $f : \mathcal{C} \to \mathcal{C}'$ be a local $\mathcal{M}_U(n, R)$ map. By Corollary 6.20 the partition $\mathcal{Q}$ induced by the $\mathcal{M}_U(n, R)$-multiplicative orbits is an F-partition with respect to the isomorphism $x \mapsto \Phi_x$. Let $Q \in \mathcal{Q}$ be the partition set that contains e_1. Hence all the standard basis vectors $e_1, \ldots, e_n$ are in Q. By Lemma 6.25 we have

$$\sum_{y \in Q} \chi(\langle y, f(x)\rangle) = \sum_{y \in Q} \chi(\langle y, x\rangle) \tag{6.2}$$

for all $x \in \mathcal{C}$. Denote the coordinate functions of f by $f_1, \ldots, f_n$. Using again Lemma 6.25 for $z = e_1$ we see that there exists an $A_1 \in \mathcal{M}_U(n, R)$ such that for all $x \in \mathcal{C}$

$$f_1(x) = \langle e_1, f(x)\rangle = \langle x, e_1 A_1\rangle = \langle x, \alpha_1 e_{\tau(1)}\rangle = \alpha_1 x_{\tau(1)}$$

where $\alpha_1 \in U$ and $\tau(1)$ is some index in $\{1, 2, \ldots, n\}$. Notice that

$$\sum_{\alpha \in U} \chi(\langle \alpha e_1, f(x)\rangle) = \sum_{\alpha \in U} \chi(\alpha f_1(x)) = \sum_{\alpha \in U} \chi(\langle \alpha\alpha_1 e_{\tau(1)}, x\rangle) = \sum_{\beta \in U} \chi(\langle \beta e_{\tau(1)}, x).$$

Notice that Q contains all vectors αe_i for all $\alpha \in U$ and $i = 1, \ldots, n$. Let $Q_i := \{\alpha e_i \mid \alpha \in U\}$. By the above the equation, then (6.2) can be reduced into

$$\sum_{y \in Q \setminus Q_1} \chi(\langle y, f(x)\rangle) = \sum_{y \in Q \setminus Q_{\tau(1)}} \chi(\langle y, x\rangle). \tag{6.3}$$

By repeating the argument for $z = e_2 \in Q \setminus Q_1$, there is $\alpha_2 \in U$ and an index $\tau(2)$ such that $\alpha_2 e_{\tau(2)} \in Q \setminus Q_{\tau(1)}$ and $f_2(x) = \langle \alpha_2 e_{\tau(2)}, x\rangle = \alpha_2 x_{\tau(2)}$. Since $e_{\tau(1)} \notin Q \setminus Q_{\tau(1)}$, $\alpha_2 e_{\tau(2)}$ is not a multiple of $e_{\tau(1)}$. Thus $\tau(2) \neq \tau(1)$.

By continuing in this fashion, we obtain for all $i = 1, \ldots, n$ a unit $\alpha_i \in U$ such that $f_i(x) = \alpha_i x_{\tau(i)}$ where $\tau(1), \tau(2), \ldots, \tau(n)$ are distinct elements of $\{1, 2, \ldots, n\}$. But this shows that f is a global $\mathcal{M}_U(n, R)$-map. □

To see the connection between this proof and the proof of Theorem 4.9, notice that when Q is the partition set that contains $e_1, \ldots, e_n$, (6.2) is equivalent to (4.2), which was a major milestone in that proof. As we can see now, we arrive at (6.2) more naturally as a consequence of the fact that the $\mathcal{M}_U(n, R)$-orbits form an F-partition.

Without difficulty we can carry over the above argument and establish the local-global property for the group $\Delta_U(n, R)$.

Theorem 6.27. *For any subgroup U of $\mathcal{U}(R)$ the group $\Delta_U(n, R)$ satisfies the local-global property on R^n.*

With this result we can now give a characterization of support-preserving maps. For $x \in R^n$ we define the support of x to be the set of all indices i for which the ith component of x is nonzero, that is $\mathrm{Supp}(x) := \{i \mid x_i \neq 0\}$. Notice that if R is a field, then $\mathrm{Supp}(x) = \mathrm{Supp}(y)$ if and only if $y = xD$ for some nonsingular diagonal matrix D over R. So a map $f : \mathcal{C} \to \mathcal{C}'$ preserves the support if and only if f is a local $\Delta(n, R)$-map. Hence Theorem 6.27 immediately leads to the the following result.

Proposition 6.28. *Let R be a field. Let $f : \mathcal{C} \to \mathcal{C}'$ be a linear isomorphism preserving the support. Then f is a global $\Delta(n, R)$-map.*

If R is not a field, there exist $x, y \in R^n$ such that $\mathrm{Supp}(x) = \mathrm{Supp}(y)$ but $y \neq xD$ for all $D \in \Delta(n, R)$. For example, let $R = \mathbb{Z}_6$. Clearly $\mathrm{Supp}(0, 2) = \mathrm{Supp}(0, 3)$. But since $2\alpha = 3$ has no solution $\alpha \in \mathbb{Z}_6$, there is no invertible diagonal 2×2 matrix D such that $(0, 2)D = (0, 3)$. But we also see that any linear map f that satisfies $f((0, 2)) = (0, 3)$ is not support-preserving since $\mathrm{Supp}(3(0, 2)) \neq \mathrm{Supp}(3(0, 3))$. So even in the case that R is not a field, Proposition 6.28 may still hold and in fact it does for general finite admissible rings.

Theorem 6.29. *Let R be a finite commutative admissible ring. Let $f : \mathcal{C} \to \mathcal{C}'$ be a support-preserving linear isomorphism. Then f is a global $\Delta(n, R)$-map.*

Proof. Recall that a finite commutative admissible ring is self-injective (see [43, Remark 3.11]). Hence by Lam [23, Theorem 15.1] R satisfies the double annihilator property, that is for any ideal I in R, $\mathrm{ann}(\mathrm{ann}(I)) = I$. Fix an $x \in \mathcal{C}$. Since f is linear and preserves the support, for any $j = 1, \ldots, n$ we have $\alpha x_j = 0$ if and only if $\alpha f_j(x) = 0$ for any $\alpha \in R$. It follows that for all $j = 1, \ldots, n$

$$\mathrm{ann}(Rx_j) = \mathrm{ann}(x_j) = \mathrm{ann}(f_j(x)) = \mathrm{ann}(Rf_j(x)).$$

By the double annihilator property we have

$$Rx_j = \mathrm{ann}(\mathrm{ann}(Rx_j)) = \mathrm{ann}(\mathrm{ann}(Rf_j(x)) = Rf_j(x).$$

Now by Lemma 4.6, there is an $\alpha_j \in \mathcal{U}(R)$ such that $f_j(x) = \alpha_j x_j$. Hence $f(x) = x \cdot \mathrm{diag}(\alpha_1, \ldots, \alpha_n)$ and we conclude that f is a local $\Delta(n, R)$-map. By the local-global property of $\Delta(n, R)$ (Theorem 6.27), we conclude that f is a global $\Delta(n, R)$-map. □

One should observe that the support may be regarded as the desymmetrized version of the Hamming weight: while the latter counts the number of nonzero entries, the support keeps track of the position of the nonzero entries. As we have just seen it is not too difficult to show that a support-preserving linear map is a local, and hence global, $\Delta(n, R)$-map. In contrast, proving that a Hamming-weight preserving map is a local $\mathcal{M}(n, R)$-map, is much more difficult (unless R is a field). Attempting this leads essentially to the same proof as Theorem 4.7 which then shows right away that the map is globally monomial.

Next we will show that $\mathrm{LT}(n, R)$, the group of all invertible lower triangular matrices, satisfies the local-global property. This group is closely related to the Rosenbloom-Tsfasman metric, which has been introduced by Rosenbloom and Tsfasman in [34] and is defined as follows. Let $\mathbb{F}$ be a finite field. For $x = (x_1, \ldots, x_n) \in \mathbb{F}^n$ the Rosenbloom-Tsfasman weight (RT-weight) is given by

$$\rho(x) := \begin{cases} 0, & x = 0 \\ \max\{i \mid x_i \neq 0\}, & \text{otherwise.} \end{cases} \tag{6.4}$$

One can check that the distance between two vectors x, y defined by $d(x,y) := \rho(x-y)$ is a metric on $\mathbb{F}^n$. This metric becomes most powerful for matrices, to which it generalizes straightforwardly by simply taking the sum of $\rho(x)$ over all rows x of the matrix (see also [10]). In the interesting paper [37], Skriganov showed that for a given matrix code $\mathcal{C}$ (that is, a subspace in $\mathbb{F}^{s\times n}$ for some fixed n, s), the orbit of $\mathcal{C}$ under the action of the RT-weight-preserving group contains codes with large Hamming distance; under certain conditions on $\mathcal{C}$ it even contains codes meeting the Gilbert Varshamov bound. This way, the Rosenbloom-Tsfasman-metric is helpful for detecting codes with large Hamming distance. Lee [28] proved that the RT-weight-preserving automorphisms of the entire space $\mathbb{F}^n$ (and even on the matrix space $\mathbb{F}^{s\times n}$) are exactly given by the invertible lower triangular matrices. This can be regarded as a special case of our Theorem 6.31 below, where we show that every RT-weight-preserving isomorphism between codes in $\mathbb{F}^n$ is given by an invertible lower triangular matrix. In Theorem 6.34 we also extend this result to codes over admissible rings.

In order to see the connection between the RT-weight and $\mathrm{LT}(n,R)$ we first prove the following lemma. This lemma is known to Dougherty ([10]).

Lemma 6.30. *Let $x, y \in \mathbb{F}^n$. Then $\rho(x) = \rho(y)$ if and only if there exists a matrix $A \in \mathrm{LT}(n,\mathbb{F})$ such that $y = xA$.*

Proof. ($\Leftarrow$) Let $A = (a_{ij}) \in \mathrm{LT}(n,\mathbb{F})$. We are going to show that $\rho(x) = \rho(xA)$. Note that $a_{ij} = 0$ for all $i < j$ and $x_i = 0$ for all $i > \rho(x)$. It follows that the jth entry of xA is given by

$$\sum_{i=1}^{n} x_i a_{ij} = \sum_{i=j}^{n} x_i a_{ij} = \sum_{i=j}^{\rho(x)} x_i a_{ij}. \tag{6.5}$$

So for $j > \rho(x)$ we have $(xA)_j = 0$ and for $j = \rho(x)$ the jth entry of xA is $x_j a_{jj} \neq 0$ (since $a_{jj} \neq 0$ and $x_j \neq 0$). It follows that $\rho(xA) = \rho(x)$.

($\Rightarrow$) Suppose $x, y \in \mathbb{F}^n$ such that $\rho(x) = \rho(y) = l$. We will construct a matrix $A = (a_{ij}) \in \mathrm{LT}(n,\mathbb{F})$ such that $xA = y$. To make A lower triangular, first set $a_{ij} = 0$ for $i < j$. We see from (6.5) that in order to have $xA = y$ for every $j = 1, \dots l$ we need to solve the equation

$$y_j = \sum_{i=j}^{l} x_i a_{ij} = \sum_{i=j}^{l-1} x_i a_{ij} + x_l a_{lj} \tag{6.6}$$

for a_{ij}. Set arbitrary nonzero values to all a_{ij} where $i \geq j$ and $i \neq l$. By doing this we ensure in particular that all main diagonal entries of A are nonzero. For the rest, by setting $a_{lj} = x_l^{-1}\left(y_j - \sum_{i=j}^{l-1} x_i a_{ij}\right)$, the a_{ij} entries satisfy the equation (6.6). □

Below we will show that $\mathrm{LT}(n,\mathbb{F})$ satisfies the local-global property. Thus, we obtain the following result.

Theorem 6.31. *If $f : \mathcal{C} \to \mathcal{C}'$ is an isometry between two codes in $\mathbb{F}^n$ with respect to the Rosenbloom-Tsfasman metric, then f is a global $\mathrm{LT}(n,\mathbb{F})$-map.*

Proof. By Lemma 6.30, f is a local $\mathrm{LT}(n,\mathbb{F})$-map. Therefore, this is a special case of Theorem 6.32 below. □

In order to prove the local-global property for the group $\mathrm{LT}(n,R)$, where R is any admissible ring, we will make use of the ring of all $n \times n$ lower triangular matrices over R, which will be denoted by $\mathrm{RLT}(n,R)$. Clearly $\mathrm{RLT}(n,R)$ is a subring of $\mathrm{Mat}(n,R)$ and the group of units of $\mathrm{RLT}(n,R)$ is $\mathrm{LT}(n,R)$. Now we are ready to prove the local-global property of $\mathrm{LT}(n,R)$.

Theorem 6.32. *The group* $\mathrm{LT}(n,R)$ *satisfies the local-global property.*

Proof. Let $f : \mathcal{C} \to \mathcal{C}'$ be a local $\mathrm{LT}(n,R)$-map. By Proposition 6.23 the $\mathrm{LT}(n,R)$-orbits form an F-partition with respect to the isomorphism $x \mapsto \Phi_{xJ}$. By Lemma 6.25 and Remark 6.26 for every $z \in R^n$ there exists a matrix $A_z \in \mathrm{LT}(n,R)$ such that

$$\langle zJ, f(x)\rangle = \langle x, zA_zJ\rangle \tag{6.7}$$

for every $x \in \mathcal{C}$. For each $i = 1,\dots,n$ let $z_i = e_iJ^{-1}$. Then by (6.7) there exists a matrix $A_i \in \mathrm{LT}(n,R)$ such that

$$f_i(x) = \langle (e_iJ^{-1})J, f(x)\rangle = \langle x, e_iJ^{-1}A_iJ\rangle = x(J^{-1}A_iJ)^Te_i^T. \tag{6.8}$$

By Proposition 6.23, $B_i := (J^{-1}A_iJ)^T \in \mathrm{LT}(n,R)$. Let $B \in \mathrm{RLT}(n,R)$ be the matrix whose ith column is the column vector $B_ie_i^T$, that is, the ith column of B_i. Then we obtain from (6.8)

$$f(x) = (f_1(x),\dots,f_n(x)) = (xB_1e_1^T,\dots,xB_ne_n^T) = xB. \tag{6.9}$$

for all $x \in \mathcal{C}$, and it remains to show that B is invertible, that is $B \in \mathrm{LT}(n,R)$. In this particular case, this can be seen directly from the diagonal of B. However, we will give the following argument which then will be further exploited after the proof for other subgroups.

Let G and G' be generator matrices for $\mathcal{C}$ and $\mathcal{C}'$ such that $\mathrm{row}_i(G') = f(\mathrm{row}_i(G))$. From (6.9) we conclude that $GB = G'$. Applying the same argument to the inverse map $g : \mathcal{C}' \to \mathcal{C}$ of f, we get a matrix C such that $G = G'C$. Since $GB = G'$ and $G = G'C$, the two cyclic right $\mathrm{RLT}(n,R)$-modules $\langle G\rangle$ and $\langle G'\rangle$ are equal. By Lemma 4.6 there is a unit M in $\mathrm{RLT}(n,R)$ such that $G' = GM$. But this means that M is in $\mathrm{LT}(n,R)$, and therefore f is a global $\mathrm{LT}(n,R)$-map. □

Before we will extend the ideas of the last paragraph to further groups let us first present the following generalization of the first part of the proof.

Remark 6.33. Let U be any subgroup of $\mathcal{U}(R)$. Then the group $\mathrm{LT}_U(n,R)$ satisfies the local-global property. This follows from the same line of arguments as in the previous proof by noticing that the diagonal elements of the matrix B are now in U.

We will use the idea of the above proof in two instances. First, we will use the argument of the last paragraph in the proof of Theorem 6.32 to generalize Theorem 6.31 to admissible rings. Thereafter, we will analyze the above proof to study for which subrings S of $\mathrm{Mat}(n, R)$ the set of all units in S (which is a subgroup of $\mathrm{GL}(n, R)$) satisfies the local-global property.

First we prove the following. We define the Rosenbloom-Tsfasman-metric as in (6.4) for vectors over an admissible ring.

Theorem 6.34. *Let R be an admissible ring. If $f : \mathcal{C} \to \mathcal{C}'$ is an isometry between two codes in R^n with respect to the Rosenbloom-Tsfasman metric, then f is a global $\mathrm{LT}(n, R)$-map.*

Proof. Due to Theorem 6.32 it suffices to show that f is a local $\mathrm{LT}(n, R)$-map. Fix any $x \in \mathcal{C}$. Consider the cyclic right $\mathrm{RLT}(n, R)$-modules generated by x and $f(x)$. If we can show that there exists a matrix $A = (a_{ij}) \in \mathrm{RLT}(n, R)$ such that $f(x) = xA$, then the last paragraph of the proof of Theorem 6.32 establishes that f is a local $\mathrm{LT}(n, R)$-map.

Let $y := f(x)$ and $l := \rho(x) = \rho(y)$. To make A lower triangular, set $a_{ij} = 0$ for $i < j$. By (6.6), in order to have $y = xA$ for every $j = 1, \ldots, l$, we need $a_{jj}, \ldots, a_{lj} \in R$ such that $y_j = \sum_{i=j}^{l} x_i a_{ij}$. The existence of such $a_{jj}, \ldots, a_{lj} \in R$ is guaranteed if we can show that $y_j \in Rx_j + \ldots + Rx_l$.

Take $\alpha \in \mathrm{ann}(Rx_j + \ldots + Rx_l)$. Then $\alpha x_i = 0$ for $i \geq j$. It follows that $\rho(\alpha x) < j$. Since f is RT weight-preserving, we have $\rho(\alpha f(x)) = \rho(\alpha y) < j$ as well. In particular $\alpha y_j = 0$. It follows that $\mathrm{ann}(Rx_j + \ldots + Rx_l) \subset \mathrm{ann}(Ry_j)$. Now by the double annihilator property of ideals in R, we have

$$Ry_j = \mathrm{ann}(\mathrm{ann}(Ry_j)) \subset \mathrm{ann}(\mathrm{ann}(Rx_j + \ldots + Rx_l)) = Rx_j + \ldots + Rx_l.$$

Therefore $y_j \in Rx_j + \ldots + Rx_l$ and we conclude that f is a local $\mathrm{LT}(n, R)$-map. By the local-global property of $\mathrm{LT}(n, R)$ (Theorem 6.32), f is a global $\mathrm{LT}(n, R)$-map. □

Now we return to the general question of which subgroups satisfy the local-global property. The proof of Theorem 6.32 works due to two particular properties of the subring $\mathrm{RLT}(n, R)$:

(1) The group of units of $\mathrm{RLT}(n, R)$, which is $\mathrm{LT}(n, R)$, satisfies the hypothesis of Proposition 6.18, that is, there is an $M \in \mathrm{GL}(n, R)$ such that $MA^TM^{-1} \in \mathrm{LT}(n, R)$ for every $A \in \mathrm{LT}(n, R)$. This property makes sure that the $\mathrm{LT}(n, R)$-orbits form an F-partition, which in turn implies the identities (6.7) and (6.8).

(2) If $A_1, \ldots, A_n \in \mathrm{RLT}(n, R)$ and A is defined as the matrix whose ith column is the ith column of A_i, then $A \in \mathrm{RLT}(n, R)$. This property results in the matrix B in (6.9).

We coin the following terminology for subrings satisfying the two conditions above.

Definition 6.35. Let S be a subring of $\mathrm{Mat}(n, R)$ and let $\mathcal{U}(S)$ be the units of S. Let $M \in \mathrm{GL}(n, R)$. The subring S is called *M-constructible* if $M\mathcal{U}(S)^T M^{-1} \subseteq \mathcal{U}(S)$ and if for any $A_1, \ldots, A_n \in S$, the matrix A that is obtained by choosing the ith column of A to be the ith column of A_i is an element of S.

Now one observes that the proof of Theorem 6.32 generalizes straightforwardly to M-constructible rings and their groups of units. Thus we arrive at the following.

Theorem 6.36. *Let S be an M-constructible subring of $\mathrm{Mat}(n, R)$. Then $\mathcal{U}(S)$ satisfies the local-global property.*

It is easy to see that $\mathrm{Mat}(n, R)$ is M-constructible for any $M \in \mathrm{GL}(n, R)$. Moreover, the ring of all diagonal matrices $R\Delta(n, R)$ is both I and J-constructible, and the ring of all upper triangular matrices $\mathrm{RUT}(n, R)$ is J-constructible. Denote the set of all units of $\mathrm{RUT}(n, R)$ by $\mathrm{UT}(n, R)$.

By Theorem 6.36 we recover our results from Proposition 6.27 (for $U = \mathcal{U}(R)$) and Theorem 6.32 and also we obtain the following.

Corollary 6.37. $\mathrm{GL}(n, R)$ *satisfies the local-global property.*

Two vectors $x, y \in R^n$ belong to the same $\mathrm{GL}(n, R)$-orbit if and only if the ideals $\langle x_1, \ldots, x_n\rangle, \langle y_1, \ldots, y_n\rangle$ are the same. For $x \in R^n$ let $I(x) := \langle x_1, \ldots, x_n\rangle$ be the ideal in R generated by the components of x. Hence any global $\mathrm{GL}(n, R)$-map f preserves this ideal, i.e., $I(x) = I(f(x))$ for all $x \in R^n$.

Let us briefly relate the last result to properties of admissible rings. Recall that the finite commutative admissible ring R is self-injective. Thus R^n is an injective module, and this means that any injective map $g : \mathcal{C} \to R^n$, where $\mathcal{C}$ is a code in R^n, can be extended to a map $\tilde{g} : R^n \to R^n$. However, it is not guaranteed that $\tilde{g}$ is an isomorphism. According to the above corollary if we even have a local $\mathrm{GL}(n, R)$-map $f : \mathcal{C} \to R^n$ (note that f is in particular injective), then f can be extended to an isomorphism $\tilde{f} : R^n \to R^n$.

Here are more examples of M-constructible rings.

Example 6.38. Let $\mathrm{RCH}(n, R)$ be the set of all $n \times n$ checkerboard matrices $A = (a_{ij})$ where $a_{ij} = 0$ if $i + j$ is odd. It is easy to see that $\mathrm{RCH}(n, R)$ is an I (and also J)-constructible ring. By Theorem 6.36, the group of all invertible checkerboard

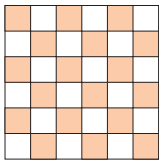


Figure 6.1: 6×6 checkerboard matrix

matrices, denoted by $\mathrm{CH}(n, R)$, satisfies the local-global property.

Example 6.39. Let $\mathrm{RX}(n, R)$ be the set of all $n \times n$ X-shaped matrices, that is for any $A \in \mathrm{RX}(n, R)$ all entries of A that are not on the diagonal or anti-diagonal are zero. One can verify that $\mathrm{RX}(n, R)$ is an I and J-constructible ring. Therefore the group $X(n, R)$ of all invertible matrices in $\mathrm{RX}(n, R)$ satisfies the local-global property.

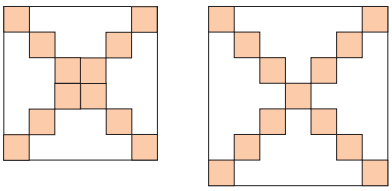


Figure 6.2: 6×6 and 7×7 X-shaped matrix

The following is a more general construction of M-constructible rings. Given $n_1, n_2 \in \mathbb{N}$. Consider the group $H := \mathrm{diag}(\mathrm{GL}(n_1, R), \mathrm{LT}(n_2, R))$ consisting of all block diagonal matrices of the form $\mathrm{diag}(A_1, A_2)$ where $A_1 \in \mathrm{GL}(n_1, R)$, $A_2 \in \mathrm{LT}(n_2, R)$. Notice that H is the group of units of the ring

$$S := \mathrm{diag}(\mathrm{Mat}(n_1, R), \mathrm{RLT}(n_2, R)),$$

which is a subring of $\mathrm{Mat}(n, R)$, where $n = n_1 + n_2$. It is not difficult to see that S is $\mathrm{diag}(I, J)$-constructible. Hence H satisfies the local-global property. Generalizing this observation we arrive at the following result.

Theorem 6.40. *(1) Let S_i be an M_i-constructible subring of $\mathrm{Mat}(n_i, R)$ for $i = 1, \ldots, t$. Put $N := n_1 + \ldots + n_t$. Then $\mathrm{diag}(S_1, \ldots, S_t)$ is a $\mathrm{diag}(M_1, \ldots, M_t)$-constructible subring of $\mathrm{Mat}(N, R)$. As a consequence, the subgroup of $\mathrm{Mat}(N, R)$ consisting of all block diagonal matrices of the form $\mathrm{diag}(A_1, \ldots, A_t)$ where $A_i \in \mathcal{U}(S_i)$, satisfies the local-global property.*

(2) Let S be an M-constructible subring of $\mathrm{Mat}(n, R)$ and let $t \in \mathbb{N}$. The subring of $\mathrm{Mat}(tn, R)$ consisting of all matrices of the form

$$A := \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1t} \\ & A_{22} & \cdots & A_{2t} \\ & & \ddots & \vdots \\ & & & A_{tt} \end{pmatrix}, \tag{6.10}$$

where $A_{ii} \in S$ for $i = 1, \ldots, t$ and A_{ij} is any matrix in $Mat(n, R)$, is an $\hat{M}$-constructible subring of $\mathrm{Mat}(tn, R)$, where $\hat{M} \in GL(tn, R)$ is the block-anti-diagonal matrix with M along the anti-diagonal. As a consequence, the subgroup of $\mathrm{Mat}(tn, R)$ consisting of all upper block triangular matrices as in (6.10) and where $A_{ii} \in \mathcal{U}(S)$, satisfies the local-global property.

Proof. Part (1) is obvious. As for (2), notice that $\hat{M} = \mathrm{diag}(M, \ldots, M)\hat{J}$, where $\hat{J}$ is the block-anti-diagonal matrix with I_n along the anti-diagonal. As in the proof of Theorem 6.23, one observes that conjugation of A^T, where A is as in (6.10), is a reflection about the anti-diagonal (along with a block-wise transposition). Thus, conjugation with $\mathrm{diag}(M, \ldots, M)$ leads to the desired result. □

Example 6.38 and Example 6.39 are in a certain sense special cases of Theorem 6.40. To see this we need the following result.

Proposition 6.41. *Let G be a subgroup of $\mathrm{GL}(n, R)$ that satisfies the local-global property. Then each conjugate $G^P := PGP^{-1}$, where $P \in \mathrm{GL}(n, R)$, also satisfies the local-global property.*

Proof. Let $f : \mathcal{C} \to \mathcal{C}'$ be a local G^P-map. Then for any $x \in \mathcal{C}$ there is an $A_x \in G$ such that $f(x) = x(PA_xP^{-1})$. It follows that $f(x)P = xPA_x$ for all $x \in \mathcal{C}$. Now define a map $g : \mathcal{C}P \to \mathcal{C}'P$ by $g(xP) := f(x)P$. Notice that g is linear and $g(xP) = xPA_x$. Hence g is a local G-map. By the local-global property of G, there exists a matrix $A \in G$ such that $g(xP) = xPA$ for all $x \in \mathcal{C}$. It follows that

$$f(x) = g(xP)P^{-1} = xPAP^{-1} \text{ for all } x \in \mathcal{C},$$

and thus f is a global G^P-map. □

Consider again Examples 6.38 and 6.39. A matrix $A \in \mathrm{RX}(6, R)$ has the form as on the left hand side of Figure 6.2. Now for $P^{-1} := \begin{pmatrix} e_1 & e_6 & e_2 & e_5 & e_3 & e_4 \end{pmatrix}$ we obtain that PAP^{-1} is a block diagonal matrix and an element of

$$\mathrm{diag}(\mathrm{Mat}(2, R), \mathrm{Mat}(2, R), \mathrm{Mat}(2, R)).$$

Similarly for all 6×6 checkerboard matrices B as in Figure 6.1, one can find a permutation matrix $Q \in \mathrm{GL}(6, R)$ such that QAQ^{-1} is a block diagonal matrix of the form $\mathrm{diag}(B_1, B_2)$ where $B_1, B_2 \in \mathrm{Mat}(3, R)$.

Chapter 7 Summary and Further Research

In this chapter we summarize our work of the previous two chapters, address some problems that remain still open, and propose some directions for further research.

Chapter 5 and Chapter 6 mainly contain generalizations of two important theorems due to Wood in Chapter 4. In Chapter 5, we generalize the MacWilliams equivalence theorem over admissible rings (Theorem 4.7) to general weight functions. While the result does not hold true in general (see Example 3.8), we obtained a necessary and sufficient condition for rational valued weight functions to satisfy the equivalence theorem (see Theorem 5.4 and 5.6). Using this condition and exploiting the structure of circulant matrices, we recover the result of Wood (Theorem 5.27) which shows that the Lee weight satisfies the equivalence theorem for residue fields $\mathbb{Z}_N$, where N is a prime of the form $N = 2p + 1$ and where p is also prime. Furthermore, we proved the new result that the Lee weight also satisfies the equivalence theorem for residue fields $\mathbb{Z}_N$, where $N = 4p+1$ and again N and p are both prime (Theorem 5.28). While we are not able to show that the Lee weight satisfies the condition in Theorem 5.4 in general (which would guarantee that it satisfies the equivalence theorem in all cases), this condition together with Proposition 5.24 allows us to check empirically that the Lee weight satisfies the equivalence theorem on all residue fields $\mathbb{Z}_N$ for the first 2010 prime numbers N. This leads us to believe that the equivalence theorem holds true for the Lee weight on all fields $\mathbb{Z}_N$ where N is prime. Yet, it is still open for $\mathbb{Z}_N$ even when N is prime.

In Chapter 6, we generalize the result in Theorem 4.9 by first realizing that a $\mathcal{P}_U$-isometry is exactly a local $\mathcal{M}_U(n, R)$-map. Then we can reformulate Theorem 4.9 in terms of a local-global property (Theorem 6.2). At that point it is natural to ask if the local-global property holds true for other subgroups G of $\mathrm{GL}(n, R)$ as well. As a motivation that this is a generalization in the right direction, we show that the famous Witt extension theorem can be rephrase in terms of the local-global property (Theorem 6.3).

We prove, among other things, that the groups $\Delta_U(n, R)$, $\mathrm{LT}_U(n, R)$ and $\mathrm{GL}(n, R)$ satisfy the local-global property (see Theorem 6.27, Theorem 6.32 and Corollary 6.37). We also show that the units of an M-constructible subring of $\mathrm{Mat}(n, R)$ satisfy the local-global property (Theorem 6.36). By reducing to the local case we are able to see that any linear isomorphism $f : \mathcal{C} \to \mathcal{C}'$ that preserves the support can be extended to a $\Delta(n, R)$-map (Theorem 6.28). Similarly, by reducing to the local case, we show that any linear isomorphism $f : \mathcal{C} \to \mathcal{C}'$ that preserves the Rosenbloom-Tsfasman weight can be extended to a $\mathrm{LT}(n, R)$-map (Theorem 6.34).

Let us now turn to some open problems. Recall that we gave another proof for Theorem 4.9 in Chapter 6, and the proof is independent from Theorem 4.7. Learning from the situation for support-preserving or RT-preserving isomorphisms, one may try to give another proof of the MacWilliams equivalence theorem for the Hamming weight by showing that any w_H-isometry $f : \mathcal{C} \to \mathcal{C}'$ is a local $\mathcal{M}(n, R)$-map. While this is obvious if R is a field, this is not clear for general admissible rings. Indeed, we

are able to show this only for principal ideal rings (so that in this case Theorem 6.2 implies that f is a monomial map and we have yet another proof of the MacWilliams equivalence theorem for the Hamming weight on principal ideal rings).

For a general weight function w on R with symmetry group $U = \mathrm{Sym}(w)$, we see similar connections. We know that $\mathcal{M}_U(n, R)$ satisfies the local-global property. If we are able to show that any w-isometry $f : \mathcal{C} \to \mathcal{C}'$ is a local $\mathcal{M}_U(n, R)$-map, then w satisfies the equivalence theorem. In fact, the condition in Theorem 5.4 tells us precisely which weights w make f a local $\mathcal{M}_U(n, R)$-map.

Let us now focus on a different aspect of our investigation. Notice that the support and the RT-weight, different from the Hamming weight on R^n, do not arise as an extension of a weight function on R. They are just functions from R^n to some set T. For a function $\varphi : R^n \to T$ we can consider the isomorphisms $f : \mathcal{C} \to \mathcal{C}'$ that preserves φ, i.e., $\varphi(x) = \varphi(f(x))$ for all $x \in \mathcal{C}$. Can one describe these maps explicitly in a similar way as w_H-preserving maps can be described as monomial maps? For this goal we do not want our φ to be too general and certainly need additional conditions on φ to stand a chance of deriving some interesting result and recover our previous results.

Note that all the functions w_H, support, and the RT-weight ρ (see (6.4)) have something in common. They are all closely related to the G-orbits of some subgroup G of $\mathrm{GL}(n, R)$ that has the local-global property. For $x, y \in R^n$ write $x \sim_G y$ if x and y belong to the same G-orbit. Using this notation, we can see the following: if $x \sim_{\mathcal{M}(n,R)} y$, then $w_H(x) = w_H(y)$; if $x \sim_{\Delta(n,R)} y$, then $\mathrm{Supp}(x) = \mathrm{Supp}(y)$; if $x \sim_{\mathrm{LT}(n,R)} y$, then $\rho(x) = \rho(y)$. It is known that the converse is not true in general (unless R is a field); see for instance the example right before Theorem 6.29. This leads to the following definition.

Definition 7.1. Let G be a subgroup of $\mathrm{GL}(n, R)$ that satisfies the local-global property and let T be a set. We say that $\varphi : R^n \to T$ is a *generalized weight on R^n with respect to G* if $\varphi(x) = \varphi(y)$ for all $x, y \in R^n$ that belong to the same G-orbit.

From this definition we clearly have that w_H, Supp and the RT-weight ρ are generalized weights on R^n with respect to $\mathcal{M}(n, R)$, $\Delta(n, R)$ and $\mathrm{LT}(n, R)$, respectively. Notice also that the Lee weight w_L studied in Section 5.4 is a generalized weight with respect to $\mathcal{M}_{\{\pm 1\}}(n, R)$.

We propose the following question to generalize the equivalence theorem.

Question 7.2. Let G be subgroup of $\mathrm{GL}(n, R)$ that satisfies the local-global property. Which generalized weight functions φ with respect to G have the property that every φ-preserving isomorphism $f : \mathcal{C} \to \mathcal{C}'$ extends to a G-map?

At this point it should be clear from our earlier work that the given linearity of f is essential.

We conjecture that the correct way to approach generalized weight functions φ is by considering the following equivalence relation. We say that two generalized weight functions with respect to G, say φ_1 and φ_2, belong to the same class if for all $x, y \in R^n$ we have $\varphi_1(x) = \varphi_1(y)$ if and only if $\varphi_2(x) = \varphi_2(y)$. That is, φ_1 and φ_2 induce the

same partition on R^n. Using this notion, the map $f : \mathcal{C} \to \mathcal{C}'$ is φ_1-preserving if and only if it is φ_2-preserving. Therefore φ_1 is a solution to Question 7.2 if and only if φ_2 is a solution as well.

Question 7.2 above is closely related and can be thought of as the natural continuation of Question 3.19. The generalized weight takes now the place of the map v in Question 3.19. We believe that the local-global property is helpful to approach this question.

Bibliography

[1] E. Artin. Geometric algebra. *Mir, Moscow*, 1969.

[2] H. Bass. K-theory and stable algebra. *Publications Mathématiques de l'IHES*, 22(1):5–60, 1964.

[3] E. Byrne, M. Greferath, and M.E. O´Sullivan. The linear programming bound for codes over finite Frobenius rings. *Designs, Codes and Cryptography*, 42(3):289–301, 2007.

[4] H.L. Claasen and R.W. Goldbach. A field-like property of finite rings. *Indagationes Mathematicae*, 3(1):11–26, 1992.

[5] W.E. Clark and D.A. Drake. Finite chain rings. In *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, volume 39, pages 147–153. Springer, 1973.

[6] I. Constantinescu and W. Heise. A metric for codes over residue class rings. *Problemy Peredachi Informatsii*, 33(3):22–28, 1997.

[7] L.E. Dickson. A new extension of dirichlets theorem on prime numbers. *Messenger of Math*, 33:155–161, 1904.

[8] H. Quang Dinh and S.R. López-Permouth. On the equivalence of codes over finite rings. *Appl. Algebra Engrg. Comm. Comput.*, 15:37–50, 2004.

[9] H.Q. Dinh and S.R. López-Permouth. On the equivalence of codes over rings and modules. *Finite Fields and Their Applications*, 10(4):615–625, 2004.

[10] S.T. Dougherty and M.M. Skriganov. Macwilliams duality and the Rosenbloom-Tsfasman metric. *Moscow Mathematical Journal*, 2(1):81–97, 2002.

[11] D.S. Dummit and R.M. Foote. *Abstract algebra*. Wiley, 2004.

[12] D.Y. Goldberg. A generalized weight for linear codes and a Witt-MacWilliams theorem. *Journal of Combinatorial Theory, Series A*, 29(3):363–367, 1980.

[13] M. Greferath and S.E. Schmidt. Finite-ring combinatorics and MacWilliams equivalence theorem. *Journal of Combinatorial Theory, Series A*, 92(1):17–28, 2000.

[14] R W Hamming. Error detecting and error correcting codes. *Bell System Technical Journal*, 29(2):147–160, 1950.

[15] A. R. Hammons, P. 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*, IT-40:301–319, 1994.

[16] Y. Hirano. On admissible rings. *Indagationes Mathematicae*, 8(1):55–59, 1997.

[17] T. Honold. Characterization of finite Frobenius rings. *Archiv der Mathematik*, 76(6):406–415, 2001.

[18] W.C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, Cambridge, 2003.

[19] I.M. Isaacs. *Character theory of finite groups*. Dover publications, 1994.

[20] V. Klee and S. Wagon. *Old and new unsolved problems in plane geometry and number theory*. Mathematical Association of America, 1991.

[21] T. Koshy. *Elementary number theory with applications*. Academic Press, 2002.

[22] I. Kra and S.R. Simanca. On circulant matrices. *Notices of the AMS*, 59(3), 2012.

[23] T.Y. Lam. *Lectures on modules and rings*, volume 189. Springer Verlag, 1999.

[24] T.Y. Lam. *A first course in noncommutative rings*. Graduate Text in Mathematics, Vol. 131. Springer, 2001.

[25] T.Y. Lam. *Introduction to quadratic forms over fields*, volume 67. Amer. Math. Society, 2005.

[26] S. Lang. *Algebra*. Graduate Text in Mathematics, Vol. 211. Springer-Verlag, 2002.

[27] C. Lee. Some properties of nonbinary error-correcting codes. *Information Theory, IRE Transactions on*, 4(2):77–82, 1958.

[28] K. Lee. The automorphism group of a linear space with the Rosenbloom-Tsfasman netric. *Europ. J. Combinatorics*, 24:607–612, 2003.

[29] F.J. MacWilliams. *Combinatorial problems of elementary abelian groups*. PhD thesis, Radcliffe College, 1962.

[30] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[31] A.A. Nechaev and T. Khonol'd. Weighted modules and representations of codes. *Problemy Peredachi Informatsii*, 35(3):18–39, 1999.

[32] H. Park, J. Park, and D. Kim. A criterion on primitive roots modulo p. *Journal-Korea Society For Industrial And Applied Mathematics*, 4(1):29–38, 2000.

[33] S. Roman. *Advanced linear algebra*, volume 135. Springer, 1992.

[34] M.Y. Rosenbloom and M.A. Tsfasman. Codes for the m-metric. *Problemy Peredachi Informatsii*, 33(1):55–63, 1997.

[35] J.P. Serre. *A course in arithmetic*, volume 7. Springer Verlag, 1973.

[36] J.P. Serre. *Linear representations of finite groups*, volume 42. Springer Verlag, 1977.

[37] M.M. Skriganov. On linear codes with large weights simultaneously for the Rosenbloom-Tsfasman and Hamming metrics. *J. Complexity*, 23:926–936, 2007.

[38] H.N. Ward and J.A. Wood. Characters and the equivalence of codes. *Journal of Combinatorial Theory, Series A*, 73(2):348–352, 1996.

[39] David W. Wilson. The On-Line Encyclopedia of Integer Sequences. http://oeis.org/A023212. Numbers n such that n and $4n + 1$ are both prime.

[40] J. A. Wood. The structure of linear codes of constant weight. *Trans. Americ. Math. Society*, 354:1007–1026, 2001.

[41] J. A. Wood. The extension theorem for the Lee and Euclidian weight. Preprint, 2009.

[42] J.A. Wood. Extension theorems for linear codes over finite rings. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 329–340, 1997.

[43] J.A. Wood. Duality for modules over finite rings and applications to coding theory. *American J. of Math.*, 121(3):555–575, 1999.

[44] J.A. Wood. Weight functions and the extension theorem for linear codes over finite rings. *Contemporary Mathematics*, 225:231–243, 1999.

[45] J.A. Wood. Factoring the semigroup determinant of a finite commutative chain ring. In *Coding theory, cryptography, and related areas: proceedings of an International Conference on Coding Theory, Cryptography, and Related Areas, held in Guanajuato, Mexico, in April 1998*, page 249. Springer Verlag, 2000.

[46] J.A. Wood. Code equivalence characterizes finite Frobenius rings. *Proc. Am. Math. Soc.*, 136(2):699, 2008.

[47] V. A. Zinoviev and T. Ericson. On Fourier-invariant partitions of finite abelian groups and the MacWilliams identity for group codes. *Problems Inform. Transmission*, 32:117–122, 1996.

Vita

Aleams Barra

Personal:
Born October 9, 1976 in Majalengka, Indonesia.

Education:

1998	S.Si., Institut Teknologi Bandung
2001	M.Si., Institut Teknologi Bandung
2004	Diploma Programme, International Center for Theoretical Physics
2007	M.Sc., University of Massachussets Amherst