2019

Equivalence of Classical and Quantum Codes

Tefjol Pllaha
University of Kentucky, tefjol.pllaha@gmail.com
Digital Object Identifier: https://doi.org/10.13023/etd.2019.014

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 needed written permission statement(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) which will be submitted to UKnowledge as Additional File.

I hereby grant to The University of Kentucky and its agents the irrevocable, non-exclusive, and royalty-free 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 an 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 thesis including all changes required by the advisory committee. The undersigned agree to abide by the statements above.

Tefjol Pllaha, Student

Dr. Heide Gluesing-Luerssen, Major Professor

Dr. Peter Hislop, Director of Graduate Studies

Equivalence of Classical and Quantum Codes

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
Tefjol Pllaha
Lexington, Kentucky

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

2019

ABSTRACT OF DISSERTATION

Equivalence of Classical and Quantum Codes

In classical and quantum information theory there are different types of error-correcting codes being used. We study the equivalence of codes via a classification of their isometries. The isometries of various codes over Frobenius alphabets endowed with various weights typically have a rich and predictable structure. On the other hand, when the alphabet is not Frobenius the isometry group behaves unpredictably. We use character theory to develop a duality theory of partitions over Frobenius bimodules, which is then used to study the equivalence of codes. We also consider instances of codes over non-Frobenius alphabets and establish their isometry groups. Secondly, we focus on quantum stabilizer codes over local Frobenius rings. We estimate their minimum distance and conjecture that they do not underperform quantum stabilizer codes over fields. We introduce symplectic isometries. Isometry groups of binary quantum stabilizer codes are established and then applied to the LU-LC conjecture.

KEYWORDS: Frobenius alphabets, isometries of codes, MacWillimas Extension Theorem, quantum stabilizer codes, LU-LC conjecture

Author's signature: Tefjol Pllaha

Date: January 31, 2019

Equivalence of Classical and Quantum Codes

By
Tefjol Pllaha

Director of Dissertation: Heide Gluesing-Luerssen

Director of Graduate Studies: Peter Hislop

Date: January 31, 2019

ACKNOWLEDGMENTS

I wholeheartedly thank my adviser Heide Gluesing-Luerssen for the continuous support and inspiration. No matter how hard I try, it is impossible to find the words to express my everlasting gratitude. In addition, I would like to thank Uwe Nagel and Jay Wood for their continuous support. I am indebted to Elton Pasku and Ridvan Peshkopia for encouraging me to pursue a PhD program. On the personal side, I thank Trish Freeman and her extended family for their southern hospitality. Thank you to all the friends for being there to play sports and games. Finally, I extend my gratitude to my parents and my sister. Thank you for your endless encouragement and support.

TABLE OF CONTENTS

LIST OF TABLES

Chapter 1 Introduction

1.1 Algebraic Coding Theory

Coding Theory deals with erroneously transmitted data over a noisy channel. Eliminating the noise is typically not an option. In fact the only efficient option is to make the data noise-proof, and this is done by adding redundancy. Coding Theory keeps under control the cost of the added redundancy and this is achieved by efficient coding tools that also allow efficient decoding algorithms. Classically, a **code $\mathcal{C}$ of length** n is an additive subgroup of $\mathbb{F}_2^n$. The binary field $\mathbb{F}_2$ is the **alphabet**, and thus, classically, $\mathcal{C}$ is a binary code. Elements of $\mathcal{C}$ are called **codewords**. A code is endowed with the **Hamming distance**, which counts the number of coordinates in which two codewords differ.

Algebraic Coding Theory considers codes with more structure, which in turn enables a wide range of tools and techniques. The alphabet is typically a finite field $\mathbb{F}_q$ and a code is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$, called a **linear** code. For a linear code one considers the **Hamming weight** of a codeword as the Hamming distance from the 0 codeword. In other words, the Hamming weight counts the number of nonzero coordinates of a codeword. The main invariant of a code is the **minimum distance**; it characterizes the error-correcting capabilities of the code. Therefore, the goal is to find codes with large minimum distance while keeping the size of the code under control. The advantage of linear codes is that the minimum distance coincides with the **minimum weight**.

The work of Hammons et al. [25] in 1994 showed that exceptionally good nonlinear binary codes can be viewed as linear codes over $\mathbb{Z}_4$ endowed with the **Lee weight**. Ever since, ring-linear coding has gained extensive attention both from a mathematical and engineering point of view. As we will see, generalizations of classical results led to the natural ring alphabet: Frobenius rings. One can generalize the idea even further. The alphabet can be taken to be a finite left (or right) R-module A, where R is a finite ring with identity. In this case a linear code is just a left submodule of A^n. The typical example is the matrix module alphabet. Another interesting special case is to consider field extensions E/F. In this context, the alphabet is ${}_FE$ and codes consist of F-linear subspaces of E^n. In the case $\mathbb{F}_{p^\ell}/\mathbb{F}_p$ we get the so-called **additive codes**. They not only form an important class of codes on their own, but also play a central role in quantum computation when $\ell = 2$. This is one out of many examples how generalizations and algebraic approaches shed light in more complex phenomena. Another way to generalize is to consider various weight functions. Typically, a weight function is just a function $\omega : A^n \longrightarrow \mathbb{R}$. Examples include the **homogeneous weight, symmetrized weight composition, Rosenbloom-Tsfasman weight**, and **poset weight**, which will be defined in Section 3.2.

1.2 Equivalence of Codes

A notion of sameness is required for any structure. In this thesis we will consider block codes over some finite module alphabet endowed with a weight function ω. In principle, for a notion of sameness one would want the algebraic structure as well as the error-correcting capabilities to be preserved. Thus two codes $\mathcal{C}$, $\mathcal{C}'$ are "the same" if there exists an isomorphism between the two that also preserves the weight. We will refer to such a map as ω-**isometry** and to the codes as **isometric**. The latter may be decorated with adjectives that display properties of the weight. These ideas can also be approached with a categorical language, as in [4] and references therein, where objects are block codes and morphisms are the linear maps that don't increase the weight.

With a notion of sameness in place one considers the respective equivalence classes and seeks for canonical representatives. The first step in doing so is to understand the structure of ω-isometries, which turns out to be a highly nontrivial task. One gains intuition by considering the (typically easy) extremal case $\mathcal{C} = A^n$. Namely, what is the structure of an ω-isometry $f : A^n \longrightarrow A^n$? This leads to two immediate followup questions. Is the structure of an ω-isometry $f : \mathcal{C} \subsetneq A^n \longrightarrow A^n$ the same as the extremal case for any code $\mathcal{C}$? And if not, how different is the structure? The former was first asked and answered affirmatively by MacWilliams [41] for binary linear codes with respect to the Hamming weight. Further generalizations led to MacWilliams Extension Theorem and the Extension Property of an alphabet [69]. However, the answer is not always affirmative; see Theorem 5.3. This fact, along with ideas discussed in [13], led Jay Wood to the notions of **isometry groups** [71]. Because we will make specific use of these ideas in Section 7.3 we briefly describe them in here. The key insight is to think of a code as a set of **messages** M embedded in A^n via a linear injective map Λ, called **encoding**. Then one studies isometries of the code $\mathcal{C} := \Lambda(M)$ via automorphisms of the **information module** M. More specifically, given a code $\mathcal{C}$ along with an information module M and encoding Λ, one defines

$$\mathrm{Iso}_\omega(\mathcal{C}) = \{f \in \mathrm{Aut}(M) \mid \omega(\Lambda(f(m))) = \omega(\Lambda(m)) \text{ for all } m \in M\}. \tag{1.1}$$

Then, inside $\mathrm{Iso}_\omega(\mathcal{C})$ one identifies the subgroup $\mathrm{Mon}_\omega(\mathcal{C})$ of all automorphisms that are restrictions of ω-isometries of A^n. Whenever MacWilliams Extension Theorem is true the two groups are the same. Otherwise one wonders how big the gap could be and what subgroups of $\mathrm{Aut}(M)$ can be realized as isometry groups. It turns out that these considerations are related with the symmetry of the weight ω (see (3.9) and (3.10)) and its actions on the alphabet and information module.

1.3 Thesis Outline

The overarching theme of this thesis is an algebraic and unified approach to the equivalence of classical and quantum codes. On the classical side we focus on linear block codes over a module alphabet, which as mentioned earlier includes several

types of codes. On the quantum side we focus on quantum stabilizer codes. A unified approach might seem impossible at a first glance because quantum codes are subspaces of a Hilbert space and thus very far from discrete. However, a discrete error model is possible and this enables a one-to-one correspondence between quantum stabilizer codes and self-orthogonal codes with respect to a certain symplectic bilinear form. Secondly, most of the equivalence questions concern weights that are additively extended from the alphabet to the ambient space; see (3.6). However, for instance, Rosenbloom-Tsfasman and poset weight do not fall under this category. Techniques described in this thesis can be used for many weight functions.

The main algebraic tool is character theory of finite abelian groups along with basic notions on rings and modules. More specifically, we will widely use partitions of the ambient space A^n and their character-theoretic duals. A key idea is to study weight-partition of the ambient space and realize it as orbit partition of some matrix group. This allows us to extract information about ω-isometries. Throughout this thesis we focus on codes over Frobenius alphabets. The aim is to provide further evidence on usefulness and naturality of Frobenius alphabets, especially in quantum error-correction.

Classical algebraic coding theory over Frobenius alphabets is well-studied. In fact, coding-theoretically motivated questions have led to ring-theoretic results such as the characterization of finite Frobenius rings and their rich duality theory [27, 68]. Unfortunately, the use of Frobenius alphabets in quantum error-correction is minor. The interest was sparked by [43] where the authors further generalized the idea of nonbinary quantum stabilizer codes to quantum stabilizer codes over Frobenius rings. Although the latter cannot outperform the former [19, 43], as pointed out in [43], one could make good use of the simpler arithmetic of Frobenius rings. On the other hand, such broader view gives new insights on previous questions. For instance, one uses a well-established classical theory to study quantum phenomena such as the LU-LC conjecture and Clifford equivalence of quantum codes.

This thesis is mainly an amalgamation of [19, 20, 51]. In Chapter 2 we provide a character-theoretic description of Frobenius bimodules. The usefulness of such approach is that it does not involve quasi-Frobenius bimodules. In order to do so we start with preliminary properties of characters as well as basic notions on rings and modules. In Chapter 3 we discuss basic notions of linear codes over Frobenius alphabets including general weights and their induced isometries. In particular, we define the symmetry groups and discuss MacWilliams Extension Theorem with respect to the Hamming weight. In Section 3.4 we discuss linear codes over local Frobenius rings. Results in this section generalize the work of [48, 49] on linear codes over chain rings. We point out that everything one needs is a principal socle rather than a chain of principal ideals. In addition, the results presented serve as a base for Section 7.2. In Chapter 4 we build up on the work of [6] to develop a duality theory of partitions of Frobenius bimodules, which as mentioned, plays a central role on our overall strategy of describing isometries of linear codes. In Chapter 5 we prove the MacWilliams Extension Theorem with respect to various weight. In particular, in Section 5.2 we prove the same result for additive codes with respect to the Rosenbloom-Tsfasman weight. Starting from Chapter 6 we focus on quantum error-correction. We describe

basic notions using the customary bra-ket notation as well as point out main differences with classical error-correction. We describe in details Shor's 9-qubit code and the stabilizer formalism introduced by Daniel Gottesman in his PhD thesis [21]. In Chapter 7 we discuss quantum stabilizer codes over Frobenius ring. We first establish a one-to-one correspondence with the so-called stabilizer codes, which in turn requires a special treatment of the error model. We continue with structural and performance results, which in turn leads us to conjecture that free stabilizer codes over Frobenius rings are as good as those over fields. In Section 7.3 we describe symplectic isometries of stabilizer codes and link this study with the LU-LC conjecture in quantum computation. To do so we make use of the machinery developed in previous chapters. In particular, we construct stabilizer codes with prescribed isometry groups. We end the chapter with a brief discussion of MacWilliams Identities. In the last chapter we list several open problems and potential future directions.

Chapter 2 Frobenius Rings and Modules

2.1 Characters of Finite Abelian Groups

In this section we briefly discuss characters of finite abelian groups. We will then focus on additive groups of finite modules. Let G be a finite abelian group. Its **character group** is defined as the set $\widehat{G} := \mathrm{Hom}(G, \mathbb{C}^*)$ of all group homomorphisms from G to $\mathbb{C}^*$, endowed with addition $(\chi_1 + \chi_2)(g) = \chi_1(g)\chi_2(g)$ for all $\chi_i \in \widehat{G}$ and $g \in G$. Then $\widehat{G}$ is again an abelian group. Its zero element is $\varepsilon_G \in \widehat{G}$ given by $\varepsilon_G(g) = 1$ for all $g \in G$. Elements of $\widehat{G}$ are called **characters** and ε_G is the **principal character** of G. If $|G| = n$ then $1 = \chi(0) = \chi(ng) = [\chi(g)]^n$ and therefore $\chi(g)$ is a nth root of unity. The additive inverse of $\chi \in \widehat{G}$ is given by $(-\chi)(g) := \overline{\chi(g)}$, where $\bar{\cdot}$ denotes the complex conjugate. The most fundamental properties of characters of a finite abelian group are the **orthogonality relations**

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} 0, & \text{if } g \neq 0, \\ |G|, & \text{if } g = 0. \end{cases} \quad \text{and} \quad \sum_{g \in G} \chi(g) = \begin{cases} 0, & \text{if } \chi \neq \varepsilon_G, \\ |G|, & \text{if } \chi = \varepsilon_G. \end{cases} \tag{2.1}$$

Next, we list some basic properties of the character group that will be needed later on. They are well-known and/or can easily be verified.

Remark 2.1. Let G be a finite abelian group.

(1) G is isomorphic to $\widehat{G}$ (though not naturally so) and hence $|G| = |\widehat{G}|$.

(2) $\widehat{G_1} \times \widehat{G_2} \cong \widehat{G_1 \times G_2}$ for any finite abelian groups G_1 and G_2. The isomorphism is given by $(\chi_1, \chi_2)(g_1, g_2) := \chi_1(g_1)\chi_2(g_2)$.

(3) G and $\widehat{\widehat{G}}$ are naturally isomorphic via the map $\zeta_G : g \longmapsto \mathrm{ev}_g$, where $\mathrm{ev}_g : \widehat{G} \longrightarrow \mathbb{C}^*$, $\chi \longmapsto \chi(g)$ denotes the evaluation map.

(4) Distinct characters of G are linearly independent in the $\mathbb{C}$-vector space of maps from G to $\mathbb{C}$.

(5) Let $\chi_1, \ldots, \chi_N$ and $\chi'_1, \ldots, \chi'_M$ be characters of G. If $\sum_{i=1}^N \chi_i = \sum_{i=1}^M \chi'_i$ as maps from G to $\mathbb{C}$, then the multisets $\{\{\chi_1, \ldots, \chi_N\}\}$ and $\{\{\chi'_1, \ldots, \chi'_M\}\}$ coincide; see [6, Prop. 3.1].

(6) Let $H \leq G$ be a subgroup and $\chi \in \widehat{H}$. Then χ can be extended to a character of G in $|G|/|H|$ ways.

(7) Let $H \leq G$ and $K \leq \widehat{G}$ be subgroups of G and $\widehat{G}$, respectively. Their **dual groups** are defined as $H^\circ := \{\chi \in \widehat{G} \mid H \subseteq \ker \chi\}$ and $K^\circ := \{g \in G \mid g \in \ker \chi \text{ for all } \chi \in K\}$, where for $\chi \in \widehat{G}$ we set $\ker \chi = \{g \in G \mid \chi(g) = 1\}$. Clearly, H° and K° are subgroups of $\widehat{G}$ and G, respectively. Then

   (i) $H^\circ \cong \widehat{G/H}$ and $K^\circ \cong \widehat{\widehat{G}/K} \cong G/K$. Thus $|H^\circ| = |G|/|H|$ and $|K^\circ| = |\widehat{G}|/|K| = |G|/|K|$.

   (ii) If $H \subseteq \ker \chi$ for all $\chi \in \widehat{G}$, then $H = \{0\}$.

   (iii) $(H^\circ)^\circ = H$ and $(K^\circ)^\circ = K$.

For the dual subgroups defined above, the orthogonality relations (2.1) straightforwardly generalize to the following.

$$\sum_{\chi\in K}\chi(g)=\begin{cases}|K|, & \text{if } g\in K^\circ,\\ 0, & \text{else.}\end{cases}\quad\text{and}\quad\sum_{h\in H}\chi(h)=\begin{cases}|H|, & \text{if } \chi\in H^\circ,\\ 0, & \text{else.}\end{cases}\tag{2.2}$$

Remark 2.2 (Additive version of characters)**.** Consider the quotient group $\mathbb{Q}/\mathbb{Z}$ and let G be a finite abelian group. Denote $G^\# := \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$. Similarly as the character group $\widehat{G}$, $G^\#$ also forms a finite abelian group under point-wise addition. One has the following commutative diagram

$$\begin{array}{ccc} G & & \\ \downarrow{\scriptstyle\psi} & \overset{\exists!\chi}{\searrow} & \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow[\exp(2\pi i\bullet)]{} & \mathbb{C}^* \end{array}\tag{2.3}$$

Namely, for every $\psi\in G^\#$ there exists a unique $\chi\in\widehat{G}$ such that for all $g\in G$ one has

$$\chi(g)=\exp(2\pi i\psi(g)),$$

and thus $\widehat{G}\cong G^\#$. In this thesis we will mainly focus on the multiplicative versions of characters. However, it is worth mentioning that the additive version is quite useful, especially when dealing with induced bilinear forms.

2.1.1 The Fourier Transform

In this section we consider in more details complex valued functions of a finite abelian group G, and show how the characters play a special role. The main goal is to prove Poisson Summation Formula, which has massive applications in coding theory. For details we refer the reader to [63]. Let $L^2(G)$ denote the space of all complex valued functions on G. Then $L^2(G)$ is canonically a complex vector space with basis $\{\delta_g \mid g\in G\}$ where

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

In particular, $L^2(G)$ has dimension n where $n=|G|$ is the cardinally of the group. Then Remark 2.1(4) implies that $\widehat{G}$ is also a basis of $L^2(G)$. Now that there are two bases floating around, one naturally wonders about a change of basis matrix. To that end, write $f\in L^2(G)$ as

$$f=\sum_{g\in G}f(g)\delta_g.\tag{2.4}$$

On the other hand, the second orthogonality relation in (2.1) implies

$$\delta_g(x)=\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\overline{\chi(g)}\chi(x).$$

Substituting in (2.4) we obtain

$$\begin{aligned} f(x) &= \sum_{g\in G} f(g)\left(\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\overline{\chi(g)}\chi(x)\right) \\ &= \sum_{\chi\in\widehat{G}}\sum_{g\in G}\frac{1}{|G|}f(g)\overline{\chi(g)}\chi(x) \\ &= \sum_{\chi\in\widehat{G}} c_\chi\chi(x), \end{aligned}$$

where

$$c_\chi = \frac{1}{|G|}\sum_{g\in G} f(g)\overline{\chi(g)}.$$

Definition 2.3. The **Fourier transform** of $f \in L^2(G)$ is the function $\widehat{f} \in L^2(\widehat{G})$ given by

$$\widehat{f}(\chi) = \sum_{g\in G} f(g)\overline{\chi(g)}$$

The above argument immediately implies the following.

Theorem 2.4 (Fourier Inversion Formula)**.** *For any $f \in L^2(G)$ we have*

$$f(x) = \frac{1}{|G|}\sum_{\chi\in\widehat{G}}\widehat{f}(\chi)\chi(x).$$

Remark 2.5. Let $G = G_1 \times \cdots \times G_n$ and $f_i \in L^2(G_i)$ for $i = 1, \ldots, n$. Define $f \in L^2(G)$ as $f(g_1, \ldots, g_n) := f_1(g_1)\cdots f_n(g_n)$. Then using $\widehat{G} \cong \widehat{G_1} \times \cdots \times \widehat{G_n}$, one has

$$\begin{aligned} \widehat{f}(\chi_1, \ldots, \chi_n) &= \sum_{(g_1,\ldots,g_n)\in G} f(g_1, \ldots, g_n)\overline{(\chi_1, \ldots, \chi_n)(g_1, \ldots, g_n)} \\ &= \sum_{\substack{g_1\in G_1 \\ \vdots \\ g_n\in G_n}} \prod_{i=1}^{n} f_i(g_i)\overline{\chi_i(g_i)} \\ &= \prod_{i=1}^{n}\sum_{g\in G_i} f_i(g)\overline{\chi_i(g)} \\ &= \prod_{i=1}^{n}\widehat{f_i}(\chi_i). \end{aligned}$$

We will next present the Poisson Summation Formula, which has vast applications in coding theory. We start with a lemma that facilitates the main result.

Lemma 2.6. *Let $H \leq G$ and let $f \in L^2(G)$ be such that $f(g + h) = f(g)$ for all $g \in G$ (that is, f is constant in the cosets of H). Write G as disjoint union of its cosets: $G = \biguplus_{i=1}^{l}(g_i + H)$. Then*

$$(1)\ \widehat{f}(\chi) = \begin{cases} |H|\sum_{i=1}^{l} f(g_i)\overline{\chi(g_i)}, & \text{if } \chi \in H^\circ, \\ 0, & \text{if } \chi \notin H^\circ. \end{cases}$$

(2) The map $\widetilde{f} \in \widehat{G/H}$, $a + H \longmapsto f(a)$ *is well-defined, and for all* $\chi \in \widehat{G/H} \cong H^\circ$ *we have*

$$\widehat{\widetilde{f}}(\chi) = \frac{1}{|H|}\widehat{f}(\chi).$$

Proof. (1) The statement follows by (2.2) and the following computation.

$$\begin{aligned}\widehat{f}(\chi) &= \sum_{g\in G} f(g)\overline{\chi(g)} = \sum_{i=1}^{l}\sum_{h\in H} f(g_i+h)\overline{\chi(g_i+h)} \\ &= \sum_{i=1}^{l} f(g_i)\overline{\chi(g_i)}\sum_{h\in H}\overline{\chi(h)}.\end{aligned}$$

(2) First of all, $\widetilde{f}$ is clearly well-defined. Next, recall that $H^\circ \cong \widehat{G/H}$. With this isomorphism one may think of a character $\chi \in \widehat{G/H}$ as a character on $\widehat{G}$ such that $\ker\chi \supseteq H$, that is, χ is automatically constant in the cosets of H. We have

$$\begin{aligned}\widehat{\widetilde{f}}(\chi) &= \sum_{g+H\in G/H} \widetilde{f}(g+H)\overline{\chi(g+H)} \\ &= \sum_{i=1}^{l} f(g_i)\overline{\chi(g_i)} \\ &\overset{(1)}{=} \frac{1}{|H|}\widehat{f}(\chi).\end{aligned}$$

□

Theorem 2.7 (Poisson Summation Formula)**.** *Let* $H \leq G$ *and fix* $g \in G$, $f \in L^2(G)$. *Then*

$$\sum_{h\in H} f(g+h) = \frac{1}{|H^\circ|}\sum_{\chi\in H^\circ}\widehat{f}(\chi)\overline{\chi(g)}. \tag{2.5}$$

In particular, for $g = 0$ *we obtain*

$$\sum_{h\in H} f(h) = \frac{1}{|H^\circ|}\sum_{\chi\in H^\circ}\widehat{f}(\chi).$$

Proof. Let $f' \in L^2(G)$ be given by $f'(g) := \sum_{h\in H} f(g+h)$. Then $f'(g+h) = f'(g)$ for all $h \in H$. As in Lemma 2.6(2) we obtain $\widetilde{f'} \in \widehat{G/H}$ given by $g + H \longmapsto f'(g)$. Thus, the left-hand-side of (2.5) equals $\widetilde{f'}(g+H)$. On the other hand we have

$$\begin{aligned}\sum_{\chi\in H^\circ}\widehat{f}(\chi)\overline{\chi(g)} &= \sum_{\chi\in H^\circ}\sum_{b\in G} f(b)\overline{\chi(b)}\cdot\overline{\chi(g)} \\ &= \sum_{\chi\in H^\circ}\sum_{i=1}^{l}\sum_{h\in H} f(g_i+h)\overline{\chi(g_i+h)}\cdot\overline{\chi(g)} && \text{(as in Lemma 2.6)} \\ &= \sum_{\chi\in H^\circ}\sum_{i=1}^{l} f'(g_i)\overline{\chi(g_i)}\cdot\overline{\chi(g)} && \text{(since } \chi\in H^\circ\text{)}\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\chi \in H^\circ} \frac{1}{|H|} \widehat{f'}(\chi)\overline{\chi(g)} && \text{(by Lemma 2.6(1))} \\
&= \sum_{\chi \in \overline{G/H}} \widehat{\widehat{f'}}(\chi)\chi(-g+H) && \text{(by Lemma 2.6(2))} \\
&= \sum_{\chi \in \overline{G/H}} \sum_{y+H} \widetilde{f'}(y+H)\chi(y+H)\chi(-g+H) \\
&= \sum_{y+H} \widetilde{f'}(y+H) \sum_{\chi \in \overline{G/H}} \chi(y-g+H) \\
&= \widetilde{f'}(g+H)\cdot|G/H|,
\end{aligned}
$$

where the last equality follows by the orthogonality relations in G/H. The result now follows from Remark 2.1(7)(i). The case when $g = 0$ is clear. □

2.2 Basic Notions on Rings and Modules

In this section we will set up some notations and discuss some preliminary properties of rings and modules that will be needed later on. Unless otherwise stated, all the rings and modules are finite. For details we refer the reader to [38, 39]. Let R be a finite associative ring with identity $1 \neq 0$. As it is customary, we denote $\mathfrak{J}(R)$ the **Jacobson Radical** and $\overline{R} := R/\mathfrak{J}(R)$ the associated semisimple ring, that is, the direct sum of matrix rings over finite fields (due to Wedderburn):

$$\overline{R} \cong \mathcal{M}_{\mu_1}(\mathbb{F}_{q_1}) \oplus \cdots \oplus \mathcal{M}_{\mu_n}(\mathbb{F}_{q_n}). \tag{2.6}$$

Let A be a unital (that is $1 \cdot a = a$ for all $a \in A$) left R-module. The **socle** of A, denoted $\mathrm{soc}({}_R A)$, is the sum of all minimal submodules of ${}_R A$. Since R is finite, and therefore artinian, this amounts to

$$\mathrm{soc}({}_R A) = \{a \in A \mid \mathfrak{J}(R)a = 0\}. \tag{2.7}$$

For a bimodule ${}_R A_R$ one considers left and right socles. In general $\mathrm{soc}({}_R A) \neq \mathrm{soc}(A_R)$, though this section and the next one will be vastly dedicated to modules with equal left and right socle. The socle $\mathrm{soc}({}_R A)$ is **essential** in A, and this implies that

$$\text{for all } a \in A, \text{there exists } r \in R \text{ such that } 0 \neq ra \in \mathrm{soc}({}_R A). \tag{2.8}$$

If A' is another left R-module, we write $\mathrm{Hom}({}_R A, {}_R A')$ for the set of homomorphisms between these modules. We denote $S := \mathrm{End}({}_R A)$ the ring of endomorphisms. The multiplication is defined as $f \cdot g := g \circ f$, where we use the convention[1] $(g \circ f)(a) := g(f(a))$. This turns A into a right S-module via $a \cdot f := f(a)$. Thus a left R-module A is canonically a (R, S)-bimodule. In addition, there is a canonical ring homomorphism

$$\Theta : R \longrightarrow \mathrm{End}(A_S),\ r \longmapsto \left\{ \begin{array}{rcl} \Theta(r) : A_S & \longrightarrow & A_S \\ a & \longmapsto & ra \end{array} \right. . \tag{2.9}$$

[1] The reason why we reverse the order is to avoid ambiguities when composing left and right linear maps simultaneously.

If Θ is an isomorphism then A is called **left balanced**, see [23, p. 2]. In a similar way one defines **right balanced** and **balanced** bimodules. We point out in here that this can be done over any (R, R')-bimodule. For the bimodule ${}_RA_S$ and $K \subseteq A, I \subseteq R, J \subseteq S$ we define the following **annihilators**[2]

$$\begin{aligned} {}^{\perp}K &:= \{r \in R \mid rK = 0\} \leq {}_RR, \qquad K^{\perp} := \{s \in S \mid Ks = 0\} \leq S_S, \\ I^{\perp} &:= \{a \in A \mid Ia = 0\} \leq A_S, \qquad {}^{\perp}J := \{a \in A \mid aJ = 0\} \leq {}_RA. \end{aligned} \tag{2.10}$$

With the same notation as above and with the aid of (2.7) we have $\operatorname{soc}({}_RA) = \mathfrak{J}(R)^{\perp}$.

Now let R be a finite associative ring with identity, and A a finite (R, R)-bimodule. Consider the (abelian) additive group of A. Due to 2.1(1) we have $A \cong \widehat{A}$ as groups. We endow $\widehat{A}$ with a (R, R)-bimodule structure as follows. For all $r \in R, a \in A$, and $\chi \in \widehat{A}$, the scalar multiplication is given by

$$(r{\cdot}\chi)(a) = \chi(ar) \quad \text{and} \quad (\chi{\cdot}r)(a) = \chi(ra). \tag{2.11}$$

We call $\widehat{A}$ the **character bimodule**. Note that the left R-module structure on $\widehat{A}$ is induced by the right R-module structure of A, and vice versa. In this sense we have a functor $\widehat{\bullet} : {}_R\mathbf{M} \longrightarrow \mathbf{M}_R$ from the category of left R-modules to the category of right R-modules. Indeed, for a morphisms $f : {}_RA \longrightarrow {}_RB$ in ${}_R\mathbf{M}$, $\widehat{f}$ maps $\chi \in \widehat{B}$ to $\chi \circ f \in \widehat{A}$. It follows by the second part of (2.11) that $\widehat{f}(\chi{\cdot}r) = (\widehat{f}(\chi)){\cdot}r$ and thus $\widehat{f}$ is a morphism in $\mathbf{M}_R$. As a special case, we can apply all the above to the (R, R)-bimodule R and consider the character bimodule $\widehat{R}$. One can straightforwardly verify that $\widehat{\bullet}$ is an exact contravariant functor. In particular this implies that $\widehat{R}$ is an injective module (since R is trivially a free R-module, and thus projective).

Remark 2.8. One may go a step further and consider the character module of the bimodule ${}_R\widehat{A}_R$. More specifically, $\widehat{\widehat{A}}$ is also a (R, R)-bimodule under the same scalar multiplication. That is, for all $\phi \in \widehat{\widehat{A}}, \chi \in \widehat{A}, r \in R$ the scalar multiplication is given by

$$(r{\cdot}\phi)(\chi) = \phi(\chi{\cdot}r) \quad \text{and} \quad (\phi{\cdot}r)(\chi) = \phi(r{\cdot}\chi)$$

In fact Remark 2.1(3) enables a canonical isomorphism of (R, R)-bimodules

$$\zeta_A : {}_RA_R \longmapsto {}_R\widehat{\widehat{A}}_R, \quad a \longmapsto \begin{cases} \operatorname{ev}_a : \widehat{A} & \longrightarrow & \mathbb{C}^* \\ \qquad \chi & \longmapsto & \chi(a) \end{cases}. \tag{2.12}$$

Analogously one considers $\widehat{\widehat{R}}$ and the bimodule isomorphism $\zeta_R : {}_RR_R \longrightarrow {}_R\widehat{\widehat{R}}_R$.

Remark 2.9. Let A be a (R, R)-bimodule. For any $n \in \mathbb{N}$ so is A^n. Out of these we can produce two more (R, R)-bimodules: $\widehat{A}^n$ and $\widehat{A^n}$. Then Remark 2.1(2) gives a canonical bimodule isomorphism

$$\widehat{A}^n \cong \widehat{A^n} \quad \text{via} \quad (\chi_1, \ldots, \chi_n)(a_1, \ldots, a_n) := \prod_{j=1}^{n} \chi_j(a_j), \tag{2.13}$$

[2] One might want to use subscripts. We omit subscripts for the sake of a lighter notation, and use them when it is absolutely necessary.

and thus, we may identify the two modules.

In what follows we study in details the character bimodule $\widehat{R}$. We start with an easily verifiable proposition that connects annihilators with the notion of dual groups defined in Remark 2.1(7). Note first that the dual subgroups of left (resp., right) submodules are right (resp., left) submodules.

Proposition 2.10 ([27, p. 409])**.** *For the character bimodule $\widehat{R}$ we have*

$$K^{\perp} = K^{\circ} \text{ for all } K \subseteq {}_R\widehat{R}, \qquad {}^{\perp}K = K^{\circ} \text{ for all } K \subseteq \widehat{R}_R, \tag{2.14}$$

$$I^{\perp} = I^{\circ} \text{ for all } I \subseteq {}_R R, \qquad {}^{\perp}J = J^{\circ} \text{ for all } J \subseteq R_R. \tag{2.15}$$

Proof. We provide a proof of the first equality, with the rest being similar and/or following by duality. For the forward containment, assume $r \in K^{\perp}$. This yields $\chi r = \varepsilon_R$ for all $\chi \in K$. By evaluating at $1 \in R$ we obtain $\chi(r) = 1$ for all $\chi \in K$, and thus $r \in K^{\circ}$. Equality follows by the fact that all the statements made were actually equivalences. □

A left R-module A is called **left faithful** if $rA = 0$ implies $r = 0$. **Right faithful** and **faithful** modules are defined similarly. We have the following.

Proposition 2.11. *The character bimodule $\widehat{R}$ is faithful.*

Proof. We show that $\widehat{R}$ is left faithful, with the right case being similar. Assume $r\widehat{R} = \{\varepsilon_R\}$. Then $1 = (r\chi)(s) = \chi(sr)$ for all $\chi \in \widehat{R}$ and $s \in R$. Thus $Rr \subseteq \ker \chi$ for all $\chi \in \widehat{R}$. Remark 2.1(7)(ii) implies $Rr = 0$, and therefore $r = 0$. This concludes the proof. □

Proposition 2.12 ([20, Prop. 2.4])**.** *The character bimodule $\widehat{R}$ is balanced.*

Proof. We show that $\widehat{R}$ is right balanced[3], with the left version being symmetric. Recall the ring homomorphism Θ from (2.9). Similarly, we have the right sided version applied to the case $A = \widehat{R}$.

$$\Phi : R \longrightarrow \mathrm{End}({}_R\widehat{R}), \; r \longmapsto \left\{ \begin{array}{rcl} \Phi(r) : {}_R\widehat{R} & \longrightarrow & {}_R\widehat{R} \\ \chi & \longmapsto & \chi r \end{array} \right. . \tag{2.16}$$

First of all, Φ is well-defined since $\chi \longmapsto \chi r$ is indeed in $\mathrm{End}({}_R\widehat{R})$. It is also straightforward to verify that Φ is a ring homomorphism as well as right R-linear. The injectivity of Φ follows from the fact that $\widehat{R}$ is left faithful; see Proposition 2.11. We show next that Φ is surjective. Recall the evaluation map form Remark 2.1(3). Note that $\mathrm{ev}_1 \circ \Phi(r) = \mathrm{ev}_r$. Remark 2.1(3) now implies

$$\widehat{\widehat{R}} = \{\mathrm{ev}_r \mid r \in R\} = \{\mathrm{ev}_1 \circ \Phi(r) \mid r \in R\}.$$

[3]We specifically show the right version because the isomorphism constructed will be used later on.

Let now $f \in \mathrm{End}({}_R\widehat{R})$. Then $\mathrm{ev}_1 \circ f \in \widehat{\widehat{R}}$, and hence $\mathrm{ev}_1 \circ f = \mathrm{ev}_1 \circ \Phi(r)$ for some $r \in R$. This means $\big(f(\chi)\big)(1) = (\chi r)(1)$ for all $\chi \in \widehat{R}$. Applying this to the characters χs for any $s \in R$ and using the left linearity of f and the left module structure of $\widehat{R}$ we obtain $\big(f(\chi)\big)(s) = (r\chi)(s)$ for all $s \in R$. Therefore $f(\chi) = \chi r$, which in turn yields $f = \Phi(r)$, as desired. □

Definition 2.13 ([26, 66])**.**

(1) A left R-module ${}_RA$ is called **quasi-Frobenius** (QF) if for any $n \in \mathbb{N}$ and for any submodule $U \leq {}_RA^n$ we have:
   (i) There exists an index set I and an injective homomorphism $A^n/U \hookrightarrow \prod_I A$.
   (ii) The canonical map $\mathrm{Hom}(A^n, A) \longrightarrow \mathrm{Hom}(U, A)$ is surjective.

(2) A (R, R')-bimodule A is called QF if for every maximal left ideal $I \leq {}_RR$ and maximal right ideal $J \leq R'_{R'}$ we have $I^\perp$ and ${}^\perp J$ are either zero or irreducible submodules of ${}_RA$.

(3) A ring R is called QF ring if ${}_RR_R$ is a QF bimodule.

Perhaps it is worth to give some intuition on the above definitions. Definition 2.13(1)(i) guarantees an analogue version of Rank-Nullity Theorem for vector spaces. On the other hand, the second condition mimics the extendability of linear forms (for vector spaces). The latter is a consequence of the injectivity of fields. Definition 2.13(2) is best explained by the following very useful characterization.

Theorem 2.14 ([23, Thm. 2.1])**.** *For a finite faithful left R-module ${}_RA$ with $S = \mathrm{End}({}_RA)$, the following are equivalent:*

(1) ${}_RA$ is a QF module.

(2) ${}_RA_S$ is a QF bimodule.

(3) ${}_RA_S$ is a balanced bimodule and any of the following equivalent conditions holds:

(i) for any submodules $K \leq {}_RA$ and $L \leq A_S$ we have

$$K = {}^\perp(K^\perp) \text{ and } L = ({}^\perp L)^\perp. \tag{2.17}$$

(ii) $\mathrm{soc}({}_RA) = \mathrm{soc}(A_S) =: \mathrm{soc}(A)$ and the $(\overline{R}, \overline{S})$-bimodule $\mathrm{soc}(A)$ is QF.

If any of the above conditions are satisfied, then for left ideals $I \leq {}_RR$ and right ideals $J \leq S_S$, we have

$${}^\perp(I^\perp) = I \text{ and } ({}^\perp J)^\perp = J. \tag{2.18}$$

Remark 2.15.

(1) Equations (2.17) and (2.18) are known in literature as the **double annihilator properties**. Classically, a QF ring is defined as those artinian rings that satisfy the double annihilator property; see [38, Thm. 15.1], for instance.

(2) Equation (2.14) along with Remark 2.1(7) implies that the character bimodule $\widehat{R}$ satisfies equation (2.17). Since $\widehat{R}$ is balanced thanks to Proposition 2.12, we can conclude that $\widehat{R}$ is a QF (R, R)-bimodule. In particular, the isomorphism Φ of Proposition 2.12 implies that ${}_R\widehat{R}_S$ is QF bimodule as well. Then Theorem 2.14(1) implies ${}_R\widehat{R}$ is a QF module.

(3) Let ${}_RA$ be a QF module. Recall that the socle is given by $\mathrm{soc}({}_RA) = \mathfrak{J}(R)^{\perp}$. Thanks to Theorem 2.14(3) and (2.7) we get

$$\mathfrak{J}(R) = {}^{\perp}(\mathfrak{J}(R)^{\perp}) = {}^{\perp}\mathrm{soc}(A). \tag{2.19}$$

We now continue with the definition of Frobenius bimodules, and then present a useful characterization in terms of the character bimodule. In the next chapter we use this insight to define Frobenius bimodules employing a purely character-theoretic approach and bypass the notion of QF. We believe that, especially in a coding-theoretic setting, this approach is by far more useful and pleasant. After all, Frobeniusness is named after Frobenius' work on similarities of representations of ${}_RR$ and ${}_R\widehat{R}$.

Definition 2.16 ([23, Def. 2.16])**.** A finite QF bimodule ${}_RA_R$ is called **Frobenius bimodule** if there are module isomorphisms

$${}_R\overline{R} \cong {}_R\mathrm{soc}(A) \quad \text{and} \quad \overline{R}_R \cong \mathrm{soc}(A)_R. \tag{2.20}$$

Theorem 2.17 ([23, Prop. 2.17])**.** *Let ${}_RA_R$ be a finite QF bimodule. Then the following are equivalent:*

(1) ${}_RA_R$ *is a Frobenius bimodule.*
(2) $\mathrm{soc}(A)$ *is a left and right cyclic R-module.*
(3) ${}_RA \cong {}_R\widehat{R}$ *and* $A_R \cong \widehat{R}_R$.

Remark 2.18.

(1) From Definition 2.16 we obviously get that a Frobenius bimodule is QF. However, including QF in the definition of a Frobenius bimodule is redundant since the condition on Theorem 2.17(3) alone implies QF, as we will see in Corollary 2.27.
(2) Classically, a (artinian) ring R (thus, not necessarily finite) is called Frobenius if ${}_RR_R$ satisfies (2.20). Even in this case, (2.20) solely implies that ${}_RR_R$ is QF; see [38, Thm. 16.14]. Moreover, for finite rings Honold [27, Thm. 2] showed that R is Frobenius iff either of isomorphisms in (2.20) exist. That is, the existence of either of the isomorphisms actually implies the other one.
(3) For the equivalence (2) $\iff$ (3) on Theorem 2.17 the assumption on ${}_RA_R$ being QF is crucial. In general, for a left R-module A we have $\mathrm{soc}({}_RA)$ is left cyclic iff ${}_RA \hookrightarrow {}_R\widehat{R}$; see [69, Prop. 5.3].
(4) In Remark 2.15(2) we mentioned that ${}_R\widehat{R}_R$ is a QF bimodule. Moreover, Theorem 2.17(3) implies that $\widehat{R}$ is trivially a Frobenius bimodule.

2.3 A Character-Theoretic Approach to Frobeniusness

Let R be a finite ring and let A be a finite (R,R)-bimodule. In this section we focus exclusively on character bimodules and give a character-theoretic approach to notions introduced in Section 2.2. The aim is to study A via ${}_R\widehat{R}_R$ and ${}_R\widehat{A}_R$. In particular, we develop the approach starting over with Definition 2.19, where we define Frobenius bimodules without resorting to quasi-Frobenius bimodules; see also Definition 2.16. Recall that the scalar multiplication that gives rise to the module structure of $\widehat{R}$ is

given in (2.11). Recall also the canonical bimodule isomorphisms ζ_R and ζ_A discussed in Remark 2.8.

Definition 2.19. Let R be any finite ring with identity and A a finite (R,R)-bimodule. Then A is called a **Frobenius bimodule** if ${}_RA \cong {}_R\widehat{R}$ and $A_R \cong \widehat{R}_R$. The ring R is called Frobenius if ${}_RR_R$ is Frobenius.

Before we start exploring the consequences of the above definition, we record a very useful result due to Wood that goes back to Bass' Theorem [7, Lem. 6.4].

Theorem 2.20 ([68, Prop. 5.1])**.** *Let R be any finite ring with identity and A a finite left R-module. Let $a, a' \in A$ be such that $Ra = Ra'$. Then there exists a unit $\alpha \in R^*$ such that $a' = \alpha a$.*

Remark 2.21.

(1) Let A be an (R,R)-Frobenius bimodule. By definition, there exists an isomorphism $\lambda : {}_RA \cong {}_R\widehat{R}$. Recall that ${}_R\widehat{R}$ is an injective module. As a consequence so is ${}_RA$. Now using the fact that the character functor $\widehat{\bullet}$ is exact and contravariant we get for free that $\widehat{A}_R$ is projective. In fact we can say much more. Recall the evaluation map form Remark 2.1(3). Then the induced map

$$R_R \longrightarrow \widehat{A}_R,\ r \longmapsto \zeta_R(r) \circ \lambda = \mathrm{ev}_r \circ \lambda \tag{2.21}$$

is an isomorphism of right R-modules. As a consequence, $\widehat{A}_R$ is a free module of rank one. Any basis vector of $\widehat{A}_R$ is called a **right generating character**. It follows that right generating characters are of the form $\zeta_R(u) \circ \lambda = \mathrm{ev}_u \circ \lambda$ for $u \in R^*$. Similarly, an isomorphism of right modules $\rho : A_R \cong \widehat{R}_R$ gives rise to **left generating characters**. To resume, given a right generating character χ and a left generating character χ' we have

$$\widehat{A} = \{\chi \cdot r \mid r \in R\} = \{r \cdot \chi' \mid r \in R\}. \tag{2.22}$$

(2) Let $\chi, \chi' \in \widehat{A}$ be two left generating characters. By definition we have $R\chi = \widehat{A} = R\chi'$. Theorem 2.20 implies that there exists a unit $u \in R^*$ such that $\chi' = u\chi$. Conversely, if χ is a left generating character the so is $u\chi$. This follows easily, for instance, from Theorem 2.22(3) below. Therefore the set of left generating characters is $R^*\chi$. Similarly for right generating characters.

(3) Recall that ${}_R\widehat{\widehat{R}}_R \cong {}_RR_R$ via ζ_R. Let A be a Frobenius bimodule. It follows directly from Definition 2.19 that ${}_R\widehat{A}_R$ is Frobenius iff R is a Frobenius ring. In fact, $\widehat{A}$ is far from being Frobenius if R is not Frobenius .

(4) Making use of Propositions 2.11 and 2.12 we get that a Frobenius bimodule is balanced and faithful. That is

$$\mathrm{End}({}_RA) \cong R \cong \mathrm{End}(A_R) \text{ as rings} \tag{2.23}$$

as well as ${}^\perp A = A^\perp = 0$; see (2.10). In particular, we have group isomorphisms

$$\mathrm{Aut}({}_RA) \cong R^* \cong \mathrm{Aut}(A_R). \tag{2.24}$$

Below we list some basic facts about generating characters of Frobenius bimodules. Recall the kernel of a character from Remark 2.1(7). The equivalences can be found in [69, Lem. 5.2, Lem. 5.3, Cor. 5.1].

Theorem 2.22. *Let ${}_RA_R$ be a Frobenius bimodule and let $\chi \in \widehat{A}$. The following are equivalent.*
(1) χ is a left generating character of A, i.e., ${}_R\widehat{A} = R\chi$.
(2) χ is a right generating character of A, i.e., $\widehat{A}_R = \chi R$.
(3) $\ker\chi$ contains no nonzero left submodule of A.
(4) $\ker\chi$ contains no nonzero right submodule of A.
Furthermore, if χ is a generating character of A and V is any left R-module then the map $\mathrm{Hom}({}_RV, {}_RA) \longrightarrow \widehat{V},\ g \longmapsto \chi \circ g$ is an injective group homomorphism.

Proof. It only remains to prove the last part. We will use part (3), that is, $\ker\chi$ does not contain any nonzero left submodule of A. To that end, assume that $(\chi \circ g)(v) = \chi(g(v)) = 1$ for all $v \in V$. This yields $\operatorname{im} g \subseteq \ker\chi$. By assumption, we obtain $\operatorname{im} g = 0$ and thus $g = 0$. □

In particular, Theorem 2.22 implies that we need not specify the sidedness of generating characters. From now on, we fix a Frobenius bimodule $A = {}_RA_R$ and a generating character χ. As in (2.22), one may write

$$\widehat{A} = \{\chi{\cdot}r \mid r \in R\} = \{s{\cdot}\chi \mid s \in R\}. \tag{2.25}$$

Note that (2.25) implies that for all $r \in R$ there exists $s_r \in R$ such that $\chi \cdot r = s_r \cdot \chi$; see also Remark 2.25. We point out in here that typically $s_r \neq r$. The case when they are equal will be considered later on; see also Theorem 2.30.

Remark 2.23. Let A be a Frobenius bimodule with generating character χ. For the left R-linear map

$$\beta_{\mathrm{l}} : {}_RA \longrightarrow {}_R\widehat{R},\quad a \longmapsto \begin{cases} \chi(\bullet a) : R & \longrightarrow & \mathbb{C}^* \\ r & \longmapsto & \chi(ra) \end{cases}, \tag{2.26}$$

we have

$$\begin{aligned} \ker\beta_{\mathrm{l}} &= \{a \in A \mid \beta_{\mathrm{l}}(a) = \varepsilon_R\} \\ &= \{a \in A \mid \chi(ra) = 1 \text{ for all } r \in R\} \\ &= \{a \in A \mid Ra \subseteq \ker\chi\} \\ &= \{0\}, \end{aligned}$$

where the very last step follows by Theorem 2.22(3). Therefore β_{l} is injective. Since A is Frobenius we have ${}_RA \cong {}_R\widehat{R}$ and in particular $|A| = |\widehat{R}|$. This implies that β_{l} is an isomorphism. Similarly, we have the following isomorphisms:

$$\begin{aligned} &\beta_{\mathrm{r}} : A_R \longrightarrow \widehat{R}_R,\quad a \longmapsto \chi(a\bullet), \\ &\alpha_{\mathrm{l}} : {}_RR \longrightarrow {}_R\widehat{A},\quad r \longmapsto \chi(\bullet r), \\ &\alpha_{\mathrm{r}} : R_R \longrightarrow \widehat{A}_R,\quad r \longmapsto \chi(r\bullet). \end{aligned} \tag{2.27}$$

We end this remark by pointing out that all the above mentioned isomorphisms are just special instances of (2.21) from Remark 2.21. Specifically, we have

$$\alpha_{\mathrm{r}}(r) = \zeta_R(r) \circ \beta_{\mathrm{l}}, \qquad \alpha_{\mathrm{l}}(r) = \zeta_R(r) \circ \beta_{\mathrm{r}}, \qquad \text{for all } r \in R, \tag{2.28}$$

$$\beta_{\mathrm{r}}(a) = \zeta_A(a) \circ \alpha_{\mathrm{l}}, \qquad \beta_{\mathrm{l}}(a) = \zeta_A(a) \circ \alpha_{\mathrm{r}}, \qquad \text{for all } a \in A. \tag{2.29}$$

Recall the endomorphism ring $S = \mathrm{End}({}_RA)$. On A we have now two right module structures: A_R and A_S as described in Section 2.2. A natural question is how do these two structures relate? To answer this question we start with the following isomorphism of rings

$$\tau : R \longrightarrow S, \quad r \longmapsto \beta_{\mathrm{l}}^{-1} \circ \Phi(r) \circ \beta_{\mathrm{l}} \tag{2.30}$$

where Φ is as in Proposition 2.12. In addition to the isomorphism τ we also have the natural ring homomorphism

$$\sigma : R \longrightarrow S, \quad r \longmapsto \begin{cases} \sigma(r) : {}_RA & \longrightarrow & {}_RA \\ a & \longmapsto & ar \end{cases}. \tag{2.31}$$

Note that $\ker \sigma = A^{\perp} = 0$ thanks to Remark 2.21(4). Hence σ is injective. Moreover, the fact that $|R| = |S|$ (thanks to (2.30)) implies that σ is an isomorphism of rings. In other words all endomorphisms of ${}_RA$ are given by right multiplication by some ring element $r \in R$. Summing up we have two different ways, yet very closely related (see Remark 2.25 below), to describe the endomorphism ring S:

$$S = \{\tau(r) \mid r \in R\} = \{\sigma(r) \mid r \in R\}. \tag{2.32}$$

An identical approach can be done with A_R and $S' := \mathrm{End}(A_R)$. Equation (2.32) along with its right-sided analogue imply the following.

Proposition 2.24. *Any subset $K \subseteq A$ satisfies*

$$K \text{ is a submodule of } A_R \Longleftrightarrow K \text{ is a submodule of } A_S,$$
$$K \text{ is a submodule of } {}_RA \Longleftrightarrow K \text{ is a submodule of } {}_{S'}A.$$

The following remark gives the relation between τ and σ.

Remark 2.25. Let χ be a generating character of A. Using (2.25) and $A^{\perp} = 0$ we have that for every $r \in R$ there exists a unique $r' \in R$ such that $r\chi = \chi r'$ as characters. This yields a bijection $g : R \longrightarrow R$, $r \longmapsto r'$. It is straightforward to check that g is in fact a ring homomorphism, and hence an automorphism of R. Moreover, by the definition of τ we have $\tau(g(r)) = \beta_{\mathrm{l}}^{-1} \circ \Phi(g(r)) \circ \beta_{\mathrm{l}} \in S$. We claim that $\tau \circ g = \sigma$. Indeed, for $a \in A$ we have

$$\Big((\tau \circ g)(r)\Big)(a) = \Big(\beta_{\mathrm{l}}^{-1} \circ \Phi(g(r)) \circ \beta_{\mathrm{l}}\Big)(a) = \beta_{\mathrm{l}}^{-1}\Big(\big(\chi g(r)\big)(\bullet a)\Big)$$
$$= \beta_{\mathrm{l}}^{-1}\Big(\big(r\chi\big)(\bullet a)\Big) = \beta_{\mathrm{l}}^{-1}\big(\chi(\bullet ar)\big) = ar = \big(\sigma(r)\big)(a).$$

We end this remark by pointing out that g is known in literature as the **Nakayama automorphism**.

We now return to annihilators defined in (2.10), and show that a Frobenius bimodule also satisfies Proposition 2.10. This will be the crucial step toward showing that Definitions 2.19 and 2.16 are equivalent. Recall that thanks to Propositions 2.12 and 2.24 we may identify $R = S$ and ${}_RA_R = {}_RA_S$. As mentioned, we have the following.

Theorem 2.26 ([20, Prop. 2.10]). *Let ${}_RA_R$ be a Frobenius bimodule and $S := \mathrm{End}({}_RA)$. Then for the bimodule ${}_RA_S$ we have the double annihilator properties*

$$\begin{aligned} ({}^\perp K)^\perp &= K \text{ for all } K \leq A_S, & {}^\perp(K^\perp) &= K \text{ for all } K \leq {}_RA \\ {}^\perp(I^\perp) &= I \text{ for all } I \leq {}_RR, & ({}^\perp J)^\perp &= J \text{ for all } J \leq S_S. \end{aligned}$$

Proof. Recall first that for the case $A = \widehat{R}$ we get the double annihilator properties by combining Proposition 2.10 and Remark 2.1(7); see also Remark 2.15(2). The strategy is to transfer the problem from A to $\widehat{R}$ and then use the above-mentioned fact.

We start by showing the very first equality. To this end, let $K \leq A_S$ be a submodule and consider $L := \beta_1(K) \subseteq \widehat{R}$. We claim that in fact $L \leq \widehat{R}_R$ is a right R module. This is not a priori clear since β_1 is only guaranteed to be left linear. Indeed, let $\chi \in L$ and write $\chi = \beta_1(a)$ for some $a \in K$. Recall that $S = \{\tau(r) \mid r \in R\}$. Since $K \leq A_S$ we have $\tau(r)(a) = a \cdot \tau(r) \in K$ for all $r \in R$. From the very definition of τ we have $\tau(r)(a) = \beta_1^{-1}\big(\beta_1(a)r\big)$, and thus $\beta_1(a)r = \beta_1\big(\tau(r)(a)\big) \in \beta_1(K) = L$. This proves the claim. For the rest of the proof we use the notation $I^{\perp_A}$ and $I^{\perp_{\widehat{R}}}$ in order to distinguish between the annihilators of an ideal $I \leq {}_RR$ in A and in $\widehat{R}$. Then left linearity and injectivity of β_1 implies $\beta_1(I^{\perp_A}) = I^{\perp_{\widehat{R}}}$ for any $I \leq {}_RR$. By the same properties we have ${}^\perp K = {}^\perp L$. Now the special case $A = \widehat{R}$ gives us $({}^\perp L)^{\perp_{\widehat{R}}} = L$ and thus we compute

$$\big|({}^\perp K)^{\perp_A}\big| = \big|\beta_1\big(({}^\perp K)^{\perp_A}\big)\big| = \big|\beta_1\big(({}^\perp L)^{\perp_A}\big)\big| = \big|({}^\perp L)^{\perp_{\widehat{R}}}\big| = |L| = |K|.$$

Together with the obvious containment $K \subseteq ({}^\perp K)^\perp$ we obtain the desired equality.

Next, let $K \leq {}_RA$. Then since β_1 is left R-linear then $\beta_1(K) \leq {}_R\widehat{R}$ is trivial. Now the second equality ${}^\perp(K^\perp) = K$ follows easily.

For the two remaining equalities we make use of the last part of Theorem 2.14. Indeed, they follow by all the above and the fact that A is Frobenius. □

Combining Proposition 2.24 and Theorem 2.26 we get the following immediate corollary.

Corollary 2.27. *For any Frobenius bimodule ${}_RA_R$ and any submodule $K \leq A_R$ we have $({}^\perp K)^\perp = K$. In particular, Definition 2.19 alone implies that a Frobenius bimodule is also a QF bimodule, and thus Frobenius in the sense of Definition 2.16 (by Theorem 2.17).*

In Sections 3.4 and 7.2 we will be focusing on local Frobenius rings. In many circumstances, if R is a commutative ring the following helps transferring the problem to local Frobenius rings.

Theorem 2.28 ([38, Thm. 15.27]). *If R is a finite commutative ring then $R \cong R_1 \times \cdots \times R_t$ for suitable local Frobenius rings R_i.*

Let R be a local QF ring with unique maximal ideal $\mathfrak{m}$. Then $\mathfrak{J}(R) = \mathfrak{m}$ and (2.7) imply $\operatorname{soc}(R) = \mathfrak{m}^{\perp}$. Moreover $\mathfrak{m} = \operatorname{soc}(R)^{\perp}$ thanks to (2.19). Definition 2.13(2) implies that $\operatorname{soc}(R)$ must be right cyclic. Similarly we may conclude that $\operatorname{soc}(R)$ is left cyclic. That is, there exists $\alpha, \beta \in R$ such that $\alpha R = \operatorname{soc}(R) = R\beta$. In particular we have the following.

Theorem 2.29. *Let R be a local ring. Then R is QF iff it is Frobenius.*

We continue with a special class of Frobenius bimodules. Note first that Definition 2.19 in general does not necessarily imply ${}_RA_R \cong {}_R\widehat{R}_R$ as bimodules. If the latter is satisfied the bimodule ${}_RA_R$ is called **symmetric**. We have the following characterizations of symmetric bimodules; see [38, Thm. 16.54] for symmetric algebras and [23, Prop. 2.11] for symmetric rings.

Theorem 2.30. *Let ${}_RA_R$ be a Frobenius bimodule. The following are equivalent.*
(1) A is symmetric.
(2) There exists a generating character $\chi \in \widehat{A}$ such that $r \cdot \chi = \chi \cdot r$ for all $r \in R$.

Proof. (1) $\Longrightarrow$ (2) Let $\Psi : {}_RA_R \longrightarrow {}_R\widehat{R}_R$ be an isomorphism of bimodules. Then $\widehat{\Psi} : {}_R\widehat{\widehat{R}}_R \longrightarrow {}_R\widehat{A}_R$, $\phi \longmapsto \phi \circ \Psi$ is again an isomorphism of bimodules. By Remark 2.8, we have ${}_R\widehat{\widehat{R}}_R \cong {}_RR_R$. With this identification, $\chi := \widehat{\Psi}(1) \in \widehat{A}$ is a generating character. Since $\widehat{\Psi}$ is left and right R-linear we have

$$r \cdot \chi = r \cdot (\widehat{\Psi}(1)) = \widehat{\Psi}(r) = (\widehat{\Psi}(1)) \cdot r = \chi \cdot r.$$

(2) $\Longrightarrow$ (1) The isomorphism of bimodules ${}_RR_R \longmapsto {}_R\widehat{A}_R$, $r \longmapsto r \cdot \chi = \chi \cdot r$ induces the required isomorphism of bimodules ${}_RA_R \cong {}_R\widehat{R}_R$. □

Remark 2.31. A character $\chi \in \widehat{A}$ such that $r \cdot \chi = \chi \cdot r$ is called **symmetric**. Thus, a bimodule ${}_RA_R$ is symmetric iff it admits a symmetric generating character. Note also that symmetric bimodules are precisely those Frobenius bimodules for which the Nakayama automorphism from Remark 2.25 is the identity.

We end this section with some examples and nonexamples.

Example 2.32.
(1) The class of Frobenius rings is quite large. It includes finite fields, finite principal ideal rings (and consequently integer residue rings), full matrix rings over Frobenius rings, finite products of Frobenius rings, finite group rings over Frobenius rings; see [68, Ex. 4.4] for instance.
(2) The easiest example of a non Frobenius ring is $R := \mathbb{F}_2[x, y]/(x^2, y^2, xy)$. It is easy to see that $\operatorname{soc}(R) = \{0, x, y, x + y\}$ which is clearly non principal. R is also a local ring with unique maximal ideal $\operatorname{soc}(R)$. This implies that R is not even QF; see Theorem 2.29.
(3) Let R be the commutative non-Frobenius ring above, and let $A = \widehat{R}$. We already know that A is Frobenius bimodule; a generating character is given by $\psi(\chi) = \chi(1)$ for all $\chi \in \widehat{R}$ as in Remark 2.21(1). We also already know that $B := \widehat{A}$ is not a

Frobenius bimodule; see Remark 2.21(3). This can be seen explicitly as follows. It is easy to see that $R = \text{span}_{\mathbb{F}_2}\{1, x, y\}$ and $A = \text{span}_{\mathbb{F}_2}\{\chi_1, \chi_2, \chi_3\}$, where

$$\begin{aligned}\chi_1(x) = \chi_1(y) = 1,\ \chi_1(1) = -1,\\ \chi_2(1) = \chi_2(y) = 1,\ \chi_2(x) = -1,\\ \chi_3(1) = \chi_3(x) = 1,\ \chi_3(y) = -1.\end{aligned}$$

We also have

$$R\chi_1 = \{\varepsilon, \chi_1\} \quad \text{and} \quad R\chi = \{\varepsilon, \chi, \chi_1, \chi + \chi_1\} \text{ for all } \chi \in A \setminus \{\varepsilon, \chi_1\},$$

which in turn says that none of the characters in $\widehat{R}$ is generating. This implies that none of the characters in $\widehat{B}$ can be generating (because $\widehat{B} \cong \widehat{R}$ as bimodules thanks to Remark 2.8).

(4) It is straightforward to check that a vector space V over a finite field $\mathbb{F}$ satisfies Definition 2.13(1)-(2), and therefore V is a QF module and bimodule over $\mathbb{F}$. Yet, V will be Frobenius iff $\dim_{\mathbb{F}}(V) = 1$. The latter makes it clear that Frobeniusness is a very strong condition with significant size constraints.

(5) Symmetric rings trivially include commutative Frobenius rings. Full matrix rings over finite fields are also symmetric (see [38, Ex. 16.57]). As a consequence of (2.6) so is every finite semisimple ring.

(6) We end this list of examples by providing two examples of Frobenius non symmetric rings.

(i) Consider the ring

$$R := \left\{ \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & a & b & 0 \\ 0 & 0 & c & 0 \\ d & 0 & 0 & c \end{pmatrix} \middle| \ a, b, c, d \in \mathbb{F}_2 \right\}.$$

Denote a matrix $A \in R$ as $A(a, b, c, d)$. The character $\chi : A(a, b, c, d) \longmapsto (-1)^{a+b+c+d}$ is a generating character, and thus R is Frobenius; see [18, Ex. 4.5]. Consider, for instance, $A := A(1, 0, 0, 0)$. It is straightforward to check that $A{\cdot}\chi \neq \chi{\cdot}A$. Next, every generating character of $\widehat{R}$ is of type $\chi_U := U{\cdot}\chi$ where $U \in R^* = \{A(1, b, 1, d) \mid b, d \in \mathbb{F}_2\}$. Similarly, one finds a matrix $A \in R$ for which $A{\cdot}\chi_U \neq \chi_U{\cdot}A$. Hence $\widehat{R}$ does not admit any symmetric generating character.

(ii) Let $\mathbb{F}_q[x, \sigma]$ be a skew polynomial ring where σ is any nontrivial automorphism of $\mathbb{F}_q$ acting via $xa = \sigma(a)x$. Then $R := \mathbb{F}_q[x; \sigma]/(x^2)$ is Frobenius but not symmetric; see [23, Ex. 2.14].

Chapter 3 Linear Codes over Rings and Modules

3.1 Basic Notions

Let R be a finite ring with identity and A be a finite unital left R-module. A submodule $0 \neq \mathcal{C} \leq {}_R A^n$ is called **block linear code of length** n. Elements of $\mathcal{C}$ are called **codewords** and A is called the **alphabet**. It is worth pointing out that this general definition is on its fullest. It includes linear codes over finite fields, that is, $A = R = \mathbb{F}_q$; it includes linear codes over finite rings, that is $A = R$; it includes sublinear codes; that is $A = R'$ where R'/R is a ring extension. The latter is a particularly interesting case. If $R' = \mathbb{F}_{p^l}$ and $R = \mathbb{F}_p$ for some prime p, the code $\mathcal{C}$ is called **additive**. Additive codes not only form an interesting class on their own, but also link with Quantum Information Theory and Quantum Error Correction. We will discuss this connection in Chapters 6 and 7. We will say $\mathcal{C}$ is a $[n,k]$-code if $|\mathcal{C}| = |R|^k$ for some $k \in \mathbb{N}$. In particular, a free module $\mathcal{C} \leq {}_R A^n$ of rank k is a $[n,k]$-code. A linear code of length n is endowed with the **Hamming weight**, where for $a = (a_1, \ldots, a_n) \in A^n$ we define

$$\mathrm{wt}_{\mathrm{H}}(a) := |\{i \mid a_i \neq 0\}|. \tag{3.1}$$

Since $\mathcal{C}$ is a submodule we have $0 \in \mathcal{C}$. The **minimum distance** of a code $\mathcal{C}$ is given by

$$\mathrm{d}_{\mathrm{H}}(\mathcal{C}) := \min\{\mathrm{wt}_{\mathrm{H}}(a) \mid a \in \mathcal{C} - \{0\}\}. \tag{3.2}$$

If in addition we have $\mathrm{d}_{\mathrm{H}}(\mathcal{C}) = d$ we say that $\mathcal{C}$ is a $[n,k,d]$-code. The minimum distance of a code is the most important invariant and completely determines its theoretical error-correcting capabilities due to the following.

Theorem 3.1. *Let $\mathcal{C}$ be a linear code of minimum distance d. Then $\mathcal{C}$ can detect any pattern of $d-1$ errors and can correct any pattern of $\lfloor (d-1)/2 \rfloor$.*

Let $\mathcal{C} \leq {}_R A^n$ be a linear code. From the very definition of the socle we have

$$\mathrm{soc}(\mathcal{C}) = \mathcal{C} \cap \big(\mathrm{soc}({}_R A)\big)^n \leq {}_R\big(\mathrm{soc}(A)\big)^n. \tag{3.3}$$

Since $\mathrm{soc}(\mathcal{C}) \subseteq \mathcal{C}$ we clearly have $\mathrm{d}_{\mathrm{H}}(\mathcal{C}) \leq \mathrm{d}_{\mathrm{H}}(\mathrm{soc}(\mathcal{C}))$. On the other hand, (2.8) implies the reverse inequality. This yields

$$\mathrm{d}_{\mathrm{H}}(\mathcal{C}) = \mathrm{d}_{\mathrm{H}}(\mathrm{soc}(\mathcal{C})). \tag{3.4}$$

Equation (3.4) points out the importance of the notion of the socle. Since the socle of a Frobenius bimodule is particularly nice, (3.4) provides yet another confirmation about the usefulness of Frobeniusness in a coding theoretic setting.

We now continue with the **dual** of a linear code. There are many approaches one can take. For our purposes it is convenient to define the dual of a code via bilinear forms.

Definition 3.2. Let ${}_RA_R$ be a bimodule. A map $\beta : A \times A \longrightarrow A$ is called a **bilinear form** if the maps $\beta(a, \bullet) : A \longrightarrow A$ and $\beta(\bullet, a) : A \longrightarrow A$ are right and left R-module homomorphisms for all $a \in A$. In addition, β is called

(1) **nondegenerate** if the maps $a \longmapsto \beta(\bullet, a)$ and $a \longmapsto \beta(a, \bullet)$ are injective.
(2) **symmetric** if $\beta(a, a') = \beta(a', a)$ for all $a, a' \in A$.
(3) **alternating** if $\beta(a, a') = -\beta(a', a)$ for all $a, a' \in A$.
(4) **symplectic** if $\beta(a, a) = 0$ for all $a \in A$.

We extend β to $\beta : A^n \times A^n \longrightarrow A$ via

$$\beta(a, a') := \sum_{j=1}^{n} \beta(a_j, a'_j). \tag{3.5}$$

Definition 3.3. The dual of a left linear code $\mathcal{C} \leq {}_RA^n$ is the left linear code

$$l(\mathcal{C}) := \{a \in A^n \mid \beta(a, c) = 0 \text{ for all } c \in \mathcal{C}\} \leq {}_RA^n.$$

The dual of a right linear code $\mathcal{C} \leq A_R^n$ is the right linear code

$$r(\mathcal{C}) := \{a \in A^n \mid \beta(c, a) = 0 \text{ for all } c \in \mathcal{C}\} \leq A_R^n.$$

Proposition 3.4. *Let A be a Frobenius bimodule with generating character χ, and $\mathcal{C} \leq {}_RA^n$ a linear code. Then*

$$l(\mathcal{C}) = \{a \in A^n \mid \chi(\beta(a, c)) = 1 \text{ for all } c \in \mathcal{C}\}$$

Proof. The forward containment is obvious. For " $\supseteq$ " assume that $a \in A^n$ is such that $\chi(\beta(a, c)) = 1$ for all $c \in \mathcal{C}$. Note that $\beta(a, \mathcal{C}) := \{\beta(a, c) \mid c \in \mathcal{C}\}$ is a right submodule of A^n and by the assumption on a we have $\beta(a, \mathcal{C}) \subseteq \ker \chi$. Now Theorem 2.22(4) implies $\beta(a, \mathcal{C}) = 0$ and hence $a \in l(\mathcal{C})$. □

Remark 3.5. Let R be a Frobenius ring with generating character χ. Take $A = R$ and let $\beta(r, s) := rs$. Then for $r, s \in R^n$, as in (3.5), we extend β to the standard dot product in R^n

$$\beta(r, s) := \sum_{j=1}^{n} r_j s_j.$$

Let $\mathcal{C} \leq {}_RR^n$ be a linear code. Using Proposition 3.4, and then Remark 2.9 we get

$$\begin{aligned} l(\mathcal{C}) &= \left\{ r \in R^n \,\middle|\, \chi\left(\sum_{j=1}^{n} r_j c_j\right) = 1 \text{ for all } c \in \mathcal{C} \right\} \\ &= \left\{ r \in R^n \,\middle|\, \prod_{j=1}^{n} (\chi \cdot r_j)(c_j) = 1 \text{ for all } c \in \mathcal{C} \right\} \\ &\cong \{\psi \in \widehat{R^n} \mid \mathcal{C} \subseteq \ker \psi\}. \end{aligned}$$

Now Remark 2.1(7) implies $l(\mathcal{C}) = \mathcal{C}^\circ \leq {}_R\widehat{R^n}$, and Proposition 2.10 further implies $l(\mathcal{C}) = \mathcal{C}^\perp$. For this reason and due to the fact that we will only consider the dual codes of linear codes over Frobenius rings, from now on we will use the common perp notation.

3.2 General Weight Functions

Let $\mathcal{C} \leq {}_RA^n$ be a linear code of length n. A **weight function** is simply a map $\omega : A^n \longrightarrow \mathbb{R}$ such that $\omega(0) = 0$. The minimum distance of $\mathcal{C}$ with respect to w is

$$\mathrm{d}_\omega(\mathcal{C}) := \min\{\omega(a) \mid a \in \mathcal{C} - \{0\}\}.$$

Before we go any further, it is worth pointing out that this definition differs from the ones commonly used in literature. Indeed, one starts with a weight function on the alphabet $\omega : A \longrightarrow \mathbb{R}$ and then extends it to $a = (a_1, \ldots, a_n) \in A^n$ via

$$\omega(a) = \sum_{i=1}^{n} \omega(a_i). \tag{3.6}$$

However, many weight functions that we will encounter later on are not of this form and therefore we think that this approach is restrictive.

The most important weight function for codes over rings or modules is the homogeneous weight. It was introduced in [36] for codes over integer residue rings and further developed for linear codes over rings and modules in [22, 44].

Definition 3.6. A weight function $\omega : A \longrightarrow \mathbb{R}$ on a finite module ${}_RA$ is called **(normalized left) homogeneous** if
(1) $\omega(a) = \omega(a')$ for all $a, a' \in A$ such that $Ra = Ra'$.
(2) $\sum_{a' \in Ra} \omega(a') = |Ra|$ for all $a \neq 0$.

In [23, Thm. 4.4] Greferath et al. establish the existence and uniqueness of the homogeneous weight on arbitrary finite modules. For finite Frobenius bimodules a very useful formula for the homogeneous weight has been established by Wood [70, Prop. 9]. It is a straightforward generalization of [27, p. 412] by Honold, where the same result was derived for finite Frobenius rings.

Theorem 3.7. *Let ${}_RA_R$ be a finite Frobenius bimodule with generating character χ. Then the homogeneous weight on A is given by*

$$\omega(a) = 1 - \frac{1}{|R^*|} \sum_{u \in R^*} \chi(au) = 1 - \frac{1}{|R^*|} \sum_{u \in R^*} \chi(ua) \quad \textit{for all } a \in A.$$

Proof. First of all, the second equality follows by the fact that $\sum_{u \in R^*} u\chi = \sum_{u \in R^*} \chi u$ is the sum of all generating characters of A. Next, as mentioned, thanks to [23, Thm. 4.4] there exists a unique homogeneous weight over a Frobenius alphabet. Thus it is enough to show that the function ω satisfies Definition 3.6. The first property follows immediately from Theorem 2.20. For the second property, let $a \neq 0$. Then

$$\sum_{a' \in Ra} \sum_{u \in R^*} \chi(a'u) = \sum_{u \in R^*} \sum_{r \in R} (\chi \cdot r)(au) = 0,$$

since $au \neq 0$ and the second inner sum above runs over all the characters $\psi \in \widehat{A}$. Now the statement follows. □

Remark 3.8.

(1) Since characters take complex values, it is not a priori clear that the function ω above takes in fact real values (as required by the definition of any weight function in general and by Definition 3.6 in particular). However, since $\{u\chi \mid u \in R^*\} = \{-u\chi \mid u \in R^*\}$ we have

$$\sum_{u\in R^*} \overline{\chi(au)} = \sum_{u\in R^*} \chi(-au) = \sum_{u\in R^*} (-u\chi)(a) = \sum_{u\in R^*} (u\chi)(a) = \sum_{u\in R^*} \chi(au).$$

This yields $\omega(a) = \overline{\omega(a)}$ and hence $\omega(a) \in \mathbb{R}$ for all $a \in A$.

(2) Note that Theorem 3.7 also makes it obvious that $\omega(0) = 0$, which again, is not a priori clear from Definition 3.6.

Remark 3.9. Let $R = \mathbb{F}_q$ be a finite field. Then, since the only non-zero ideal of R is R itself, we have $\omega(r) = q/(q-1)$ for all $r \neq 0$. Conversely, assume that $\omega(r) = \alpha$ for all $r \neq 0$. Then all non-zero ideals $I \leq R$ satisfy the size condition $\alpha = |I|/(|I|-1)$. Thus all non-zero ideals of R have the same size, and therefore R is a field. This means that the homogeneous weight ω over a ring R is the Hamming weight (up to a scaling factor) iff R is a field. In particular, ω is the Hamming weight (up to a factor of 2) iff $R = \mathbb{F}_2$.

Example 3.10. Obviously the homogeneous weight depends on the alphabet. Let $R = \mathbb{F}_2 \times \mathbb{F}_2$. Let ω be the homogeneous weight on the R-module R. One computes from definition 3.6 $\omega(0,0) = \omega(1,1) = 0$ and $\omega(0,1) = \omega(1,0) = 2$. If we take the homogeneous weight $\hat{\omega}$ on the $\mathbb{F}_2$-vector space $\mathbb{F}_2 \times \mathbb{F}_2$, then $\hat{\omega}(a) = 2$ for all $a \neq 0$. On the other hand, if we take the homogeneous weight on $\mathbb{F}_2$ and extend it additively on $\mathbb{F}_2 \times \mathbb{F}_2$ as in (3.6), we obtain $\tilde{\omega}(1,0) = \tilde{\omega}(0,1) = 1$ and $\tilde{\omega}(1,1) = 2$.

We continue next with the Rosenbloom-Tsfasman weight (RT-weight) introduced in [54]. The RT-weight was used in [60] to detect matrix codes with large Hamming distance. In addition, the RT-weight provides an instance of a weight that is not an additive extension from $A \longrightarrow \mathbb{R}$.

Definition 3.11. The RT-weight of a vector $a = (a_1, \ldots, a_n) \in A^n$ is defined as

$$\mathrm{wt}_{\mathrm{RT}}(a) = \begin{cases} \max\{i \mid a_i \neq 0\}, & \text{if } a \neq 0 \\ 0, & \text{if } a = 0 \end{cases}.$$

The RT-weight as well as the Hamming weight are special cases of the following. Let $\leq$ be a partial order on $[n] := \{1, \ldots, n\}$ and consider the poset $\mathbb{P} := ([n], \leq)$. A subset $S \subseteq [n]$ is called an ideal if $i \in S$ and $j \leq i$ imply $j \in S$. We denote by $\langle S \rangle$ the smallest ideal generated by S. For $a = (a_1, \ldots, a_n) \in A^n$ we denote by $\mathrm{supp}(a) := \{i \mid a_i \neq 0\}$ the **support** of a.

Definition 3.12. The **poset weight** of $a = (a_1, \ldots, a_n) \in A^n$ is given by

$$\mathrm{wt}_{\mathbb{P}}(a) = |\langle \mathrm{supp}(a) \rangle|.$$

As mentioned, both the Hamming weight and the RT-weight are special instances of the poset weight. Indeed, let $\mathbb{P}$ be an **anti-chain**, that is, every two elements are incomparable. In this case we have $\operatorname{supp}(a) = \langle \operatorname{supp}(a) \rangle$ and therefore $\mathrm{wt}_{\mathrm{H}}(a) = \mathrm{wt}_{\mathbb{P}}(a)$. On the other hand, if the partial order $\leq$ is the usual order of the naturals we have $\mathrm{wt}_{\mathrm{RT}}(a) = \mathrm{wt}_{\mathbb{P}}(a)$.

Recall that if ${}_RA$ is a left R-module then $S := \operatorname{End}({}_RA)$ acts on A from the right via $a \cdot f := f(a)$. Now let $G \leq S^*$, that is, a subgroup of the group of automorphisms of ${}_RA$. Denote A/G the orbit space of this group action and write $A/G = \bigcup_{i=1}^{l} \mathcal{O}_i$. For an orbit $\mathcal{O} \in A/G$ and a vector $a = (a_1, \ldots, a_n) \in A^n$ denote

$$\mathrm{swc}_{\mathcal{O}}(a) := |\{i \mid a_i \in \mathcal{O}\}|.$$

Definition 3.13. With the same notation as above, the **symmetrized weight composition** (with respect to G) of a vector $a \in A^n$ is defined as

$$\mathrm{swc}_G(a) := \big(\mathrm{swc}_{\mathcal{O}_1}(a), \ldots, \mathrm{swc}_{\mathcal{O}_l}(a)\big).$$

That is, $\mathrm{swc}_G(a)$ encodes the number of entries of a that are contained in each orbit $\mathcal{O}_i$. Note that if $R = A$ are fields and $G = S^*$ then the symmetrized weight composition encodes the same information as the Hamming weight. The other extremal case $G = \{1\}$ gives the **complete weight** of a, that is, the number of coordinates equal to a fixed module element; see [40, p. 142]. Note in addition that

$$\mathrm{swc}_G(a) = \mathrm{swc}_G(b) \implies \mathrm{wt}_{\mathrm{H}}(a) = \mathrm{wt}_{\mathrm{H}}(b). \tag{3.7}$$

3.3 Isometries of Linear Codes

An isometry is intended to capture the sameness of two linear codes. Thus, we want an isometry to preserve the algebraic structure of the code (linearity, for starters) as well as the weight function the code is endowed with.

Definition 3.14. Let $\mathcal{C} \leq A^n$ be a linear code and ω a weight function on $\mathcal{C}$. A R-linear map $f : C \longrightarrow A^n$ is called an ω-**isometry** if $\omega(f(x)) = \omega(x)$ for all $x \in \mathcal{C}$. We call two codes ω-**isometric** if there exists an ω-isometry between them.

If for a given weight function ω, $0 \in \mathcal{C}$ is the only codeword of weight zero (e.g. $\mathrm{wt}_{\mathbb{P}}$, and therefore $\mathrm{wt}_{\mathrm{H}}, \mathrm{wt}_{\mathrm{RT}}$) we get that an ω-isometry is injective and therefore an isomorphism of modules onto its image. It is easy to see that the inverse of such a map is an ω-isometry as well.

Of course, two isometric codes have the same minimum distance and therefore the same error-correcting capabilities.

Recall that for a left R-module ${}_RA$, $S := \operatorname{End}({}_RA)$ acts on A from the right. Similarly $\operatorname{End}({}_RA^n)$ acts on ${}_RA^n$ from the right via $a \cdot f := f(a)$. We have a ring isomorphism

$$\Phi : \mathcal{M}_n(S) \longrightarrow \operatorname{End}({}_RA^n), \quad M \longmapsto \begin{cases} \Phi(M) : {}_RA^n & \longrightarrow & {}_RA^n \\ a & \longmapsto & a \cdot M \end{cases}. \tag{3.8}$$

As a consequence, every $f \in \mathrm{End}({}_R A^n)$ acts on ${}_R A^n$ as right multiplication by a matrix with entries in S. Clearly, (3.8) implies $\mathrm{Aut}({}_R A^n) \cong \mathrm{GL}_n(S)$.

A weight function ω comes associated with the left and right **symmetry groups**. For a fixed $n \in \mathbb{N}$ we define

$$G_{\omega,l} := \{u \in R^* \mid \omega(ua) = \omega(a) \text{ for all } a \in A^n\}, \tag{3.9}$$

$$G_{\omega,r} := \{\tau \in \mathrm{GL}_n(S) \mid \omega(a \cdot \tau) = \omega(a) \text{ for all } a \in A^n\}. \tag{3.10}$$

Example 3.15. Let $R = \mathcal{M}_k(\mathbb{F}_q)$, $A = \mathcal{M}_{k\times m}(\mathbb{F}_q)$, $\omega = \mathrm{wt_H}$, and $n = 1$. Then $G_{\omega,l} = \mathrm{GL}_k(\mathbb{F}_q)$ and $G_{\omega,r} = \mathrm{GL}_m(\mathbb{F}_q)$. In particular, for $k = 1$ we get $G_{\omega,l} = \mathbb{F}_q^*$ and for $m = 1$ we get $G_{\omega,r} = \mathbb{F}_q^*$.

In $\mathrm{Aut}({}_R A^n)$ we identify two subgroups of matrices: The group of lower triangular matrices

$$\mathrm{LT}_n(S) := \{M \in \mathrm{GL}_n(S) \mid M \text{ is lower triangular}\}, \tag{3.11}$$

and the group of **monomial** matrices

$$\mathrm{Mon}_n(S) := \left\{ M \in \mathrm{GL}_n(S) \;\middle|\; \begin{array}{l} M \text{ has exactly one nonzero entry} \\ \text{in each row and column} \end{array} \right\}. \tag{3.12}$$

And in general, for a subgroup $G \leq S^* = \mathrm{Aut}({}_R A)$ we define

$$\mathrm{Mon}_{G,n}(S) := \{M \in \mathrm{Mon}_n(S) \mid \text{the nonzero entries of } M \text{ are in } G\}. \tag{3.13}$$

For a given weight function ω and a linear code $\mathcal{C} \leq {}_R A^n$ a natural question is to understand the structure of an ω-isometry $f : \mathcal{C} \longrightarrow A^n$. This turns out to be straightforward for the extremal case $\mathcal{C} = A^n$ and is given by the following.

Theorem 3.16. *Let $f \in \mathrm{End}({}_R A^n)$ and $M \in \mathcal{M}_n(S)$ be such that $f(a) = a \cdot M$ for all $a \in A^n$. Then*

(1) f is $\mathrm{wt_H}$-preserving iff $M \in \mathrm{Mon}_n(S)$.
(2) f is $\mathrm{wt_{RT}}$-preserving iff $M \in \mathrm{LT}_n(S)$.
(3) f is swc*-preserving with respect to $G \leq S^*$ iff $M \in \mathrm{Mon}_{G,n}(S)$.*

As a consequence, if A is Frobenius bimodule, (2.24) implies $M \in \mathrm{Mon}_n(R), M \in \mathrm{LT}_n(R)$, $M \in \mathrm{Mon}_{G,n}(R)$ respectively.

Proof. We prove the first part, with the rest being similar. The "if part" is obvious. For the "only-if part", put $A_j := 0 \times \cdots \times A \times \cdots \times 0$. Let $M = (m_{i,j}) \in \mathrm{End}({}_R A^n)$ be such that $f(a) = aM$ as in (3.8). Whenever f is a Hamming isometry, for all $a \in A_j$ ($a \neq 0$, of course), $f(a)$ must be a weight one vector. Hence, there exists a permutation $\sigma \in S_n$ such that $f(A_j) \subseteq A_{\sigma(j)}$. In addition, f is an isomorphism. This yields $f_{|A_j}$ is also an isomorphism and $f(A_j) = A_{\sigma(j)}$. This means $m_{\sigma(j),j} \in \mathrm{Aut}({}_R A)$. This concludes the proof. □

Note that Theorem 3.16 establishes the right symmetry groups $G_{\omega,r}$ for the specified weight ω. On the other hand, it is easy to see that $G_{\omega,l} = R^*$ in all the cases. In this sense, all the above mentioned weight functions have **full left symmetry**. On the other hand, none of the weights has full right symmetry in general.

Remark 3.17. In [50] the authors establish the right symmetry group of a general poset weight for the case $R = A = \mathbb{F}_q$. We sketch the proof for the general case. The details can be filled similarly as in [50]. Let f and M be as in Theorem 3.16, and assume f is $\mathrm{wt}_{\mathbb{P}}$-preserving. Put $A_j := 0 \times \cdots \times A \times \cdots \times 0$. Then, the ideals $\langle \mathrm{supp}(f(a)) \rangle$ have the same unique maximal element for all $a \in A_j - \{0\}$; see [50, Lem. 1.2]. This gives a map $\phi_f : j \longmapsto \max\{\langle \mathrm{supp}(f(a)) \rangle\}$. Then, similarly as in [50, Thm. 1.2], we have

$$f(A_j) = \prod_{i \leq j} A_{\phi_f(i)}. \tag{3.14}$$

On the other hand, (3.14) implies that the jth column of M has entries $m_{\phi_f(i),j} \in S$ if $i \leq j$ and 0 else. So in essence, the right symmetry group is still the set of "lower" triangular matrices where "lower" is in terms of the poset structure.

Remark 3.18.

(1) Let $M = (m_{i,j}) \in \mathrm{Mon}_n(S)$. By the very definition of a monomial matrix, there exists a permutation π such that $m_{i,j} \in S^*$ if $i = \pi(j)$ and $m_{i,j} = 0$ else. Since the nonzero entries of M depend only on one coordinate, we will write m_j instead of $m_{\pi(j),j}$. With the same notation as in (3.8), the map $f := \Phi^{-1}(M)$ is called **monomial map**. For $a = (a_1, \ldots, a_n) \in A^n$ we have

$$f(a) = \big(m_1(a_{\pi(1)}), \ldots, m_n(a_{\pi(n)})\big). \tag{3.15}$$

If $G \leq S^*$ and $m_j \in G$ for all j then f is called a G-**monomial map**. Recall that in the case when A is a Frobenius bimodule we have $S \cong R$, and therefore $S^* \cong R^*$. In this case (3.15) reads as

$$f(a) = (a_{\pi(1)}u_1, \ldots, a_{\pi(n)}u_n), \tag{3.16}$$

where $u_j \in R^*$ correspond to $m_j \in S^*$.

(2) By the very definition of the Hamming weight and (2.1), for $a \in A$ we have

$$1 - \mathrm{wt}_{\mathrm{H}}(a) = \frac{1}{|A|} \sum_{\chi \in \widehat{A}} \chi(a).$$

For $a = (a_1, \ldots, a_n) \in A^n$ we have

$$n - \mathrm{wt}_{\mathrm{H}}(a) = \sum_{j=1}^{n} \big(1 - \mathrm{wt}_{\mathrm{H}}(a_j)\big) = \frac{1}{|A|} \sum_{j=1}^{n} \sum_{\chi \in \widehat{A}} \chi(a_j). \tag{3.17}$$

Now let A be a Frobenius bimodule with generating character χ. Then $\widehat{A} = \{r\chi \mid r \in R\} = \{\chi r \mid r \in R\}$ and $|A| = |R|$, and (3.17) reads as

$$n - \mathrm{wt}_{\mathrm{H}}(a) = \frac{1}{|R|} \sum_{j=1}^{n} \sum_{r \in R} \chi(a_j r) = \frac{1}{|R|} \sum_{j=1}^{n} \sum_{r \in R} \chi(r a_j). \tag{3.18}$$

Now, assume we have a linear map $f : \mathcal{C} \leq {}_R A^n \longrightarrow A^n$. Let $p_j : A^n \longrightarrow A$ be the projection on the j^{th} coordinate. Denote $f_j := p_j \circ f$. Let $\iota : \mathcal{C} \longrightarrow A^n$ be the canonical embedding, and similarly denote $\iota_j := p_j \circ \iota$. In other words, for all $x \in \mathcal{C}$, $\iota(x) = (\iota_1(x), \cdots, \iota_n(x))$ and $f(x) = (f_1(x), \ldots, f_n(x))$. Making use of (3.18) we conclude that f is a Hamming isometry iff for all $x \in \mathcal{C}$ we have

$$\sum_{i=1}^{n} \sum_{r \in R} \chi(\iota_i(rx)) = \sum_{j=1}^{n} \sum_{r \in R} \chi(f_j(rx)). \tag{3.19}$$

So far we have dealt with isometries of the special case $\mathcal{C} = {}_R A^n$. In this case we took high advantage of the fact that ι_j are defined on the entire ambient space A^n. What about when $\mathcal{C} \subsetneq A^n$? As we will see later on, this question is highly nontrivial. The question was posed and answered first by MacWilliams [41] for the case $R = A = \mathbb{F}_2$. A particularly elegant proof using character theory was given in [64] for the case $R = A = \mathbb{F}_q$, which eventually led Wood to the case of Frobenius alphabets. The strategy, as we will see, works very well for any weight that is extended additively as in (3.6). However, the strategy would not work for weights without this property (e.g. poset weight and RT-weight). In Chapter 5 we will see a new strategy that works for any weight function.

Theorem 3.19. *Let A be a Frobenius bimodule and $\mathcal{C} \leq {}_R A^n$ be a linear code. Then $f : \mathcal{C} \longrightarrow A^n$ is a Hamming isometry iff there exists $M \in \mathrm{Mon}_n(R)$ such that $f(x) = x \cdot M$ for $x \in \mathcal{C}$.*

Proof. The if part follows directly by Theorem 3.16(1). For the only if part, let $\mathcal{C} \leq {}_R A^n$ be a linear code and $f : \mathcal{C} \longrightarrow A^n$ be a Hamming isometry. We will show that f is as in (3.16). We will use the same notation as in Remark 3.18(2). Note first that it is enough to show that $\iota_j = f_{\pi(j)} u_j$ for some units $u_j \in R^*$ and $\pi \in S_n$. Since f is a Hamming isometry, (3.19) implies

$$\sum_{i=1}^{n} \sum_{r \in R} (\chi r) \circ \iota_i = \sum_{j=1}^{n} \sum_{s \in R} (\chi s) \circ f_j \tag{3.20}$$

as characters on $\mathcal{C}$. Then Remark 2.1(5) implies that the multisets $\{\{(\chi r) \circ \iota_i \mid r \in R, i \in [n]\}\}$ and $\{\{(\chi s) \circ f_j \mid s \in R, j \in [n]\}\}$ coincide. The group $\mathrm{Hom}({}_R\mathcal{C}, {}_R A)$ is a right R-module via $(g \cdot r)(x) := g(rx)$ for all $x \in \mathcal{C}$ and $r \in R$. Assume without loss of generality that $\iota_1 R$ is a maximal (with respect to inclusion) among submodules $\iota_1 R, \ldots, \iota_n R, f_1 R, \ldots, f_n R$. For $r = 1_R$, there must exist $k \in [n]$ and $s \in R$, such that $\chi \circ \iota_1 = (\chi s) \circ f_k$. This yields

$$\chi(\iota_1(a)) = \chi(f_k(sa)) = \chi\big((f_k s)(a)\big), \qquad \text{for all } a \in \mathcal{C}.$$

Thus $\mathrm{im}\,(\iota_1 - f_k s) \subseteq \ker \chi$. Theorem 2.22(3) implies $\iota_1 = f_k s$ and thus $\iota_1 R \subseteq f_k R$. Since $\iota_1 R$ was chosen maximal, we have $f_k R = \iota_1 R$. Now Theorem 2.20 guarantees the existence of a unit $u_1 \in R^*$ such that $\iota_1 = f_k u_1$. Then $(\chi r) \circ \iota_1 = (\chi r) \circ (f_k u_1) = \chi \circ (f_k r u_1)$ implies

$$\sum_{r \in R} (\chi r) \circ \iota_1 = \sum_{r \in R} \chi \circ (f_k r u_1) = \sum_{s \in R} \chi \circ (f_k s) = \sum_{s \in R} (\chi s) \circ f_k.$$

Using the above, one may delete the first and kth term from the outer sums in (3.20) and then proceed similarly. □

3.4 Linear Codes Over Local Frobenius Rings

Throughout this section R is a finite commutative local Frobenius ring. We will denote $\mathfrak{m}$ its unique maximal ideal $\mathfrak{J}(R) = \mathfrak{m}$ and $\mathbb{F} := R/\mathfrak{m}$ its residue field. Since a Frobenius ring has a cyclic socle, we fix a generator

$$\operatorname{soc}(R) = \alpha R. \tag{3.21}$$

In addition, for a local Frobenius rings we have

$$\operatorname{soc}(R) = \mathfrak{m}^{\perp} \text{ and } \mathfrak{m} = \operatorname{soc}(R)^{\perp}. \tag{3.22}$$

Let $\mathfrak{m} = (z_1, \ldots, z_t)$ be minimally generated. Because $\mathfrak{m}$ is the Jacobson radical of a finite ring (and thus artinian), each z_i is nilpotent. Let k_i be the nilpotency index of z_i, that is the smallest integer such that $z_i^{k_i} = 0$. It is clear that $(z_1^{k_1-1} \cdots z_t^{k_t-1}) \subseteq \mathfrak{m}^{\perp} = \operatorname{soc}(R)$. But a local Frobenius ring has exactly one minimal ideal, namely $\operatorname{soc}(R)$; see [11, Thm. 6.5]. Thus, if $z_1^{k_1-1} \cdots z_t^{k_t-1} \neq 0$, we may conclude

$$\operatorname{soc}(R) = (z_1^{k_1-1} \cdots z_t^{k_t-1}). \tag{3.23}$$

Example 3.20 (see also [42, Prop. 3.3])**.** Consider the ring $R = \mathbb{F}_2[x, y]/(x^2+y^2, xy)$. Then $\mathfrak{m} = (x, y)$. We have $x^2 = y^2 \neq 0$ and $x^3 = y^3 = 0$. Thus the nilpotency index of both x and y is 3. Yet $x^2y^2 = xy = 0$ and thus (3.23) cannot be true in this case. In fact $\operatorname{soc}(R) = (x^2) = (y^2)$.

Before continuing with the main results of this section we discuss a special class of commutative local Frobenius rings and their properties. A commutative ring R is called **chain ring** if it is local and every ideal is principal. Obviously a chain ring is Frobenius since by definition its socle is principal. In the following remark we list some basic properties.

Remark 3.21. Let R be a chain ring. Then the following hold:

(1) Let γ be a generator of the maximal ideal $\mathfrak{m}$, that is, $\mathfrak{m} = (\gamma)$. If ν is the smallest integer such that $\gamma^{\nu} = 0$, then

$$0 = (\gamma^{\nu}) \subsetneq (\gamma^{\nu-1}) \subsetneq \cdots \subsetneq \mathfrak{m} = (\gamma) \subsetneq R \tag{3.24}$$

forms a chain[1] of **all** ideals of R. As a consequence, $\operatorname{soc}(R) = (\gamma^{\nu-1})$.

(2) Thanks to (3.22) we have $(\gamma^{\nu-1}) = (\gamma)^{\perp}$ and $(\gamma^{\nu-1})^{\perp} = (\gamma)$. In fact, for chain rings we have a stronger result. That is, for all $0 \leq i \leq \nu - 1$ we have $(\gamma^i)^{\perp} = (\gamma^{\nu-i-1})$.

[1] This is the reason why commutative local principal ideal rings are called chain rings.

The arithmetic of chain rings is quite simple due to (3.24) (and its consequences). This is in the heart of structural results on linear codes over chain rings discovered in [48, 49]. A commutative local Frobenius is not a chain ring iff its maximal ideal **is not** principal. Therefore, as we will see (e.g. Theorem 3.25), the arithmetic of a general commutative local Frobenius ring is messier than that of a chain ring. However, many of results from [48] remain true. It turns out that all we need is a cyclic socle rather than every ideal being principal.

We now return to general commutative local Frobenius rings. The socle $\mathrm{soc}(R) = \alpha R$ is an $\mathbb{F}$-vector space in a natural way. The map $\alpha r \longmapsto \overline{r} := r + \mathfrak{m}$ is an isomorphism of $\mathbb{F}$-vector spaces thanks to (3.22). For any $n \in \mathbb{N}$ this map extends to a $\mathbb{F}$-isomorphism

$$\rho : \alpha R^n \longrightarrow \mathbb{F}^n, \quad \alpha(r_1, \ldots, r_n) \longmapsto (\overline{r_1}, \ldots, \overline{r_n}). \tag{3.25}$$

We will write $\overline{r} := (\overline{r_1}, \ldots, \overline{r_n})$ for $r = (r_1, \ldots, r_n)$. Again thanks to (3.22) we have

$$\alpha r = 0 \iff \overline{r} = 0. \tag{3.26}$$

Thus ρ preserves the Hamming weight, and therefore it is a Hamming isometry.

We also have a R-linear surjective map induced by multiplication by α

$$m_\alpha : R^n \longrightarrow \alpha R^n, \quad r \longmapsto \alpha r.$$

Again, thanks to (3.22), we get $\ker m_\alpha = \mathfrak{m}^{(n)} := \{(r_1, \ldots, r_n) \mid r_i \in \mathfrak{m} \text{ for all } i\}$.

Definition 3.22. (1) For any $x \in R$, the **colon code** of a linear code $\mathcal{C} \leq R^n$ is defined as

$$(\mathcal{C} : x) := \{r \in R^n \mid xr \in \mathcal{C}\}.$$

(2) For any set $X \subseteq R^n$ we define the **reduction** $\overline{X} := \{\overline{x} \mid x \in X\}$, where $\overline{x} := x + \mathfrak{m}$. In other words

$$\overline{X} = \rho(\alpha X) = \{\rho(\alpha x) \mid x \in X\}.$$

Theorem 3.23. *Let $\{r_1, \ldots, r_k\} \subseteq R^n$. Then $\{r_1, \ldots, r_k\}$ is R-independent iff $\{\overline{r_1}, \ldots, \overline{r_n}\}$ is $\mathbb{F}$-independent. In particular, if $\mathcal{C} \leq R^n$ is a free code then $\dim_R(\mathcal{C}) = \dim_{\mathbb{F}}(\overline{\mathcal{C}})$.*

Proof. The first statement follows easily by (3.26). The second statement is an obvious corollary of the first one. □

Of particular interest for us will be the colon code $(\mathcal{C} : \alpha) = m_\alpha^{-1}(\mathcal{C})$, for which we have the following easily verifiable properties.

Proposition 3.24. *Let $\mathcal{C} \leq R^n$ be a linear code. Then*
(1) $\mathcal{C} \subseteq (\mathcal{C} : \alpha)$ and $\alpha(\mathcal{C} : \alpha) = \mathcal{C} \cap \alpha R^n \subseteq \mathcal{C}$.
(2) $\overline{\mathcal{C}}$ is a $\mathbb{F}$-vector space and $\overline{\mathcal{C}} = \rho(\alpha\mathcal{C}) \cong \alpha\mathcal{C} \cong \mathcal{C}/(\mathcal{C} \cap \mathfrak{m}^{(n)})$. In particular

$$|\overline{\mathcal{C}}| = \frac{|\mathcal{C}|}{|\mathcal{C} \cap \mathfrak{m}^{(n)}|}.$$

Theorem 3.25. *Let $\mathcal{C} \leq R^n$ be a linear code such that $\overline{\mathcal{C}} \neq 0$. Then $\mathrm{d_H}(\mathcal{C}) = \mathrm{d_H}\big(\overline{(\mathcal{C} : \alpha)}\big) \leq \mathrm{d_H}(\overline{\mathcal{C}})$.*

Proof. We saw in Proposition 3.24(1) that $\alpha(\mathcal{C} : \alpha) \subseteq \mathcal{C}$ and $\mathcal{C} \subseteq (\mathcal{C} : \alpha)$. Note that $\alpha(\mathcal{C} : \alpha) = 0$ iff $(\mathcal{C} : \alpha) \subseteq \mathfrak{m}$. The latter implies $\mathcal{C} \subseteq \mathfrak{m}$ and hence $\overline{\mathcal{C}} = 0$. As a consequence $\alpha(\mathcal{C} : \alpha) \neq 0$. This implies $\mathrm{d_H}(\mathcal{C}) \leq \mathrm{d_H}(\alpha(\mathcal{C} : \alpha))$. Making use of the $\mathrm{wt_H}$-preserving isomorphism ρ we get

$$\mathrm{d_H}(\mathcal{C}) \leq \mathrm{d_H}\left(\alpha(\mathcal{C} : \alpha)\right) = \mathrm{d_H}\left(\rho\left(\alpha(\mathcal{C} : \alpha)\right)\right) = \mathrm{d_H}\left(\overline{(\mathcal{C} : \alpha)}\right).$$

To achieve equality above, it is enough to show that $\mathrm{d_H}(\alpha(\mathcal{C} : \alpha)) \leq \mathrm{d_H}(\mathcal{C})$. We will do so by showing that for every $v \in \mathcal{C}$ there exists $0 \neq v' \in \alpha(\mathcal{C} : \alpha)$ such that $\mathrm{wt_H}(v') \leq \mathrm{wt_H}(v)$. Note first that for $v \in \mathcal{C}$, $v \in \alpha(\mathcal{C} : \alpha)$ iff $v = \alpha w$ for some $w \in R^n$. We write in this case $\alpha \mid v$. Write $\mathfrak{m} = (z_1, \ldots, z_t)$ and let $v \in \mathcal{C}$. Set $v^{(0)} := v$. If $\alpha \mid v^{(0)}$ then there is nothing to do. Otherwise, there exists a maximal k_1 such that $v^{(1)} := z_1^{k_1} v^{(0)} \neq 0$. Maximality of k_1 implies $z_1 v^{(1)} = 0$. If $\alpha \mid v^{(1)}$ we are done. Otherwise, there exists a maximal k_2 such that $v^{(2)} := z_2^{k_2} v^{(1)} \neq 0$. Again, maximality of k_2 implies $z_2 v^{(2)} = 0$. If $\alpha \mid v^{(2)}$ we are done, otherwise proceed similarly. In the worst case scenario, for $1 \leq i \leq t$, there exists a maximal k_i such that $v^{(i)} := z_i^{k_i} v^{(i-1)} \neq 0$ and $z_i v^{(i)} = 0$. Clearly $v^{(i)} \in \mathcal{C}$ and $\mathrm{wt_H}(v^{(i)}) \leq \mathrm{wt_H}(v)$ for all i. Note that maximality of k_i implies $z_i v^{(t)} = 0$ for all i. Hence $v^{(t)} \in \mathfrak{m}^\perp \times \cdots \times \mathfrak{m}^\perp$. Since $\mathfrak{m}^\perp = \alpha R$ we get that $\alpha \mid v^{(t)}$. Thus $v^{(t)} \in \alpha(\mathcal{C} : \alpha)$ and $\mathrm{wt_H}(v^{(t)}) \leq \mathrm{wt_H}(v)$.

Next, $\mathcal{C} \subseteq (\mathcal{C} : \alpha)$ implies $\overline{\mathcal{C}} \subseteq \overline{(\mathcal{C} : \alpha)}$. Since $\overline{\mathcal{C}} \neq 0$ we get $\overline{(\mathcal{C} : \alpha)} \neq 0$ and thus $\mathrm{d_H}\left(\overline{(\mathcal{C} : \alpha)}\right) \leq \mathrm{d_H}(\overline{\mathcal{C}})$. □

The next result gives a **standard form** for free codes and it constitutes the crucial step toward achieving the desired equality $\mathrm{d_H}(\mathcal{C}) = \mathrm{d_H}(\overline{\mathcal{C}})$.

Lemma 3.26. *Let $\mathcal{C} \leq R^n$ be a free code of dimension k. Then $\mathcal{C}$ is monomially[2] isometric with a free code of form $\mathcal{C}' = \mathrm{im}\,(I_k \mid M')$ for some matrix $M' \in \mathcal{M}_{k\times(n-k)}(R)$.*

Proof. Let $\{a_1, \ldots, a_k\}$ be a R-basis for $\mathcal{C}$. Then $\mathcal{C} = \mathrm{im}\, M$ where the ith row of $M \in R^{k\times n}$ is a_i. Note that a_1 has to have at least one unit because otherwise $\alpha a_1 = 0$. Permute the columns to bring a unit in the first column and then perform row operations to get a matrix of form

$$\left(\begin{array}{c|ccc} 1 & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & M_1 & \\ 0 & & & \end{array}\right).$$

By the same argument, the first row of M_1 has to have a unit (as long as $k > 1$) and we proceed similarly to get the desired shape. □

[2]Theorem 3.19 says that any Hamming isometry is a monomial map, so we call $\mathrm{wt_H}$-isometric codes **monomially** isometric.

Theorem 3.27. *Let $\mathcal{C} = \operatorname{im}(I_k \mid M)$. Then $\mathcal{C} \cap \alpha R^n = \alpha\mathcal{C}$. As a consequence $\overline{(\mathcal{C} : \alpha)} = \overline{\mathcal{C}}$ and $\mathrm{d_H}(\mathcal{C}) = \mathrm{d_H}(\overline{\mathcal{C}})$. As a consequence of Lemma 3.26, the same is true for any free code.*

Proof. Obviously $\alpha\mathcal{C} \subseteq \mathcal{C} \cap \alpha R^n$. Now let $a \in \mathcal{C} \cap \alpha R^n$. Then there exists $x \in R^k$ such that $a = x(I_k \mid M) = (x \mid xM) \in \alpha R^n$. Hence, there exists $y \in R^k$ such that $a = (\alpha y \mid \alpha yM) = \alpha(y \mid yM) \in \alpha\mathcal{C}$. Using Proposition 3.24(1), it follows that

$$\overline{(\mathcal{C} : \alpha)} = \rho(\alpha(\mathcal{C} : \alpha)) = \rho(\alpha\mathcal{C}) = \overline{\mathcal{C}}.$$

The above and Theorem 3.25 imply $\mathrm{d_H}(\mathcal{C}) = \mathrm{d_H}(\overline{\mathcal{C}})$. □

Recall from Remark 3.5 the notion of the dual of a linear code over R.

Corollary 3.28. *Let $\mathcal{C} \leq R^n$ be a free code of dimension k. Then $\mathcal{C}^\perp$ is free and $\dim_R(\mathcal{C}^\perp) = n - k$.*

Proof. Thanks to Lemma 3.26, we may assume without loss of generality that $\mathcal{C} = \operatorname{im}(I_k \mid M)$. Then $\operatorname{im}(-M^\intercal \mid I_{n-k}) \subseteq \mathcal{C}^\perp$. Equality follows from Remark 3.5 and Remark 2.1(7)(i). □

Remark 3.29. For a linear code $\mathcal{C} \leq R^n$ we have $\overline{\mathcal{C}^\perp} \subseteq \overline{\mathcal{C}}^\perp$. This containment is obviously strict in general. However, when $\mathcal{C}$ is a free code, Theorem 3.23 implies equality. In particular, thanks to Theorem 3.27, we have $\mathrm{d_H}(\mathcal{C}^\perp) = \mathrm{d_H}(\overline{\mathcal{C}}^\perp) = \mathrm{d_H}(\overline{\mathcal{C}^\perp})$.

Let R be a chain ring and $\mathcal{C} \leq R^n$ a linear code. With the same notation as in Remark 3.21, we have a chain of colon codes

$$\mathcal{C} = (\mathcal{C} : \gamma^0) \subseteq (\mathcal{C} : \gamma) \subseteq \cdots \subseteq (\mathcal{C} : \gamma^{\nu-1}) \subseteq (\mathcal{C} : \gamma^\nu) = R^n. \tag{3.27}$$

It turns out that the chain (3.27) is strongly related with the corresponding chain of $\mathcal{C}^\perp$. Indeed, for any $0 \leq i \leq \nu - 1$ the authors show in [48, Thm. 3.2(ii)]

$$\overline{(\mathcal{C}^\perp : \gamma^i)} = \overline{(\mathcal{C} : \gamma^{\nu-i-1})}^\perp. \tag{3.28}$$

When R is a commutative local Frobenius ring we have the following result that corresponds to the extremal cases $i = \nu - 1$ and $i = 0$.

Theorem 3.30. *Let $\mathcal{C} \leq R^n$ be a linear code. Then*
(1) $(\mathcal{C}^\perp : \alpha) = (\alpha\mathcal{C})^\perp$ and $\overline{(\mathcal{C}^\perp : \alpha)} = \overline{\mathcal{C}}^\perp$. As a consequence $\overline{\mathcal{C}}^\perp = \overline{(\alpha\mathcal{C})^\perp}$.
(2) $\overline{\mathcal{C}^\perp} = \overline{(\mathcal{C} : \alpha)}^\perp$.

Proof. (1) The first part of the statement follows by the chain of equivalences

$$\begin{aligned} r \in (\mathcal{C}^\perp : \alpha) &\iff \alpha r \in \mathcal{C}^\perp \\ &\iff (\alpha r) \cdot c = 0 \text{ for all } c \in \mathcal{C} \\ &\iff r \cdot (\alpha c) = 0 \text{ for all } c \in \mathcal{C} \\ &\iff r \in (\alpha\mathcal{C})^\perp. \end{aligned}$$

We next show $\overline{(\mathcal{C}^\perp : \alpha)} \subseteq \overline{\mathcal{C}}^\perp$. Let $x \in \overline{(\mathcal{C}^\perp : \alpha)}$ and $r \in (\mathcal{C}^\perp : \alpha)$ be such that $x = \overline{r}$. Then $\alpha r \in \mathcal{C}^\perp$. This yields $\alpha(r \cdot c) = (\alpha r) \cdot c = 0$ for all $c \in \mathcal{C}$. Making use of (3.26) we get $x \cdot \overline{c} = \overline{r} \cdot \overline{c} = 0$ for all $c \in \mathcal{C}$. Thus $x \in \overline{\mathcal{C}}^\perp$. Conversely, let $x \in \overline{\mathcal{C}}^\perp$ and $r \in R^n$ be such that $x = \overline{r}$. Then $\overline{r} \cdot \overline{c} = 0$ for all $c \in \mathcal{C}$. In other words $r \cdot (\alpha c) = 0$ for all $c \in \mathcal{C}$. This yields $r \in (\alpha\mathcal{C})^\perp = (\mathcal{C}^\perp : \alpha)$. Hence $x = \overline{r} \in \overline{(\mathcal{C}^\perp : \alpha)}$.
(2) Let $x \in \overline{\mathcal{C}^\perp}$ and $y \in \overline{(\mathcal{C} : \alpha)}$. Write $x = \overline{v}$ and $y = \overline{w}$ for some $v \in \mathcal{C}^\perp$ and $w \in (\mathcal{C} : \alpha)$. Then (3.26) implies

$$x \cdot y = 0 \iff \alpha(v \cdot w) = v \cdot (\alpha w) = 0.$$

But the last equality is true since $v \in \mathcal{C}^\perp$ and $\alpha w \in C$. Thus, we have $\overline{\mathcal{C}^\perp} \subseteq \overline{(\mathcal{C} : \alpha)}^\perp$ and $\overline{(\mathcal{C} : \alpha)} \subseteq \left(\overline{\mathcal{C}^\perp}\right)^\perp$. Thanks to part (1) and (2.17) we have

$$\overline{(\mathcal{C} : \alpha)} \subseteq \left(\overline{\mathcal{C}^\perp}\right)^\perp = \overline{\left((\mathcal{C}^\perp)^\perp : \alpha\right)} = \overline{(\mathcal{C} : \alpha)}.$$

This yields $\left(\overline{\mathcal{C}^\perp}\right)^\perp = \overline{(\mathcal{C} : \alpha)}$. Now (2.17) concludes the proof. □

Example 3.31. Let $R = \mathbb{F}_2[x, y]/(x^2, y^2)$. It is easy to see that $\mathfrak{m} = (x, y)$ and $\operatorname{soc}(R) = (xy)$; see also (3.23). In particular R is a (commutative) local Frobenius (non-chain) ring. Let $\mathcal{C} \leq R^3$ be the linear code generated by the codeword $c = (x, x, y)$. Since $xc = (0, 0, xy), yc = (xy, xy, 0) \in \mathcal{C}$ one computes

$$(\mathcal{C} : xy) = \operatorname{im} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{3.29}$$

Similarly one concludes

$$(\mathcal{C}^\perp : xy) = \operatorname{im} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = R^3. \tag{3.30}$$

Clearly $\overline{\mathcal{C}} = 0$ and thus $\overline{\mathcal{C}}^\perp = \mathbb{F}_2^3$. Moreover (3.30) implies $\overline{(\mathcal{C}^\perp : xy)} = \mathbb{F}_2^3$. It also follows from (3.29) that

$$\overline{\mathcal{C}^\perp} = \overline{(\mathcal{C} : xy)}^\perp = \operatorname{im} \begin{pmatrix} 1 & 1 & 0 \end{pmatrix} \leq \mathbb{F}_2^3.$$

The rate of a linear code $\mathcal{C} \leq R^n$ is defined as $\mathrm{r}(\mathcal{C}) := (\log_{|R|} |\mathcal{C}|)/n$. Thus, when $\mathcal{C}$ is a free code of dimension k, thanks to Theorem 3.23 we have $\mathrm{r}(\mathcal{C}) = \mathrm{r}(\overline{\mathcal{C}}) = k/n$. The following result tells us that free codes over local Frobenius rings are as good as linear codes over fields.

Theorem 3.32.

$$\max\{\mathrm{r}(\mathcal{C}) \mid \mathcal{C} \leq R^n, \mathcal{C} \textit{ free}, \mathrm{d_H}(\mathcal{C}) = d\} = \max\{\mathrm{r}(\mathcal{C}) \mid \mathcal{C} \leq \mathbb{F}^n, \mathrm{d_H}(\mathcal{C}) = d\}.$$

Proof. Let $\mathcal{C} \leq R^n$ be a free code. Then $\mathrm{d_H}(\mathcal{C}) = \mathrm{d_H}(\overline{\mathcal{C}})$ and $\mathrm{r}(\mathcal{C}) = \mathrm{r}(\overline{\mathcal{C}})$ imply " $\leq$ ". Conversely, let $\mathcal{C} \leq \mathbb{F}^n$ be a linear code of maximal rate $\mathrm{r}(\mathcal{C})$ and such that $\mathrm{d_H}(\mathcal{C}) = d$. If $\{x_1, \ldots, x_k\}$ is a $\mathbb{F}$-basis of $\mathcal{C}$, then $\{r_1, \ldots, r_k\}$ where $x_i = \overline{r_i}$ is R-independent thanks to Theorem 3.23. Thus $\operatorname{span}_R\{r_1, \ldots, r_k\} \leq R^n$ is a free code with the same rate and Hamming distance as $\mathcal{C}$. □

Chapter 4 Partitions of Frobenius Alphabets

In this chapter we discuss partitions of finite Frobenius bimodules and their character-theoretic duals. This generalizes the results in [17] where partitions of R^n with R a Frobenius ring were considered. We will first consider partitions of abelian groups and then, as usual, we will focus on the additive group of a Frobenius bimodule. The module structure will allow us to define a different notion of dual partition. Although the duality theory developed for partitions of Frobenius alphabets is interesting on its own, we will focus on weight partitions and use the theory to prove extensions theorems in the next chapter.

We start with some general notations. Let $\mathcal{P} = (P_k)_{k=1}^K$ be a partition of a finite set X, i.e., X is the disjoint union of the subsets $P_1, \dots, P_K$. The sets P_k are called **blocks**, and $|\mathcal{P}| = K$ is the number of blocks of $\mathcal{P}$ (assuming all blocks are nonempty). A partition $\mathcal{P}$ is called **finer** than the partition $\mathcal{Q}$ if every block of $\mathcal{P}$ is contained in some block of $\mathcal{Q}$. In this case we write $\mathcal{P} \le \mathcal{Q}$, and it follows that $|\mathcal{Q}| \le |\mathcal{P}|$. Two partitions $\mathcal{P}$, $\mathcal{Q}$ of X are called **identical** if $\mathcal{P} \le \mathcal{Q}$ and $\mathcal{Q} \le \mathcal{P}$. We will denote by $\sim_{\mathcal{P}}$ the equivalence relation induced by the partition $\mathcal{P}$, that is, $x_1 \sim_{\mathcal{P}} x_2$ iff there exists a (unique) block P_i that contains x_1, x_2. Note that if $\mathcal{P} \le \mathcal{Q}$ then $x_1 \sim_{\mathcal{P}} x_2$ implies $x_1 \sim_{\mathcal{Q}} x_2$.

Definition 4.1. Let G be a finite abelian group and $\mathcal{P} = (P_k)_{k=1}^K$ be a partition of G. The **dual partition** of $\mathcal{P}$, denoted by $\widehat{\mathcal{P}}$, is the partition of $\widehat{G}$ defined via the equivalence relation

$$\psi \sim_{\widehat{\mathcal{P}}} \psi' \iff \sum_{g \in P_k} \psi(g) = \sum_{g \in P_k} \psi'(g) \quad \text{for all} \quad k = 1, \dots, K.$$

We call $\mathcal{P}$ **reflexive** if $\mathcal{P} = \widehat{\widehat{\mathcal{P}}}$ (where we identify G and $\widehat{\widehat{G}}$).

In the following remark we list some properties of $\widehat{\mathcal{P}}$ and $\widehat{\widehat{\mathcal{P}}}$ of a given partition $\mathcal{P}$.

Remark 4.2.
(1) $\widehat{\mathcal{P}} = -\widehat{\mathcal{P}} = \widehat{-\mathcal{P}}$, where $-\mathcal{P} = -P_1, \dots, -P_K$ and $-P_k := \{-g \mid g \in P_k\}$.
(2) If $\mathcal{P} \le \mathcal{Q}$ then $\widehat{\mathcal{P}} \le \widehat{\mathcal{Q}}$.
(3) The singleton $\{\varepsilon_G\}$ is always a block of $\widehat{\mathcal{P}}$.
(4) $|\mathcal{P}| \le |\widehat{\mathcal{P}}|$ and $\widehat{\widehat{\mathcal{P}}} \le \mathcal{P}$. Furthermore, $|\mathcal{P}| = |\widehat{\mathcal{P}}| \iff \mathcal{P} = \widehat{\widehat{\mathcal{P}}}$; see [17, Thm. 2.4].

From now on, let A be a finite Frobenius bimodule with generating character χ. As it is customary in coding theory, we will consider $a \in A^n$ as row vector and otherwise we will write $a^\top$. Clearly A^n is also a R-bimodule. Recall from (2.13) the (R, R)-bilinear isomorphism

$$\widehat{A}^n \cong \widehat{A^n} \quad \text{via} \quad (\chi_1, \dots, \chi_n)(a_1, \dots, a_n) := \prod_{j=1}^n \chi_j(a_j). \tag{4.1}$$

In particular $\widehat{R^n} \cong \widehat{R}^n$, and therefore $|A^n| = |\widehat{A}^n| = |R^n| = |\widehat{R}^n|$. Let $\langle \bullet, \bullet \rangle$ denote both the standard dot products $A^n \times R^n \longrightarrow A$, $\langle a, r \rangle := ar^{\mathsf{T}} = \sum_{i=1}^n a_i r_i$ and $R^n \times A^n \longrightarrow A$, $\langle r, a \rangle := ra^{\mathsf{T}} = \sum_{i=1}^n r_i a_i$. Thanks to Proposition 2.11 these bilinear forms are non-degenerate; see Definition 3.2(1).

We now are ready to define specific left and right dual partitions in R^n and A^n using the module structure and Frobeniusness.

Definition 4.3. For a partition $\mathcal{P} = (P_k)_{k=1}^K$ of R^n the χ-**left dual** and χ-**right dual partitions** are the partitions of A^n defined via

$$a \sim_{\widehat{\mathcal{P}}^{[\chi,l]}} a' \iff \sum_{r \in P_k} \chi(\langle r, a \rangle) = \sum_{r \in P_k} \chi(\langle r, a' \rangle) \text{ for all } k = 1, \ldots, K,$$

and

$$a \sim_{\widehat{\mathcal{P}}^{[\chi,r]}} a' \iff \sum_{r \in P_k} \chi(\langle a, r \rangle) = \sum_{r \in P_k} \chi(\langle a', r \rangle) \text{ for all } k = 1, \ldots, K.$$

Similarly, for a partition $\mathcal{Q} = (Q_k)_{k=1}^L$ of A^n the χ-**left dual** and χ-**right dual partitions** are the partitions of R^n defined by the equivalence relations

$$r \sim_{\widehat{\mathcal{Q}}^{[\chi,l]}} r' \iff \sum_{a \in Q_k} \chi(\langle a, r \rangle) = \sum_{a \in Q_k} \chi(\langle a, r' \rangle) \text{ for all } k = 1, \ldots, L,$$

and

$$r \sim_{\widehat{\mathcal{Q}}^{[\chi,r]}} r' \iff \sum_{a \in Q_k} \chi(\langle r, a \rangle) = \sum_{a \in Q_k} \chi(\langle r', a \rangle) \text{ for all } k = 1, \ldots, L.$$

The so defined dual partitions are very closely related with the dual notion of Definition 4.1. To see this we need some preparation. Recall the isomorphisms β_{l}, β_{r}, α_{l}, α_{r} from Remark 2.23. They extend to isomorphisms

$$\left.\begin{aligned} \beta_{\mathrm{l}} &: {}_R(A^n) \longrightarrow {}_R(\widehat{R}^n), \quad a \longmapsto \chi(\langle \bullet, a \rangle), \\ \beta_{\mathrm{r}} &: (A^n)_R \longrightarrow (\widehat{R}^n)_R, \quad a \longmapsto \chi(\langle a, \bullet \rangle) \end{aligned}\right\} \tag{4.2}$$

$$\left.\begin{aligned} \alpha_{\mathrm{l}} &: {}_R(R^n) \longrightarrow {}_R(\widehat{A}^n), \quad r \longmapsto \chi(\langle \bullet, r \rangle), \\ \alpha_{\mathrm{r}} &: (R^n)_R \longrightarrow (\widehat{A}^n)_R, \quad r \longmapsto \chi(\langle r, \bullet \rangle) \end{aligned}\right\} \tag{4.3}$$

It follows directly by the definitions above that

$$\alpha_{\mathrm{l}}(r)(a) = \chi(\langle a, r \rangle) = \chi\Big(\sum_{i=1}^n a_i r_i\Big) = \prod_{i=1}^n (r_i \chi)(a_i),$$

and thus with the identification (4.1) we obtain the isomorphism

$$\alpha_{\mathrm{l}} : {}_R(R^n) \longrightarrow {}_R(\widehat{A}^n), \quad r \longmapsto (r_1\chi, \ldots, r_n\chi) \tag{4.4}$$

$$\alpha_{\mathrm{r}} : (R^n)_R \longrightarrow (\widehat{A}^n)_R, \quad r \longmapsto (\chi r_1, \ldots, \chi r_n) \tag{4.5}$$

Again thanks to Proposition 2.11 we have $r_i\chi = \varepsilon_A$ iff $r_i = 0$ and thus both α_{l} and α_{r} are Hamming isometries. Similarly we have $\beta_{\mathrm{l}}(a) = (\chi(\bullet a_1), \ldots, \chi(\bullet a_n))$ for all

$a \in A^n$ and likewise for β_{r}.

The isomorphisms in (4.2) and (4.3) satisfy the simple relations

$$\alpha_{\mathrm{l}}(r)(a) = \beta_{\mathrm{r}}(a)(r) \quad \text{and} \quad \alpha_{\mathrm{r}}(r)(a) = \beta_{\mathrm{l}}(a)(r) \quad \text{for all } r \in R^n,\, a \in A^n; \tag{4.6}$$

see also (2.28). These isomorphisms will be crucial for developing a duality theory for partitions.

As mentioned we have the following straightforward observations.

Remark 4.4.

(1) Let $\mathcal{P}$ be a partition of R^n and $\mathcal{Q}$ be a partition of A^n. Then
   (i) $\widehat{\mathcal{P}}^{[\chi,l]} := {\beta_{\mathrm{l}}}^{-1}(\widehat{\mathcal{P}})$ and $\widehat{\mathcal{P}}^{[\chi,r]} := {\beta_{\mathrm{r}}}^{-1}(\widehat{\mathcal{P}})$.
   (ii) $\widehat{\mathcal{Q}}^{[\chi,l]} := {\alpha_{\mathrm{l}}}^{-1}(\widehat{\mathcal{Q}})$ and $\widehat{\mathcal{Q}}^{[\chi,r]} := {\alpha_{\mathrm{r}}}^{-1}(\widehat{\mathcal{Q}})$.
   As a consequence of Remark 4.2(4), for each partition $\mathcal{P}$ of R^n or A^n we have

$$|\widehat{\mathcal{P}}^{[\chi,l]}| = |\widehat{\mathcal{P}}^{[\chi,r]}| = |\widehat{\mathcal{P}}| \geq |\mathcal{P}|. \tag{4.7}$$

(2) The dual partitions of Definition 4.3 clearly depend on the choice of the generating character χ. But this can easily be described. Suppose χ' is another generating character of A. Then thanks to (2.21) we can write $\chi' = u\chi = \chi\tilde{u}$ for some units $u, \tilde{u} \in R^*$. As a consequence, $\chi'(\langle r, a\rangle) = \chi(\langle r, au\rangle)$ and therefore for any partition $\mathcal{P}$ of R^n we have $a \sim_{\widehat{\mathcal{P}}^{[\chi',l]}} a' \iff au \sim_{\widehat{\mathcal{P}}^{[\chi,l]}} a'u$ and thus $\widehat{\mathcal{P}}^{[\chi',l]}u = \widehat{\mathcal{P}}^{[\chi,l]}$, where the latter means that each block is right multiplied by u. In the same way $\tilde{u}\widehat{\mathcal{P}}^{[\chi',r]} = \widehat{\mathcal{P}}^{[\chi,r]}$. Analogous relations hold true for the duals of partitions of A^n.

Remark 4.4 allows us to prove the following analogue of [6, Prop. 4.4].

Theorem 4.5. *Let $\mathcal{P}$ be any partition of R^n or A^n. Then*

$$\widehat{\widehat{\mathcal{P}}^{[\chi,l]}}^{[\chi,r]} = \widehat{\widehat{\mathcal{P}}} = \widehat{\widehat{\mathcal{P}}^{[\chi,r]}}^{[\chi,l]},$$

where $\widehat{\widehat{\mathcal{P}}}$ is the bidual in the sense of Definition 4.1. As a consequence,

$$\mathcal{P} \text{ is reflexive} \iff \mathcal{P} = \widehat{\widehat{\mathcal{P}}^{[\chi,l]}}^{[\chi,r]} \iff \mathcal{P} = \widehat{\widehat{\mathcal{P}}^{[\chi,r]}}^{[\chi,l]}.$$

Proof. Let $\mathcal{P}$ be a partition of A^n. Set $\mathcal{Q} = (Q_k)_{k=1}^N = \widehat{\mathcal{P}}^{[\chi,l]}$ and $\mathcal{R} = \widehat{\mathcal{Q}}^{[\chi,r]} = {\beta_{\mathrm{r}}}^{-1}(\widehat{\mathcal{Q}})$. Let $a, a' \in A^n$. With the aid of (4.6) we compute

$$\begin{aligned} a \sim_{\mathcal{R}} a' &\iff \beta_{\mathrm{r}}(a) \sim_{\widehat{\mathcal{Q}}} \beta_{\mathrm{r}}(a') \\ &\iff \sum_{r \in Q_k} \beta_{\mathrm{r}}(a)(r) = \sum_{r \in Q_k} \beta_{\mathrm{r}}(a')(r) \quad \text{for all } k = 1, \dots, N \\ &\iff \sum_{r \in Q_k} \alpha_{\mathrm{l}}(r)(a) = \sum_{r \in Q_k} \alpha_{\mathrm{l}}(r)(a') \quad \text{for all } k = 1, \dots, N \end{aligned}$$

$$\begin{aligned}
&\iff \sum_{\Psi\in\alpha_l(Q_k)} \Psi(a) = \sum_{\Psi\in\alpha_l(Q_k)} \Psi(a') \text{ for all } k = 1,\dots,N\\
&\iff a\sim_{\widehat{\alpha_l(\mathcal{Q})}} a'\\
&\iff a\sim_{\widehat{\widehat{\mathcal{P}}}} a'.
\end{aligned}$$

This establishes $\widehat{\widehat{\mathcal{P}}^{[\chi,l]}}^{[\chi,r]} = \widehat{\widehat{\mathcal{P}}}$. The other identity as well as those for partitions of R^n are shown in the same way. The rest follows. □

For a matrix $M \in R^{n\times m}$ and for $a \in A^n$ we have aM, $(Ma^\mathsf{T})^\mathsf{T} \in A^m$ in the obvious way. This gives rise to the following group actions. Their orbits will play a crucial role later on.

Definition 4.6. Let $\mathcal{U}$ be a subgroup of $\mathrm{GL}_n(R)$. Then $\mathcal{U}$ induces a right and left group action[1] on A^n via

$$A^n \times \mathcal{U} \longrightarrow A^n,\ (a,U) \longmapsto aU \quad\text{and}\quad \mathcal{U}\times A^n \longrightarrow A^n,\ (U,a)\longmapsto (Ua^\mathsf{T})^\mathsf{T}.$$

Denote by $\mathcal{P}_{A^n,\mathcal{U}}$ and $\mathcal{P}_{A^n,\mathcal{U}^\mathsf{T}}$ the respective orbit partitions on A^n.

Remark 4.7. Let $\omega : A^n \longrightarrow \mathbb{R}$ be a weight function. Then ω induces a **weight partition** $\mathcal{P}_\omega$ via $a\sim_{\mathcal{P}_\omega} a' \iff \omega(a) = \omega(a')$. A map $f : A^n \longrightarrow A^n$ is ω-isometry iff $a\sim_{\mathcal{P}_\omega} f(a)$ for all $a \in A^n$. This allows us to study the structure of ω-isometries by realizing $\mathcal{P}_\omega$ as a orbit partition induced by some subgroup $\mathcal{U} \le \mathrm{GL}_n(R)$, and will be the main tool used in the next chapter.

The orbit partitions of group actions defined above have interesting duality relations. We address this with the following two results.

Lemma 4.8. *Let $\mathcal{U}$ be a subgroup of $\mathrm{GL}_n(R)$. Then*
(1) $\mathcal{P}_{R^n,\mathcal{U}} \le \widehat{\mathcal{P}_{A^n,\mathcal{U}^\mathsf{T}}}^{[\chi,r]}$ *and* $\mathcal{P}_{R^n,\mathcal{U}^\mathsf{T}} \le \widehat{\mathcal{P}_{A^n,\mathcal{U}}}^{[\chi,l]}$.
(2) $\mathcal{P}_{A^n,\mathcal{U}} \le \widehat{\mathcal{P}_{R^n,\mathcal{U}^\mathsf{T}}}^{[\chi,r]}$ *and* $\mathcal{P}_{A^n,\mathcal{U}^\mathsf{T}} \le \widehat{\mathcal{P}_{R^n,\mathcal{U}}}^{[\chi,l]}$.

Proof. Set $\mathcal{P} := \mathcal{P}_{R^n,\mathcal{U}}$, $\mathcal{Q} := \mathcal{P}_{A^n,\mathcal{U}^\mathsf{T}}$. Let $r, r' \in R^n$ be such that $r\sim_{\mathcal{P}} r'$, thus $r' = rU$ for some $U \in \mathcal{U}$. Then for any $a \in A^n$ we have $\langle r', a\rangle = \langle rU, a\rangle = \langle r, (Ua^\mathsf{T})^\mathsf{T}\rangle$. Let Q be any block of $\mathcal{Q}$. Then the closedness of Q under the left action of $\mathcal{U}$ yields

$$\sum_{a\in Q} \chi(\langle r', a\rangle) = \sum_{a\in Q} \chi(\langle r, (Ua^\mathsf{T})^\mathsf{T}\rangle) = \sum_{a\in Q} \chi(\langle r, a\rangle).$$

This shows $r\sim_{\widehat{\mathcal{Q}}^{[\chi,r]}} r'$. The other relations are shown in the same way. □

Theorem 4.9. *Let $\mathcal{U}$ be a subgroup of $\mathrm{GL}_n(R)$. Then*

$$\begin{aligned}
\mathcal{P}_{R^n,\mathcal{U}} &= \widehat{\mathcal{P}_{A^n,\mathcal{U}^\mathsf{T}}}^{[\chi,r]}, & \mathcal{P}_{R^n,\mathcal{U}^\mathsf{T}} &= \widehat{\mathcal{P}_{A^n,\mathcal{U}}}^{[\chi,l]},\\
\mathcal{P}_{A^n,\mathcal{U}} &= \widehat{\mathcal{P}_{R^n,\mathcal{U}^\mathsf{T}}}^{[\chi,r]}, & \mathcal{P}_{A^n,\mathcal{U}^\mathsf{T}} &= \widehat{\mathcal{P}_{R^n,\mathcal{U}}}^{[\chi,l]}.
\end{aligned}$$

As a consequence, all these partitions are reflexive. Moreover, the right (resp. left) group action of $\mathcal{U}$ on R^n and the left (resp. right) action of $\mathcal{U}$ on A^n lead to the same number of orbits.

[1] Of course these actions can be defined on any (R,R)-bimodule. In particular on R^n.

Proof. Combining Remark 4.4(1) and Lemma 4.8 we obtain

$$|\mathcal{P}_{R^n,\mathcal{U}}| \geq |\widehat{\mathcal{P}_{A^n,\mathcal{U}^\intercal}}^{[\chi,r]}| \geq |\mathcal{P}_{A^n,\mathcal{U}^\intercal}| \geq |\mathcal{P}_{R^n,\mathcal{U}}|.$$

Thus we have equality everywhere, and again with Lemma 4.8 we arrive at the first identity. Next, by applying Theorem 4.5 on the first identity we obtain the forth identity. The two left are shown in the same way. □

Remark 4.10. We mentioned in Remark 4.7 that the main idea is to realize the partition $\mathcal{P}_\omega$ induced by a weight function ω as the orbit partition of some subgroup of $\mathrm{GL}_n(R)$. Let $\mathcal{U} \coloneqq G_{\omega,r}$, where $G_{\omega,r}$ is the right symmetry group defined in (3.10), and consider the orbit partition $\mathcal{P} = \mathcal{P}_{A^n,\mathcal{U}}$ as in Definition 4.6. It follows from the very definitions that $\mathcal{P} \leq \mathcal{P}_\omega$, that is, $\mathcal{P}_\mathcal{U}$ is a finer partition than $\mathcal{P}_\omega$. As we will see in the next chapter, for nicely behaved weight functions we have equality $\mathcal{P} = \mathcal{P}_\omega$. In turn, thanks to Theorem 4.9, this implies that $\mathcal{P}_\omega$ is reflexive. We will see in the next chapter that the reflexivity of $\mathcal{P}_\omega$ is crucial for understanding ω-isometries.

We are now ready to prove the following crucial result for the next chapter.

Lemma 4.11. *Let $\mathcal{C} \leq {}_RA^n$ be a linear code and let $\mathcal{U}$ be a subgroup of $\mathrm{GL}_n(R)$. Assume $f : \mathcal{C} \longrightarrow A^n$ is a linear map such that for all $x \in \mathcal{C}$ there exists a matrix $U_x \in \mathcal{U}$ such that $f(x) = xU_x$. Then, for all $r \in R^n$ there exists a matrix $M_r \in \mathcal{U}$ such that $\langle f(x), r\rangle = xM_r r^\intercal$ for all $x \in \mathcal{C}$.*

Proof. Let P be a block of $\mathcal{P}_{R^n,\mathcal{U}^\intercal} = \widehat{\mathcal{P}_{A^n,\mathcal{U}}}^{[\chi,l]}$. Then for all $x \in \mathcal{C}$

$$\sum_{r\in P} \chi(\langle f(x), r\rangle) = \sum_{r\in P} \chi(\langle xU_x, r\rangle) = \sum_{r\in P} \chi(\langle x, (U_x r^\intercal)^\intercal\rangle) = \sum_{r\in P} \chi(\langle x, r\rangle),$$

where the last step follows from the invariance of P under the left action of $\mathcal{U}$. As a consequence,

$$\sum_{r\in P} \chi(\langle f(\bullet), r\rangle) = \sum_{r\in P} \chi(\langle \bullet, r\rangle)$$

and each side of the identity is a sum of elements in the character group $\widehat{\mathcal{C}}$. Fix $r \in R^n$ and assume that r is contained in the block P of $\mathcal{P}_{R^n,\mathcal{U}^\intercal}$. Remark 2.1(5) implies that the character $\chi(\langle f(\bullet), r\rangle)$ must appear on the right hand side of the above identity. In other words, there exists $r' \in P$ i.e., $r' = (M_r r^\intercal)^\intercal$ for some $M_r \in \mathcal{U}$, such that $\chi(\langle f(\bullet), r\rangle) = \chi(\langle \bullet, r'\rangle)$. Thanks to Theorem 2.22 we conclude that $\langle f(\bullet), r\rangle = \langle \bullet, r'\rangle$ as maps in $\mathrm{Hom}({}_R\mathcal{C}, {}_RA)$. This implies $\langle f(x), r\rangle = \langle x, (M_r r^\intercal)^\intercal\rangle = xM_r r^\intercal$, as desired. □

We end this chapter with some examples.

Example 4.12.

(1) If the ring R is Frobenius as well, Theorem 4.9 implies

$$|\mathcal{P}_{R^n,\mathcal{U}}| = |\mathcal{P}_{A^n,\mathcal{U}^\intercal}| = |\mathcal{P}_{A^n,\mathcal{U}}| = |\mathcal{P}_{A^n,\mathcal{U}^\intercal}|.$$

In other words, the right and left action of $\mathcal{U}$ leads to the same number of orbits. However, this is not the case if the ring R is not Frobenius. Consider the commutative non-Frobenius ring $R = \mathbb{F}_2[x,y]/(x^2,y^2,xy)$; see Example 2.32(2). Let A be the Frobenius bimodule $A = \widehat{R}$ and let

$$\mathcal{U} = \left\{ \begin{pmatrix} 1 & r \\ 0 & u \end{pmatrix} \middle| \, r \in R,\, u \in R^* \right\}.$$

Then one can compute that both, $\mathcal{P}_{R^2,\mathcal{U}}$ and $\mathcal{P}_{A^2,\mathcal{U}^\intercal}$, consist of 17 orbits whereas $\mathcal{P}_{R^2,\mathcal{U}^\intercal}$ and $\mathcal{P}_{A^2,\mathcal{U}}$ consist of 20 orbits.

(2) We will focus on weight partitions in the next chapter. However, we address here a particularly easy case. Let $\mathcal{P}_{\mathrm{wt_H}}$ be the Hamming partition on A, that is, $a \sim_{\mathcal{P}_{\mathrm{wt_H}}} a'$ iff $\mathrm{wt_H}(a) = \mathrm{wt_H}(a')$ for all $a, a' \in A$. By the very definition of the Hamming weight, it follows that $\mathcal{P}_{\mathrm{wt_H}}$ has two blocks. Namely $\{0\}$ and $A \setminus \{0\}$. By Remark 4.2(3) we always have that $\{\varepsilon_A\}$ is a block of $\widehat{\mathcal{P}_{\mathrm{wt_H}}}$. It follows by the orthogonality relations (2.1) that $\widehat{A} \setminus \{\varepsilon_A\}$ is also a block of $\mathcal{P}_{\mathrm{wt_H}}$. Thanks to Remark 4.2(4) we conclude that $\mathcal{P}_{\mathrm{wt_H}}$ is reflexive. In fact, the same is true for the Hamming weight on A^n. In this case $\mathcal{P}_{A^n,\mathrm{wt_H}} = (P_k)_{k=1}^n$ where $P_k = \{a \in A^n \mid \mathrm{wt_H}(a) = k\}$; see [17, Ex. 2.3(c)]. In addition, we have

$$\widehat{\mathcal{P}_{A^n,\mathrm{wt_H}}}^{[\chi,l]} = \widehat{\mathcal{P}_{A^n,\mathrm{wt_H}}}^{[\chi,r]} = \mathcal{P}_{R^n,\mathrm{wt_H}}.$$

Making use of the $\mathrm{wt_H}$-isometries α_{l} and α_{r}, and the reflexivity of the Hamming partition, we also have

$$\widehat{\mathcal{P}_{R^n,\mathrm{wt_H}}}^{[\chi,l]} = \widehat{\mathcal{P}_{R^n,\mathrm{wt_H}}}^{[\chi,r]} = \mathcal{P}_{A^n,\mathrm{wt_H}}.$$

(3) Consider the weight partition $\mathcal{P}_{\mathrm{swc}}$ induced by the symmetrized weight composition swc. Then (3.7) implies $\mathcal{P}_{\mathrm{swc}} \leq \mathcal{P}_{\mathrm{wt_H}}$. This yields $|\mathcal{P}_{\mathrm{wt_H}}| \leq |\mathcal{P}_{\mathrm{swc}}|$, and $|\widehat{\mathcal{P}_{\mathrm{wt_H}}}| \leq |\widehat{\mathcal{P}_{\mathrm{swc}}}|$ thanks to Remark 4.2.

Chapter 5 Equivalence of Classical Codes

In this chapter we study the equivalence of linear codes over Frobenius bimodules. We use tools from the duality theory of partitions developed in the previous chapter. The goal is to understand the structure of ω-isometries of a linear code $\mathcal{C} \leq_R A^n$ for a given weight function ω. In Theorem 3.16 and Remark 3.17 we establish the structure of various isometries for the extremal case $\mathcal{C} = A^n$. On the other hand, Theorem 3.19 gives the structure of all Hamming isometries $f : \mathcal{C} \subsetneq A^n \longrightarrow A^n$. Namely, f is a Hamming isometry iff f is a monomial map; see Remark also 3.18(1). This means that f can be extended to a Hamming isometry $\tilde{f} : A^n \longrightarrow A^n$. Or in other words, any isometry $f : \mathcal{C} \subsetneq A^n \longrightarrow A^n$ is the restriction of Hamming isometry $\tilde{f} : A^n \longrightarrow A^n$. For these reasons Theorem 3.19 is known in the literature as the **MacWilliams Extension Theorem**.

In general, given an alphabet A and a weight function ω, the structure of ω-isometries of the ambient space A^n is easily seen. So one can ask what is the structure of ω-isometries $\mathcal{C} \longrightarrow A^n$? Do they extend to an ω-isometry of A^n? These questions are well studied in literature. We provide answers to some open questions as well as alternative proofs to existing answers.

5.1 Variations of MacWilliams Extension Theorem

Throughout this section A is a finite Frobenius bimodule and $\chi \in \widehat{A}$ is a generating character. For a given weight ω we will establish whether or not ω-isometries $f : \mathcal{C} \subsetneq A^n$ are restriction of ω-isometries of A^n. We start with a definition.

Definition 5.1. Let ω be a weight function on a module ${}_RV$. Then ω **satisfies the MacWilliams Extension Property** if for any code $\mathcal{C} \leq_R V$ every ω-isometry $f : \mathcal{C} \longrightarrow V$ can be extended to an ω-isometry of V.

The above definition deviates from others uses in literature in the sense that the length of the code is fixed through the module V. This is necessary so that we can also deal with weights that do not arise as the extension of a weight on the alphabet as in (3.6). Yet, the above definition covers various cases. For instance, if $V = A^n$ is endowed with the Hamming weight with respect to the alphabet A, the above is the classical MacWilliams extension property for module alphabets. On the other hand, if we endow V with the Hamming weight (with respect to V), then the Hamming isometries are precisely linear injective maps. In this case the extension property asks whether injective maps on submodules extend to injective maps of the entire module. The latter is closely related with the notions of **injective** and **pseudo-injective** modules. A left R-module V is called **injective** if for any pair of left R-modules $M_1 \leq M_2$, any linear map $f : M_1 \longrightarrow V$ can be extended to a linear map $\widetilde{f} : M_2 :\longrightarrow V$. On the other hand, V is called **pseudo-injective** if for every submodule $\mathcal{C} \leq_R V$, any injective linear map $f : \mathcal{C} \longrightarrow V$ can be extended to a linear

map $\tilde{f} : V \longrightarrow V$. In general, there is no reason to expect $\tilde{f}$ to be injective. However, Dihn and López-Permouth [12, Prop. 3.2] show that this is actually the case[1].

Theorem 5.2. *Let $\mathcal{C} \leq_R V$ be a linear code and $f : \mathcal{C} \longrightarrow V$ be a linear injective map. Then f extends to an injective map $\tilde{f} : \mathcal{C} \longrightarrow V$ iff V is pseudo-injective.*

Note that the above theorem says that the Hamming weight on an alphabet A satisfies the extension property for linear codes of length one iff the alphabet A is pseudo-injective. Jay Wood [69, Thm. 5.2, Thm. 6.2] pushed Theorem 5.2 one step further.

Theorem 5.3. *Let $V = A^n$. The Hamming weight on A^n (with respect to A) satisfies the extension property iff A is pseudo-injective and has a cyclic socle.*

Recall that a Frobenius bimodule A has a cyclic socle; see also 2.17(2). We also mentioned in Section 2.2 that the character bimodule $\widehat{R}$ is injective. In particular $\widehat{R}$ is pseudo-injective, and thus so is ${}_RA \cong {}_R\widehat{R}$. In other words, the above theorem implies Theorem 3.19. We provide an alternative proof of the latter using tools from Chapter 4.

Alternative proof of Theorem 3.19. We use the same notation as in the proof of Theorem 3.19 and Remark 3.18(2). Let $f : \mathcal{C} \longrightarrow A^n$ be a Hamming isometry. Recall that we need to find a permutation $\pi \in S_n$ and units $u_j \in R^*$ such that $\iota_j = f_{\pi(j)}u_j$.

Let $\mathcal{P}$ be the Hamming partition on A^n as in Example 4.12(2). As mentioned $\widehat{\mathcal{P}}^{[\chi,l]}$ is again the Hamming partition on R^n. Thus $Q := \{re_i \mid 0 \neq r \in R, i \in [n]\}$, where $\{e_1, \ldots, e_n\}$ is the standard basis of R^n, is a block of $\widehat{\mathcal{P}}^{[\chi,l]}$. As in Lemma 4.11 (the proof) we obtain

$$\sum_{z\in Q} \chi(\langle \bullet, z\rangle) = \sum_{z\in Q} \chi(\langle f(\bullet), z\rangle) \tag{5.1}$$

as sum of characters of $\mathcal{C}$. Now Remark 2.1(5) implies that $\chi(\langle \bullet, e_1\rangle)$ must appear on the right hand side of (5.1). In other words, there exists $0 \neq r_1 \in R$ and $\pi(1) \in [n]$ such that $\chi(\langle \bullet, e_1\rangle) = \chi(\langle f(\bullet), r_1 e_{\pi(1)}\rangle)$. Hence $\langle \bullet, e_1\rangle = \langle f(\bullet), r_1 e_{\pi(1)}\rangle$ as maps on $\mathcal{C}$. This yields $\iota_1 = f_{\pi(1)}r_1$. Similarly as in the proof of Theorem 3.19, r_1 can be chosen to be a unit, call it u_1.

Now consider $Q_i := \{re_i \mid 0 \neq r \in R\} \subset Q$. In fact Q is disjoint union of all the Q_i. We have

$$\begin{aligned}\sum_{x\in Q_1} \chi(\langle \bullet, x\rangle) &= \sum_{r\in R\setminus\{0\}} \chi(\langle \bullet, re_1\rangle) = \sum_{r\in R\setminus\{0\}} \chi(\langle \bullet, e_1\rangle r) \\ &= \sum_{r\in R\setminus\{0\}} \chi(\langle f(\bullet), u_1 e_{\pi(1)}\rangle r) \\ &= \sum_{x\in Q_{\pi(1)}} \chi(\langle f(\bullet), x\rangle).\end{aligned}$$

[1] Recall that V is finite.

Thus, (5.1) can be reduced to

$$\sum_{z\in Q\setminus Q_1}\chi(\langle\bullet,z\rangle)=\sum_{z\in Q\setminus Q_{\pi(1)}}\chi(\langle f(\bullet),z\rangle).$$

This enables us to repeat the same argument with the character $\chi(\langle f(\bullet),e_2\rangle)$ to produce a unit u_2 such that $\iota_2=f_{\pi(2)}u_2$. Proceeding in this way we arrive at the desired result. □

Now we consider the symmetrized weight composition with respect to $G\le S^*=\mathrm{Aut}({}_RA)$. Thanks to (2.24) we work with subgroups of units $G\le R^*$. The following result was proven in [14, Thm. 13] similarly as Theorem 3.19 and in [69, Thm. 8.1] using averaging characters. We provide a proof using the same strategy as above. Recall that the structure of swc-isometries for the extremal case $\mathcal{C}=A^n$ was given in Theorem 3.16(c).

Theorem 5.4. *Let $\mathcal{C}\le_R A^n$ be a linear code and $f:\mathcal{C}\longrightarrow A^n$ be a* swc*-isometry with respect to $G\le R^*$. Then there exists a matrix $M\in\mathrm{Mon}_{G,n}(R)$ such that $f(x)=xM$ for all $x\in\mathcal{C}$.*

Proof. Put $U=\mathrm{Mon}_{G,n}(R)$ and consider the partition $\mathcal{P}:=\mathcal{P}_{A^n,U}$ as in Definition 4.6. Then $Q:=\{ue_i\mid i\in[n],u\in G\}$ is a block of $\widehat{\mathcal{P}}^{[\chi,l]}=\mathcal{P}_{R^n,\mathcal{U}^\intercal}$ thanks to Theorem 4.9. This yields

$$\sum_{z\in Q}\chi(\langle\bullet,z\rangle)=\sum_{z\in Q}\chi(\langle f(\bullet),z\rangle).\tag{5.2}$$

Hence, there exist $u_1\in G$ and $\pi(1)\in[n]$ such that $\iota_1=f_{\pi(1)}u_1$. Again, using $Q_i:=\{ue_i\mid u\in G\}\subset Q$ we obtain

$$\sum_{z\in Q\setminus Q_{\pi(1)}}\chi(\langle\bullet,z\rangle)=\sum_{z\in Q\setminus Q_1}\chi(\langle f(\bullet),z\rangle),$$

which allows us to repeat the same argument on finding $u_2\in G$ and $\pi(2)$. □

It is obvious that when tools from Chapter 4 are used, the proofs of Theorems 3.19 and 5.4 are very similar. In fact both proofs fall under the same roof. We omit the proof of the following theorem to avoid unnecessary repetition. Recall that the Hamming partition and orbit partitions are reflexive.

Theorem 5.5 ([20, Thm. 4.14])**.** *Let $\mathcal{P}$ be a reflexive partition of ${}_RA^n$ and let $\mathcal{C}\le_R A^n$ be a linear code. Suppose $f:\mathcal{C}\longrightarrow A^n$ is a linear map that preserves the partition, that is,*

$$x\sim_{\mathcal{P}}f(x)\quad\text{for all } x\in\mathcal{C}.\tag{5.3}$$

Assume further that $S\subseteq R\setminus\{0\}$ is a subset such that the set $Q:=\{se_i\mid s\in S,i=1,\dots,n\}$ is a block of the dual partition $\widehat{\mathcal{P}}^{[\chi,l]}$. Then

(1) If S is a subgroup of R^* there exists a matrix $M\in\mathrm{Mon}_{S,n}(R)$ such that $f(x)=xM$ for all $x\in\mathcal{C}$.

(2) If $R^*S := \{\alpha s \mid \alpha \in R^*, s \in S\} = S$ *and* $1 \in S$ *there exists a matrix* $M \in \mathrm{Mon}_n(R)$ *such that* $f(x) = xM$ *for all* $x \in \mathcal{C}$.

We consider next the RT-weight and establish the structure of $\mathrm{wt}_{\mathrm{RT}}$-isometries. Recall that the RT-weight cannot be obtained via (3.6), and therefore we use the full power of Definition 5.1. We need first two preparatory results.

Lemma 5.6. *Let* A_R *be any finite module. Let* $\mathcal{C}, \mathcal{C}' \leq A^n$ *and* $f : \mathcal{C} \longrightarrow \mathcal{C}'$ *a bijective map. Suppose there exists a subring* S *of the matrix ring* $\mathcal{M}_n(R)$ *with the property*
(1) for all $x \in \mathcal{C}$ *there exists a matrix* $M'_x \in S$ *such that* $f(x) = xM'_x$,
(2) for all $y \in \mathcal{C}'$ *there exists a matrix* $M''_y \in S$ *such that* $f^{-1}(y) = yM''_y$.
Then there exists for every $x \in \mathcal{C}$ *a matrix* $M_x \in S^*$ *such that* $f(x) = xM_x$.

Proof. This is a simple consequence of Theorem 2.20. □

Theorem 5.7. *Let* $\mathcal{C} \leq A^n$ *be a linear code and let* $f : \mathcal{C} \longrightarrow A^n$ *be a* $\mathrm{wt}_{\mathrm{RT}}$*-isometry. Then, for all* $x \in \mathcal{C}$ *there exists a matrix* $M_x \in \mathrm{LT}_n(R)$ *such that* $f(x) = xM_x$.

Proof. Let $x = (x_1, \ldots, x_n) \in \mathcal{C}$ and set $f(x) = y = (y_1, \cdots, y_n)$. Since $\mathcal{C}_j := x_jR + \cdots + x_nR \leq A_R^n$ is a right module, we can make use of the double annihilator property (see Corollary 2.27) as well as Lemma 5.6. Note first that if $r \in {}^{\perp}\mathcal{C}_j$ then $\mathrm{wt}_{\mathrm{RT}}(ry) < j$. Since f is a $\mathrm{wt}_{\mathrm{RT}}$-isometry the latter yields

$$\mathrm{wt}_{\mathrm{RT}}(ry) = \mathrm{wt}_{\mathrm{RT}}(rf(x)) = \mathrm{wt}_{\mathrm{RT}}(f(rx)) = \mathrm{wt}_{\mathrm{RT}}(ry) < j.$$

In particular $ru_j = 0$ and thus ${}^{\perp}\mathcal{C}_j \subseteq {}^{\perp}(y_jR)$. Taking right annihilators and using the annihilator property we obtain $y_jR \subseteq \mathcal{C}_j$. In other words, there exist $m_{i,j} \in R$ such that $y_j = \sum_{i=j}^n x_i m_{i,j}$. Hence $y = f(x) = xM_x$ where $M_x = (m_{i,j})$ with $m_{i,j} = 0$ for $i < j$. This is precisely the condition on Lemma 5.6(1) above where S is the ring of lower triangular matrices.

Note now that $f^{-1} : f(\mathcal{C}) \longrightarrow \mathcal{C}$ is also a $\mathrm{wt}_{\mathrm{RT}}$-isometry. Proceeding similarly as above we see that the second condition on Lemma 5.6(2) is satisfied. Therefore, M_x can be chosen to be invertible, that is, $M_x \in \mathrm{LT}_n(R)$ for all $x \in \mathcal{C}$. □

Theorem 5.8. *Let* $\mathcal{C} \leq A^n$ *be a linear code and let* $f : \mathcal{C} \longrightarrow A^n$ *be a* $\mathrm{wt}_{\mathrm{RT}}$*-isometry. Then, there exists a matrix* $M \in \mathrm{LT}_n(R)$ *such that* $f(x) = xM$ *for all* $x \in \mathcal{C}$.

Proof. Thanks to Theorem 5.7, for all $x \in \mathcal{C}$ there exists $M_x \in \mathrm{LT}_n(R)$ such that $f(x) = xM_x$. Let $\{e_1, \ldots, e_n\}$ be the standard basis of ${}_RR^n$. Then Lemma 4.11 implies that for each $i \in [n]$ there exists $M_i \in \mathrm{LT}_n(R)$ such that $\langle f(x), e_i \rangle = xM_ie_i^{\top}$ for all $x \in \mathcal{C}$. Define the matrix $M = (M_1e_1^{\top}, \ldots, M_ne_n^{\top})$. Then M is clearly lower triangular and invertible because each M_i is. Furthermore, by construction $f(x) = xM$ for all $x \in \mathcal{C}$. □

Lastly, we establish the structure of ω-isometries where ω is the homogeneous weight on A extended additively on A^n via (3.6). They have been already classified in [23, Thm. 4.15] using the Möbius function. However, we take advantage of the useful formula of Theorem 3.7 and provide a much shorter proof. It is easy to see

that the partition induced by the homogeneous weight is not reflexive in general; see [16, Ex. 3.4(b)]. Therefore Theorem 5.5 cannot be applied in this case. However, the similarities between the Hamming weight and the homogeneous weight over a Frobenius alphabet are clear from Theorem 3.7 and Remark 3.18(2). Therefore, to no surprise, we can use the same techniques.

Theorem 5.9. *Let $\mathcal{C} \leq A^n$ be a linear code and let $f : \mathcal{C} \longrightarrow A^n$ be a linear map. Then f is an ω-isometry iff there exists a matrix $M \in \mathrm{Mon}_n(R)$ such that $f(x) = xM$ for all $x \in \mathcal{C}$.*

Proof. The "if part" is obvious. For the "only if part", consider $Q = \{ue_i \mid u \in R^*, i \in [n]\}$. Theorem 3.7 implies

$$\omega(x_1, \ldots, x_n) = n - \frac{1}{|R^*|} \sum_{i=1}^{n} \sum_{u \in R^*} \chi(x_i u) = n - \frac{1}{|R^*|} \sum_{y \in Q} \chi(\langle x, y \rangle).$$

Thus f is ω-preserving iff

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

But the latter is exactly (5.2) for the subgroup $S = R^*$. As usual, this is sufficient to obtain a matrix $M \in \mathrm{Mon}_n(R)$ such that $f(x) = xM$ for all $x \in \mathcal{C}$. □

Corollary 5.10. *A map $f : \mathcal{C} \longrightarrow A^n$ is wt_{H}-isometry iff it is ω-isometry. Moreover, an ω-isometry is injective*[2]*.*

The structure of $\mathrm{wt}_{\mathbb{P}}$-isometries for the extremal case $\mathcal{C} = A^n$ is given in Remark 3.17. To establish the general case we need the following definition. A poset $\mathbb{P} = ([n], \leq)$ is called hierarchical there exists a partition $[n] = \cup_{i=1}^{t} \Gamma_i$ such that for all $i_1 < i_2$ every element of Γ_{i_1} is less that Γ_{i_2}, and no other elements are comparable. The following can be proven as in [6, Thm. 7.4, Thm. 7.6] with straightforward generalizations.

Theorem 5.11. *The poset weight on A^n satisfies the extension property iff the poset is hierarchical.*

In particular, the results of this section show that the Hamming weight, the homogeneous weight, the symmetrized weight composition, and the RT-weight satisfy the extension property of Definition 5.1. In fact, the extension property is strongly related to Frobeniusness. Wood showed [68, Thm. 6.4] showed that a finite commutative ring R is Frobenius iff the Hamming weight on R satisfies the extension property. When we switch to module alphabet A, the strongest result is Theorem 5.3. So if the Hamming weight on A satisfies the extension property we are guarantied that $\mathrm{soc}({}_R A)$ is cyclic, however we are not guarantied that A is Frobenius; see also Remark 2.18(3).

[2] This is not a priori clear since there might exist nonzero elements of homogeneous weight 0.

5.2 Equivalence of Additive Codes

Let q be a power of some prime number. In this section we consider the case where the alphabet $A = \mathbb{F}_{q^\ell}$ $(\ell > 1)$ is a finite field viewed as a module over the finite field $R = \mathbb{F}_q$. Of course A is a vector space over R of dimension ℓ. In particular A does not have a cyclic socle. As a consequence of Theorem 5.3, the Hamming weight on A does not satisfy the extension property. Dyshko [13, Ex. 5] provides a linear code of length $q+1$ and a Hamming isometry that cannot be represented as in Theorem 3.19. Yet, in the same paper it is shown that any Hamming isometry of any linear code of length at most $q = |\mathbb{F}_q|$ is a monomial map.

In this section, unlike the Hamming weight, we show that the RT-weight on A satisfies the extension property. As usual, we first establish the structure of $\mathrm{wt}_{\mathrm{RT}}$-isometries of the extremal case $\mathcal{C} = A^n$, and then proceed to the general case. To this end, we set up some notation. Set $\mathbb{F} := \mathbb{F}_q$ and let $\phi : \mathbb{F}_{q^\ell} \longrightarrow \mathbb{F}^\ell$ be any $\mathbb{F}$-isomorphism of vector spaces. Then for any $n \in \mathbb{N}$, $\mathbb{F}_q^n$ is isomorphic to $(\mathbb{F}^\ell)^n = \mathbb{F}^{\ell n}$ via $\Phi : (x_1, \ldots, x_n) \longmapsto (\phi(x_1), \ldots, \phi(x_n))$. Then the RT-weight on $(\mathbb{F}^\ell)^n$ is the pullback of the RT-weight on $\mathbb{F}^{\ell n}$ under Φ, that is,

$$\mathrm{wt}_{\mathrm{RT},\ell}(x_1, \ldots, x_n) := \mathrm{wt}_{\mathrm{RT}}(\phi^{-1}(x_1), \cdots, \phi^{-1}(x_n))$$

for all $x_i \in \mathbb{F}^\ell$.

Put $\tilde{\mathbb{F}} := \mathbb{F}_{q^\ell}$. Then, a map $f : \mathcal{C} \leq {}_{\mathbb{F}}\tilde{\mathbb{F}}^n \longrightarrow \tilde{\mathbb{F}}^n$ is $\mathrm{wt}_{\mathrm{RT}}$-isometry iff the map $\tilde{f} := \Phi \circ f \circ \Phi^{-1} : \Phi(\mathcal{C}) \longrightarrow \mathbb{F}^{\ell n}$ is a $\mathrm{wt}_{\mathrm{RT},\ell}$-isometry. Note that, as an endomorphism of $\mathbb{F}^{\ell n} = (\mathbb{F}^\ell)^n$, the matrix representation of $\tilde{f}$ is a $\ell n \times \ell n$ block matrix over $\mathbb{F}$ where each block is a $\ell \times \ell$ matrix; see also (3.8).

Then, similarly as in Theorem 3.16(2) we have the following; see also [20, Prop. 5.2].

Proposition 5.12. *Let $f : \tilde{\mathbb{F}}^n \longrightarrow \tilde{\mathbb{F}}^n$ be a $\tilde{\mathbb{F}}$-linear map. Then the following are equivalent.*
(1) f is $\mathrm{wt}_{\mathrm{RT}}$-isometry.
(2) $\tilde{f} : \mathbb{F}^{\ell n} \longrightarrow \mathbb{F}^{\ell n}$ is a $\mathrm{wt}_{\mathrm{RT},\ell}$-isometry.
(3) There exists a matrix $M \in \mathrm{LT}_n(\mathcal{M}_\ell(\mathbb{F}))$ such that $\tilde{f}(x) = xM$ for all $x \in \mathbb{F}^{\ell n}$

Note that the above result does not mean that the map $f : \tilde{\mathbb{F}}^n \longrightarrow \tilde{\mathbb{F}}^n$ is given by right multiplication with a lower triangular matrix with entries in $\tilde{\mathbb{F}}$. This is simply due to the fact that $\mathrm{GL}_\ell(\mathbb{F}_q) \nsubseteq (\mathbb{F}_{q^\ell})^*$.

Theorem 5.13. *Let $\mathcal{C} \leq_{\mathbb{F}} \tilde{\mathbb{F}}^n$ be a linear code and $f : \mathcal{C} \longrightarrow \tilde{\mathbb{F}}^n$ be a linear map. Then f is a $\mathrm{wt}_{\mathrm{RT}}$-isometry iff there exists a matrix $M \in \mathrm{LT}_n(\mathcal{M}_\ell(\mathbb{F}))$ such that $\tilde{f}(x) = xM$ for all $x \in \mathbb{F}^{\ell n}$. In particular, the RT-weight on ${}_{\mathbb{F}}\tilde{\mathbb{F}}$ satisfies the extensions property.*

Proof. As usual, the "if-part" follows by Proposition 5.12. For the "only if-part" we induct on the length n of the code. The statement is clear for $n = 1$. Put $\tilde{\mathcal{C}} := \Phi(\mathcal{C})$, and

let $n \geq 2$. Recall that $\tilde{f}$ is a $\mathrm{wt}_{\mathrm{RT},\ell}$-isometry. If $\tilde{f}(x_1,\ldots,x_{n-1},x_n) = (y_1,\ldots,y_{n-1},y_n)$ then

$$x_n = 0 \iff y_n = 0. \tag{5.4}$$

Consider the subspace

$$\tilde{\mathcal{C}}' := \{(x_1,\ldots,x_{n-1}) \mid (x_1,\ldots x_{n-1},0) \in \tilde{\mathcal{C}}\} \leq \mathbb{F}^{\ell(n-1)}.$$

We obtain an induced map

$$\tilde{f}' : \tilde{\mathcal{C}}' \longrightarrow \mathbb{F}^{\ell(n-1)}, \quad (x_1,\ldots,x_{n-1}) \longmapsto (y_1,\ldots,y_{n-1})$$

where $(y_1,\ldots y_{n-1})$ is such that $\tilde{f}(x_1,\ldots,x_{n-1},0) = (y_1,\ldots,y_{n-1},0)$, which is a $\mathrm{wt}_{\mathrm{RT},\ell}$-isometry thanks to (5.4). By induction, there exists a matrix

$$A' = \begin{pmatrix} A_{11} & 0 & \cdots & 0 \\ A_{21} & A_{22} & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ A_{n-1,1} & \cdots & A_{n-1,n-2} & A_{n-1,n-1} \end{pmatrix} \in \mathrm{LT}_{n-1}(\mathcal{M}_\ell(\mathbb{F}))$$

such that $\tilde{f}'(x) = xA'$ for all $x \in \tilde{\mathcal{C}}'$. In other words

$$\tilde{f}(x_1,\ldots,x_{n-1},0) = ((x_1,\ldots,x_{n-1})A',0) \text{ for all } (x_1,\ldots,x_{n-1},0) \in \tilde{\mathcal{C}}. \tag{5.5}$$

Let p_n be the projection on the nth coordinate. Then, the map $\tilde{f}_n : p_n(\tilde{\mathcal{C}}) \longrightarrow \mathbb{F}^\ell$ given by $x_n \longmapsto p_n(\tilde{f}(x_1,\ldots,x_n))$ is well defined and an isometry. From the base case, there exists $A_{n,n} \in \mathrm{GL}_\ell(\mathbb{F})$ such that $\tilde{f}_n(x_n) = x_n A_{n,n}$. Then we can clearly find matrices $A_{n,j,x} \in \mathcal{M}_r(\mathbb{F})$ such that

$$y_j - \sum_{i=j}^{n-1} v_i A_{ij} = x_n A_{n,j,x} \quad \text{for } j = 1,\ldots,n-1.$$

Setting $A_{n,j,0} = 0 \in \mathcal{M}_\ell(\mathbb{F})$ we obtain matrices

$$A_x = \begin{pmatrix} A_{11} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ A_{n-1,1} & \cdots & A_{n-1,n-1} & 0 \\ A_{n,1,x} & \cdots & A_{n,n-1,x} & A_{nn} \end{pmatrix} \in \mathrm{LT}_n(R) \text{ for all } x \in \mathcal{C}$$

which, by construction, satisfy $\tilde{f}(x) = xA_x$ for all $x \in \tilde{\mathcal{C}}$.

Note that the matrices on the diagonal do not depend on x. Put $A'' = \mathrm{diag}(A_{11},\cdots,A_{nn}) \in \mathrm{GL}_n(\mathcal{M}_\ell(\mathbb{F}))$. The map

$$\tilde{f}' : \tilde{\mathcal{C}} \longrightarrow \mathbb{F}^{\ell n}, \quad x \longmapsto xA_x(A')^{-1}$$

is again a $\mathrm{wt}_{\mathrm{RT},\ell}$-isometry on $\mathbb{F}^{\ell n}$. However, $A_x(A'')^{-1} \in \mathrm{LT}_{\ell n}(\mathbb{F})$ and thus $\tilde{f}'$ is actually $\mathrm{wt}_{\mathrm{RT}}$-isometry on $\mathcal{C} \leq_{\mathbb{F}} \mathbb{F}^{\ell n}$. Now Theorem 5.8 concludes the proof. □

Remark 5.14. It is worth mentioning here that the proof above is very similar with the proof of [6, Thm. 7.4], where it is shown that the poset weight over A^n (with A Frobenius bimodule) satisfies the extension property. As mentioned the RT-weight is a special instance of the poset weight. Yet, a similar proof works just as well for the non-Frobenius bimodule ${}_{\mathbb{F}}\tilde{\mathbb{F}}$.

We end this section with a simple observation.

Example 5.15. Let $R = \mathbb{Z}_4 \times \mathbb{Z}_4$ and consider the subring $S := \{00, 11, 22, 33\} \leq R$. Let ${}_SR$ be the alphabet. Consider the S-linear codes

$$\mathcal{C} = \{(00, 00, 00), (20, 20, 00), (02, 02, 00), (22, 22, 00)\}$$

and

$$\mathcal{D} = \{(00, 00, 00), (20, 22, 00), (00, 22, 20), (20, 00, 20)\}$$

on R^3. Since $\mathcal{C}$ has an all-zero coordinate and $\mathcal{D}$ does not, it is easy to see that any Hamming isometry between the two cannot be a monomial map.

Chapter 6 Quantum Error-Correction

6.1 Basic Notions

We first set up some terminology in terms of the customary (and handy) bra-ket notation. For details we refer the reader to [47]. Throughout, let $\mathcal{H}$ be a finite dimensional complex Hilbert space. The inner product and the corresponding norm will be denoted $\langle \bullet \,|\, \bullet \rangle : \mathcal{H} \times \mathcal{H} \longrightarrow \mathbb{C}$ and $\| \bullet \|$. Its elements will be denoted as $|\psi\rangle$. With $\mathcal{H}^*$ we will denote the dual of $\mathcal{H}$, and its elements will be denoted as $\langle\psi|$. We will always have a specified orthonormal basis, with respect to which $|\psi\rangle$ will be thought as a column vector. Thus $\langle\psi|$ may be thought as a row vector, namely, the transpose conjugate of $|\psi\rangle$. For this reason it is also customary to use $|\psi\rangle^\dagger := \langle\psi| \in \mathcal{H}^*$. With this notation we have

$$|\psi\rangle^\dagger(|\phi\rangle) = \langle\psi|(|\phi\rangle) = \langle\, \phi \,|\, \psi \,\rangle,$$

for all $|\psi\rangle, |\phi\rangle \in \mathcal{H}$. Moreover, if $\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ is an orthonormal basis of $\mathcal{H}$ we have

$$|\psi\rangle = \sum_{i=1}^{n} \langle\, \psi_i \,|\, \psi \,\rangle |\psi_i\rangle \tag{6.1}$$

for all $|\psi\rangle \in \mathcal{H}$.

Let $T : \mathcal{H} \longrightarrow \mathcal{H}$ be a linear transformation. We will omit the parenthesis and write $T|\psi\rangle$ or $|T\psi\rangle$ instead of $T(|\psi\rangle)$. The **adjoint** of T is the unique linear transformation $T^\dagger : \mathcal{H} \longrightarrow \mathcal{H}$ that satisfies

$$\langle\, T^\dagger\psi \,|\, \phi \,\rangle = \langle\, \psi \,|\, T\phi \,\rangle$$

for all $|\psi\rangle, |\phi\rangle \in \mathcal{H}$. A linear transformation T is called **self-adjoint** if $T^\dagger = T$. Of particular interest is the self-adjoint transformation $T_\psi := |\psi\rangle\langle\psi|$. Thus

$$T_\psi(|\phi\rangle) = (|\psi\rangle\langle\psi|)(|\phi\rangle) = \langle\, \psi \mid \phi \,\rangle |\psi\rangle.$$

Let $T : \mathcal{H} \longrightarrow \mathcal{H}$ be a linear operator and λ be an eigenvalue of T, that is, $T|\psi\rangle = \lambda|\psi\rangle$ for some $0 \neq |\psi\rangle \in \mathcal{H}$. We will denote

$$\mathrm{eig}\,(T, \lambda) := \{|\psi\rangle \in \mathcal{H} \mid T|\psi\rangle = \lambda|\psi\rangle\},$$

the eigenspace of T corresponding to λ.

We will write $\mathcal{H}_n$ if $\dim_{\mathbb{C}} \mathcal{H} = n$. Consider any two-dimensional complex Hilbert space $\mathcal{H}_2$ and fix a orthonormal basis $\mathcal{B}_1 = \{|0\rangle, |1\rangle\}$. Let

$$\mathcal{H}_{2^n} := \bigotimes_{i=1}^{n} \mathcal{H}_2 =: \mathcal{H}_2^{\otimes n}$$

be the n-fold tensor product of $\mathcal{H}_2$. We write $|x_1 \cdots x_n\rangle$ for $|x_1\rangle \otimes \cdots \otimes |x_n\rangle$. As an orthonormal basis we use

$$\mathcal{B}_n := \mathcal{B}_1^{\otimes n} = \{|a\rangle \mid a \in \mathbb{F}_2^n\} = \{|j\rangle \mid j = 0, \ldots, 2^n - 1\} \tag{6.2}$$

where $\mathbb{F}_2 = \{0, 1\}$ is the field with two elements.

Definition 6.1.

(1) The pair $(\mathcal{H}_2, \mathcal{B}_1)$ is called a **quantum bit** (qubit). A unit vector in $\mathcal{H}_2$ is called a **state** of the qubit. The set of all states is called the **state space**.

(2) The pair $(\mathcal{H}_{2^n}, \mathcal{B}_n)$ is called a **quantum register** or a n-qubit. The basis elements $|a\rangle$ are called **computational basis states**.

(3) A **quantum gate** is a unitary transformation $U : \mathcal{H}_{2^n} \longrightarrow \mathcal{H}_{2^n}$.

Definition 6.2. An **observable** in $\mathcal{H}_{2^n}$ is a set of subspaces $\mathcal{O} \coloneqq \{H_0, \ldots, H_r\}$ such that $H_i \perp H_j$ for $i \neq j$ and $\mathcal{H}_{2^n} = H_0 \oplus \cdots \oplus H_r$.

Remark 6.3. Let $T : \mathcal{H} \longrightarrow \mathcal{H}$ be a self-adjoint operator and let $\lambda_0, \ldots, \lambda_r$ be all its different eigenvalues. Due to the Spectral Theorem, we have $\mathcal{H} = \operatorname{eig}(T, \lambda_0) \otimes \cdots \otimes \operatorname{eig}(T, \lambda_r)$ and $|\psi\rangle \in \mathcal{H}$ can be written uniquely as

$$|\psi\rangle = \sum_{i=0}^{r} \lambda_i |T_i \psi\rangle, \tag{6.3}$$

where $T_i : \mathcal{H} \longrightarrow \operatorname{eig}(T, \lambda_i)$ is the corresponding orthogonal projection. In other words, the set $\{\operatorname{eig}(T, \lambda_0), \ldots, \operatorname{eig}(T, \lambda_r)\}$ is an observable. That is, any self-adjoint transformation can be thought as an observable, and vice versa.

Example 6.4.

(1) Take the two dimensional complex Hilbert space $\mathbb{C}^2$ and take $\mathcal{B}_1 = \{|0\rangle, |1\rangle\}$ where $|0\rangle \coloneqq (1,0)^\intercal$, $|1\rangle \coloneqq (0,1)^\intercal$. A state of the qubit $(\mathbb{C}^2, \mathcal{B}_1)$ is any vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$. Using (6.2), to produce a 2-qubit we take $(\mathbb{C}^4, \mathcal{B}_2)$ where

$$|0\rangle \coloneqq |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |1\rangle \coloneqq |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |2\rangle \coloneqq |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |3\rangle \coloneqq |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

(2) By definition, a quantum gate is a unitary transformation. The definition is clear since we would want the state space to be preserved under a quantum gate. The following are gates of special interest:

$$X \coloneqq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Since $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$, X is called the **bit-flip** gate. On the other hand Z is called the **phase-flip** gate because $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$. Put $Y \coloneqq iXZ$. It is easy to see that $\{I_2, X, Y, Z\}$ form a linearly independent set of the vector space $\mathcal{M}_2(\mathbb{C})$. Thus

$$\mathcal{M}_2(\mathbb{C}) = \operatorname{span}_{\mathbb{C}}\{I_2, X, Y, Z\}. \tag{6.4}$$

X, Y, and Z are called the **Pauli matrices**.

Let $\mathcal{O} := \{H_0, \ldots, H_r\}$ be an observable. Then, any $|\psi\rangle \in \mathcal{H}$ can be written uniquely as

$$|\psi\rangle = \sum_{i=0}^{r} \alpha_i |\psi_i\rangle \tag{6.5}$$

where $|\psi_i\rangle$ is the projection of $|\psi\rangle$ onto H_i. Let $P_i : \mathcal{H} \longrightarrow H_i$ be given by $|\psi\rangle \longmapsto |\psi_i\rangle$; see also Remark 6.3. With this notation, we have the following.

Definition 6.5. A **measurement** of an n-qubit with respect to the observable $\mathcal{O}$ is the following: For a state written as in (6.5), pick a subspace H_i with probability $\|P_i|\psi\rangle\|^2$ and output the classical information i. After the measurement, the n-qubit will collapse to the state $P_i|\psi\rangle/\|P_i|\psi\rangle\|$.

Remark 6.6.

(1) Note that a measurement on $\mathcal{H}_n$ can provide at most n outcomes. When it can provide exactly n the measurement is called **maximal**. Note that maximal measurements correspond to orthonormal bases of $\mathcal{H}$.

(2) A measurement will irreversibly destroy a state, unless the state falls entirely into any of H_i's. Thus, as we will see in more details later on, much of quantum error-correction has to deal with producing states (or collection of states) that admit efficient observables.

(3) Recall that we can view H_i's as eigenspaces of some self-adjoint operator T. Thus the outcomes of a measurement are precisely the distinct eigenvalues of T, and after the measurement the n-qubit collapses to a normalized eigenstate (corresponding to the known eigenvalue).

(4) The orthonormal basis $\mathcal{B}_n$ gives rise to a particularly nice observable, called the **standard observable**, $\mathcal{O}_n$. With the same notation as in (6.1) and (6.2), it follows that $|\psi\rangle$ will collapse to the basis state $|j\rangle$ with probability $|\langle j \,|\, \psi \rangle|^2$.

Example 6.7.

(1) The **dual observable** (of $\mathcal{O}_1$) is $\mathcal{O}_1' = \{H_0, H_1\}$ where $H_0 = \mathrm{span}_{\mathbb{C}}\{|0'\rangle\}$ and $H_1 := \mathrm{span}_{\mathbb{C}}\{|1'\rangle\}$ with

$$|0'\rangle := \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ and } |1'\rangle := \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Consider a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Thus

$$|\psi\rangle = \frac{\alpha+\beta}{\sqrt{2}}|0'\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1'\rangle.$$

It follows that a measurement of $|\psi\rangle$ with respect to $\mathcal{O}'$ will produce the outcome 0 (resp., 1) with probability $|\alpha+\beta|^2/2$ (resp., $|\alpha-\beta|^2/2$).

(2) In Remark 6.6(4) we discussed measurements of a n-qubit. Let us consider a slightly different scenario. Assume we have a 2-qubit $(\mathcal{H}_4, \mathcal{B}_2)$ and a state $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \in \mathcal{H}_4$. Consider the observable $\mathcal{O} = \{H_0^1, H_1^1\}$ where

$$H_0^1 = \mathrm{span}_{\mathbb{C}}\{|00\rangle, |01\rangle\} \text{ and } H_1^1 = \mathrm{span}_{\mathbb{C}}\{|10\rangle, |11\rangle\}.$$

Then, we get the outcome i with probability $|\alpha_{i0}|^2 + |\alpha_{i1}|^2$ and the post-measurement state is

$$\frac{\alpha_{i0}|i0\rangle + \alpha_{i1}|i1\rangle}{\sqrt{|\alpha_{i0}|^2 + |\alpha_{i1}|^2}}.$$

The above can be thought as a measurement of the first qubit of the 2-qubit $|\psi\rangle$. Similarly one can measure the second qubit of $|\psi\rangle$ using the observable $\mathcal{O} = \{H_0^2, H_1^2\}$ where

$$H_0^2 = \text{span}_{\mathbb{C}}\{|00\rangle, |10\rangle\} \text{ and } H_1^2 = \text{span}_{\mathbb{C}}\{|01\rangle, |11\rangle\}.$$

Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ be a state. Then there exists a quantum gate U_ψ such that $U_\psi|\psi 0\rangle = |\psi\psi\rangle$. Namely

$$U_\psi := I_2 \otimes \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix}.$$

In other words, it is possible to **clone** any quantum state. However, the drawback is that the quantum gate U_ψ depends on $|\psi\rangle$. As it turns out, there is no **universal** gate that simultaneously clones every state. This fact constitutes a key difference between quantum and classical information theory.

Theorem 6.8 (No-Cloning Theorem)**.** *A qubit cannot be cloned. That is, there exists no quantum gate U such that $U|\psi 0\rangle = |\psi\psi\rangle$ for all states $|\psi\rangle \in \mathcal{H}_2$.*

Proof. Let $|\psi\rangle \neq |\phi\rangle$ be any two states and assume that there exists a unitary matrix U such that $U|\psi 0\rangle = |\psi\psi\rangle$ and $U|\phi 0\rangle = |\phi\phi\rangle$. Then for the state $|\alpha\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle)$ one has

$$U|\alpha 0\rangle = \frac{1}{\sqrt{2}}(|\psi\psi\rangle + |\phi\phi\rangle),$$

whereas

$$|\alpha\alpha\rangle = \frac{1}{2}(|\psi\psi\rangle + |\phi\phi\rangle + |\psi\phi\rangle + |\phi\psi\rangle).$$

Thus $U|\alpha 0\rangle \neq |\alpha\alpha\rangle$ in general. □

6.2 Error Detection and Correction

There are two obvious challenges in quantum information theory. First, the only way to extract information from a qubit is via measurements. In this case we obtain only one classical bit of information and quantum states are irreversibly lost. So any attempt of extracting information could have fatal consequences. Secondly, due to the No-Cloning Theorem, much of the classical information theory is simply not possible. For instance, the simplest error-correcting code in classical information theory is the repetition code where one adds redundancy as necessary. As mention, this is not possible in quantum information theory. However, this challenges (and others) can be overcome. The first attacking strategies where developed by Shor and Steane [59, 62]. The theory was quickly developed and generalized [9, 10]. In particular, Daniel

Gottesman developed in his PhD thesis [21] the stabilizer formalism, which gives a compact and algebraic description of quantum error-correction.

Much of quantum error-correction has to do with producing states that admit efficient measurements. Two states are called **distinguishable** if there exists a measurement that with **certainty** (that is, probability 1) tells us which one is which. We have the following.

Theorem 6.9. *Two states $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}_{2^n}$ are distinguishable iff $\langle \psi_1 | \psi_2 \rangle = 0$.*

Proof. Assume that $\langle\psi_1|\psi_2\rangle = 0$. Then $\mathcal{O} = \{H_1, H_2\}$ where $H_1 = \mathrm{span}_{\mathbb{C}}\{|\psi_1\rangle\}$ and $H_2 = H_1^{\perp} \ni |\psi_2\rangle$ is an observable. Measuring with $\mathcal{O}$ will output, with certainty, i if the qubit was initially in the state $|\psi_i\rangle$. Conversely, if two states $|\psi_1\rangle, |\psi_2\rangle$ are not orthogonal there are no mutually orthogonal subspaces each containing one of the states. In other words, there exists no measurement that with certainty outputs different values for $|\psi_1\rangle$ and $|\psi_2\rangle$. □

The above is the reason of the unitary constrain on quantum states. Indeed, two parallel states are not distinguishable and thus we may scale to unit vectors. This is commonly known as "the global phase is not noticeable". Also, the above is (in essence) the reason of Definition 6.12(2) of detectable quantum errors.

Definition 6.10.

(1) An **error** on the n-qubit $\mathcal{H}_{2^n}$ is a linear transformation $E : \mathcal{H}_{2^n} \longrightarrow \mathcal{H}_{2^n}$, which we also may think of as a matrix $E \in \mathcal{M}_{2^n}(\mathbb{C})$.

(2) The **Pauli group** $\mathcal{P}_1$ is the multiplicative group generated by the Pauli matrices; see Example 6.4. In other words

$$\mathcal{P}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}.$$

Then, the **Pauli group of a n-qubit** $\mathcal{P}_n$ is

$$\begin{aligned}\mathcal{P}_n &= \{E_1 \otimes \cdots \otimes E_n \mid E_i \in \mathcal{P}_1\} \\ &= \{i^\lambda X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n} \mid \lambda \in \mathbb{Z}_4, a_i, b_i \in \mathbb{F}_2\} \\ &=: \{i^\lambda X(a)Z(b) \mid \lambda \in \mathbb{Z}_4, a, b \in \mathbb{F}_2^n\}.\end{aligned}$$

Remark 6.11. The Pauli matrices satisfy $E^\dagger = E$ and $X^2 = Y^2 = Z^2 = I$. In addition

$$\begin{aligned} XY &= iZ, \quad & YZ &= iX, \quad & XZ &= -iY, \\ YX &= -iZ, \quad & ZY &= -iX, \quad & ZX &= iY. \end{aligned}$$

It follows that the Pauli matrices either commute ($EE' = E'E$) or anticommute ($EE' = -E'E$). Moreover, the Pauli matrices are hermitian (self-adjoint if thought as operators) and unitary. Due to (6.4) we have that any error on a n-qubit is a linear combination of elements of $\mathcal{P}_n$. We saw in Example 6.4 that X, Z and Y can be viewed as the bit-flip, phase-flip, and bit-phase-flip error respectively. We will see that these are all the errors one needs to consider. In this sense the Pauli group plays the role of an **error group**.

Definition 6.12.

(1) A **quantum code of length** n is a proper subspace $\mathcal{Q}$ of $\mathcal{H}_{2^n}$.

(2) A quantum code $\mathcal{Q} \leq \mathcal{H}_{2^n}$ **detects** an error $E \in \mathcal{M}_{2^n}(\mathbb{C})$ if for all $|\psi\rangle, |\phi\rangle \in \mathcal{Q}$ we have

$$\langle \psi \,|\, \phi \rangle = 0 \implies \langle \psi \,|\, E\phi \rangle = 0.$$

(3) A quantum code $\mathcal{Q} \leq \mathcal{H}_{2^n}$ **corrects** a set of errors $\mathcal{E} \subset \mathcal{M}_{2^n}(\mathbb{C})$ if for all $|\psi\rangle, |\phi\rangle \in \mathcal{Q}$ and for all $E, E' \in \mathcal{E}$ we have

$$\langle \psi \,|\, \phi \rangle = 0 \implies \langle E\psi \,|\, E'\phi \rangle = 0.$$

Remark 6.13.

(1) In principle, a quantum code $\mathcal{Q}$ corrects an error E if for all $|\psi\rangle \in \mathcal{Q}$, there exists a quantum algorithm[1] that takes as input $E|\psi\rangle$ and outputs $|\psi\rangle$. It turns out that the existence of such an algorithm is equivalent (see [21, Sec. 2.3], for instance) to Definition 6.12(3), which we use as starting point. It is now easy to see that if $\mathcal{Q}$ corrects $\mathcal{E}$ then it will also correct the linear span of $\mathcal{E}$. Thanks to (6.4), $\mathcal{Q} \leq \mathcal{H}_2$ corrects any error $E \in \mathcal{M}_2(\mathbb{C})$ iff it corrects the errors X, Y, and Z.

(2) Since $(E|\psi\rangle)^\dagger = \langle\psi|E^\dagger$ we have

$$\langle E\psi \,|\, E'\phi \rangle = \langle \psi \,|\, E^\dagger E' \,|\, \phi \rangle.$$

Therefore, a quantum code corrects a set of errors $\mathcal{E}$ iff it detects every error in $\mathcal{E}^\dagger\mathcal{E} = \{E^\dagger E' \mid E, E' \in \mathcal{E}\}$.

6.2.1 Shor's 9-qubit code

In this section we describe the first quantum code found that corrects any error on one qubit. This quantum code was discovered by Shor [59]. We first describe how to correct the bit-flip error X. Consider the quantum code $\mathcal{Q} := \mathrm{span}_{\mathbb{C}}\{|000\rangle, |111\rangle\} \leq \mathcal{H}_8$. Hence, a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is encoded as $\alpha|000\rangle + \beta|111\rangle$. Note first that this does not violate the no-cloning theorem because we have cloned only the basis states $|0\rangle$, $|1\rangle$ and not the general state $|\psi\rangle$. The error-correcting procedure is as follows. Compare the first two qubits and the second two qubits. If the first two qubits are the same and the second two qubits are the same, then no error occurred. If the first two qubits are different and the second two qubits are the same, the first qubit is flipped during the transmission. This procedure can be implemented by measuring the encoded state with respect to the observable $\mathcal{O} := \{H_0, H_1, H_2, H_3\}$ where

$$\left.\begin{aligned} H_0 &:= \mathrm{span}_{\mathbb{C}}\{|000\rangle, |111\rangle\}, \quad & H_1 &:= \mathrm{span}_{\mathbb{C}}\{|100\rangle, |011\rangle\}, \\ H_2 &:= \mathrm{span}_{\mathbb{C}}\{|010\rangle, |101\rangle\}, \quad & H_3 &:= \mathrm{span}_{\mathbb{C}}\{|001\rangle, |110\rangle\}. \end{aligned}\right\} \tag{6.6}$$

The outcome of this measurement will tell us what error occurred. If the outcome is 0 then no error happened. If the outcome is i then a bit flip has happened on the ith qubit. Note that the measurement will not collapse the encoded state. Indeed,

[1] A quantum algorithm is a finite number of quantum gates and measurements.

assume $\alpha|000\rangle + \beta|111\rangle$ is transmitted and $|\psi'\rangle$ is received. Then $|\psi'\rangle \in H_0$ iff there is no bit flip (and also no other errors, of course!). Also, $|\psi'\rangle \in H_i$ iff the ith bit is flipped during transmission.

All the above shows that there exists a quantum algorithm (consisting of the described measurement) that corrects one bit-flip. On the other hand, it is easy to see that $\mathcal{Q}$ and $\mathcal{E} = \{X \otimes I_2 \otimes I_2, I_2 \otimes X \otimes I_2, I_2 \otimes I_2 \otimes X\}$[2] satisfy Definition 6.12(3).

In a very similar way one can describe the correction of the phase-flip error Z. In this case we use $|0'\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$ and $|1'\rangle := (|0\rangle - |1\rangle)/\sqrt{2}$ (see also Example 6.7) and $\mathcal{Q} := \mathrm{span}_{\mathbb{C}}\{|0'0'0'\rangle, |1'1'1'\rangle\} \leq \mathcal{H}_8$. Then, we can either measure with respect to a similar observable as in (6.6) or straightforwardly check that $\mathcal{Q}$ and $\{ZII, IZI, IIZ\}$ satisfy Definition 6.12(3).

So far we used 3-qubit codes. In order to correct a combination of the bit-flip and phase-flip error, that is the XZ error, we will need a 9-qubit code. We point out here that any code that corrects XZ will also correct Y (due to linearity of quantum error-correction). Thus, such a code will correct any error $E \in \mathcal{M}_2(\mathbb{C})$. Shor's 9-qubit quantum code is

$$\mathcal{Q} := \mathrm{span}_{\mathbb{C}}\{(|000\rangle + |111\rangle)^{\otimes 3}, (|000\rangle - |111\rangle)^{\otimes 3}\} \leq \mathcal{H}_{2^9}$$

The idea is again very similar. A bit-flip is corrected via an analogous observable to (6.6), whereas a phase-flip error is corrected by comparing the phases of the blocks. Definition 6.12(3) is particularly handy in this case.

6.2.2 Quantum Stabilizer Codes

Stabilizer formalism gives a compact and algebraic approach to quantum error-correction. In here we discuss the binary case developed by Daniel Gottesman in his PhD thesis [21]. The purpose is to give some motivation and background. We will address the details when dealing with stabilizers over local Frobenius rings in Section 7.1.

Let $\mathcal{Q} \leq \mathcal{H}_{2^n}$ be a quantum code. We can attach to $\mathcal{Q}$ a set of errors via

$$\mathfrak{S}(\mathcal{Q}) := \{E \in \mathcal{P}_n \mid E|\psi\rangle = |\psi\rangle \text{ for all } |\psi\rangle \in \mathcal{Q}\}.$$

It is clear that $\mathfrak{S}(\mathcal{Q})$ is a subgroup of $\mathcal{P}_n$. Moreover, $-I \notin \mathfrak{S}(\mathcal{Q})$ since otherwise $\mathcal{Q} = 0$. We saw in Remark 6.11 that elements of $\mathcal{P}_n$ either commute or anticommute. If $\mathfrak{S}(\mathcal{Q})$ contains two anticommuting errors E, E' then

$$|\psi\rangle = EE'|\psi\rangle = -E'E|\psi\rangle = -|\psi\rangle$$

implies $\mathcal{Q} = 0$. As a consequence $\mathfrak{S}(\mathcal{Q}) \leq \mathcal{P}_n$ is an abelian subgroup. Commuting errors have the desirable property of having simultaneous eigenvalues. This motivates the following definition.

Definition 6.14.

[2] In what follows we will omit the tensor and write XII, IXI, IIX

(1) An abelian subgroup $S \leq \mathcal{P}_n$ such that $-I \notin S$ is called a **stabilizer**.
(2) A **quantum stabilizer code** associated to a stabilizer S is the subspace

$$\mathfrak{Q}(S) := \{|\psi\rangle \in \mathcal{H}_{2^n} \mid E|\psi\rangle = |\psi\rangle \text{ for all } E \in S\}.$$

All quantum codes presented in the previous section are examples of quantum stabilizer codes. Their stabilizer can be easily seen and described. In fact, many efficient quantum codes are of this nature, including the 5-qubit code [37] (the shortest code that can correct any 1-qubit error), the Steane's 7-qubit code [61], the so-called graph stabilizer codes [57] etc.. The most beautiful feature of quantum stabilizer codes is that they admit a **syndrome decoding** algorithm as in the classical case; see [21, p. 20].

Given two stabilizers $S \leq S'$ it follows directly by the definition that $\mathfrak{Q}(S') \leq \mathfrak{Q}(S)$. Similarly, if $Q \leq Q'$ then $\mathfrak{S}(\mathcal{Q}') \leq \mathfrak{S}(Q)$. Also from the very definition, for any quantum code $\mathcal{Q}$ and stabilizer S we have

$$\mathcal{Q} \leq \mathfrak{Q}(\mathfrak{S}(\mathcal{Q})) \text{ and } S \leq \mathfrak{S}(\mathfrak{Q}(S)). \tag{6.7}$$

Applying the above to the quantum stabilizer code $\mathfrak{Q}(S)$ and to the stabilizer $\mathfrak{S}(\mathcal{Q})$ we obtain

$$\mathfrak{Q}(S) = \mathfrak{Q}(\mathfrak{S}(\mathfrak{Q}(S))) \text{ and } \mathfrak{S}(\mathcal{Q}) = \mathfrak{S}(\mathfrak{Q}(\mathfrak{S}(\mathcal{Q}))). \tag{6.8}$$

Quantum stabilizer codes have a nice error-correction criteria.

Theorem 6.15. *Consider a set of errors $\mathcal{E} = \{E_i\} \subseteq \mathcal{P}_n$. Then:*
(1) $\mathcal{E}$ is corrected by a stabilizer code $\mathfrak{Q}(S)$ if $E_i^\dagger E_j \notin \mathcal{C}(S) - S$ for all i, j where $\mathcal{C}(S)$ is the centralizer of S in $\mathcal{P}_n$.
(2) $\mathcal{E}$ is detected by a stabilizer code $\mathfrak{Q}(S)$ if $E_i \notin \mathcal{C}(S) - S$ for all $E_i \in \mathcal{E}$.

Proof. (1) We use Definition 6.12(3). If $E_i^\dagger E_j \notin \mathcal{C}(S) - S$ then either $E_i^\dagger E_j \in S$ or $E_i^\dagger E_j \in \mathcal{P}_n - \mathcal{C}(S)$. Assume first that $E_i^\dagger E_j \in S$ and let $|\psi\rangle, |\phi\rangle \in \mathfrak{Q}(S)$ be such that $\langle\psi|\phi\rangle = 0$. Since $E_i^\dagger E_j|\phi\rangle = |\phi\rangle$ we immediately get

$$0 = \langle \psi \,|\, \phi \rangle = \langle \psi \,|\, E_i^\dagger E_j \,|\, \phi \rangle.$$

Assume now that $E_i^\dagger E_j \in \mathcal{P}_n - \mathcal{C}(S)$. Then there exists $E \in S$ that does not commute with $E_i^\dagger E_j$. Hence E and $E_i^\dagger E_j$ must anticommute. Also, since $E \in S$ we have $\langle\psi|E = \langle\psi|$ and $E|\phi\rangle = |\phi\rangle$. This yields

$$\begin{aligned} \langle \psi \,|\, E_i^\dagger E_j \,|\, \phi \rangle &= \langle \psi \,|\, E_i^\dagger E_j E \,|\, \phi \rangle \\ &= -\langle \psi \,|\, E E_i^\dagger E_j \,|\, \phi \rangle \\ &= -\langle \psi \,|\, E_i^\dagger E_j \,|\, \phi \rangle, \end{aligned}$$

and consequently, $\langle \psi \,|\, E_i^\dagger E_j \,|\, \phi \rangle = 0$, without even assuming $\langle \psi \,|\, \phi \rangle = 0$.
(2) Consider the cases $E_i \in \mathcal{P}_n - S$ and $E_i \in S$ and proceed as in part (1) to show that Definition 6.12(2) holds. □

By the very definition, errors in S have no physical impact on $\mathfrak{Q}(S)$. On the other hand Theorem 6.15(2) says that an error outside $\mathcal{C}(S)$ is automatically detected by $\mathfrak{Q}(S)$. Thus the troubles come from $\mathcal{C}(S) - S$, and the bigger this difference is the more errors one has to control. Later on, we will study the size of this difference, that is, the "true" errors, with classical tools. This suggests the following definition.

Definition 6.16.
(1) The **weight** of a Pauli operator $E = i^\lambda E_1 \otimes \cdots \otimes E_n \in \mathcal{P}_n$ where $E_i \in \{I, X, Y, Z\}$ is

$$\mathrm{wt}(E) = |\{i \mid E_i \neq I\}|.$$

(2) The **minimum distance** of a quantum stabilizer code $\mathfrak{Q}(S)$ is

$$\mathrm{dist}(\mathfrak{Q}(S)) = \begin{cases} \min\{\mathrm{wt}(E) \mid E \in \mathcal{C}(S) - S\}, & \text{if } S \subsetneq \mathcal{C}(S) \\ \min\{\mathrm{wt}(E) \mid E \in S - \{I\}\}, & \text{if } S = \mathcal{C}(S) \end{cases}.$$

Corollary 6.17. *A quantum stabilizer code with minimum distance at least $2t + 1$ corrects any error of weight at most t.*

Proof. Note first that $\mathrm{wt}(EE') \leq \mathrm{wt}(E) + \mathrm{wt}(E')$ and $\mathrm{wt}(E^\dagger) = \mathrm{wt}(E)$ for all $E, E' \in \mathcal{P}_n$. Then, if E, E' are two errors of weight at most t, it follows that

$$\mathrm{wt}(E^\dagger E') \leq \mathrm{wt}(E^\dagger) + \mathrm{wt}(E') = \mathrm{wt}(E) + \mathrm{wt}(E') \leq t + t.$$

Hence, if $\mathrm{dist}(\mathfrak{Q}(S)) \geq 2t + 1$ we get $E^\dagger E' \notin \mathcal{C}(S) - S$. The result then follows by Theorem 6.15. □

Chapter 7 Stabilizer Codes over Frobenius Rings

The usefulness and easiness of binary quantum stabilizer is already clear from Section 6.2.2. As mentioned the Pauli group plays the role of an error basis, which in turn yields stabilizers and quantum stabilizer codes. The same ideas were developed in a more mathematical language and eventually led to general error bases, Pauli groups, and non-binary quantum stabilizer codes; see for instance [3, 32, 34]. One notices that the underlying idea is to use the nice structure of characters of the additive group of a finite field. This nice property is precisely Frobeniusness discussed extensively on earlier chapters. This idea was used by Nadella/Klappenecker [43] to define quantum stabilizer codes over arbitrary Frobenius rings.

7.1 Introduction

One particularly appealing feature of quantum stabilizer codes is their connection with classical additive codes and symplectic geometry. This was first discovered in [9] and then further developed in [10]. In here we give the appropriate definition of the Pauli group over any Frobenius ring and discuss some of the details left out from Section 6.2.2.

Recall the Pauli operators X, Z from Definition 6.10. For $a = (a_1, \cdots, a_n) \in \mathbb{F}_2^n$ we use the notation $X(a) := X^{a_1} \otimes \cdots \otimes X^{a_n}$. With the same notation as in (6.2) one easily verifies that

$$X(a)|b\rangle = |a + b\rangle \text{ for all } |b\rangle \in \mathcal{B}_n. \tag{7.1}$$

Similarly, one has

$$Z(a)|b\rangle = (-1)^{a\cdot b}|b\rangle \text{ for all } |b\rangle \in \mathcal{B}_n \tag{7.2}$$

where $a \cdot b = \sum_{i=1}^{n} a_i b_i$ is the standard dot product. One uses this idea to define general X and Z operators. But first, we drop the bra-ket notation. Throughout, let R be a finite Frobenius ring[1] with cardinality $|R| = d$ and generating character χ. A **qudit** is the d-dimensional Hilbert space $\mathbb{C}^d$ together with a specified orthonormal basis $\mathcal{B}_1$ labeled via the ring elements. That is

$$\mathcal{B}_1 = \{v_x \in \mathbb{C}^d \mid x \in R\}.$$

Then again, a n-qudit is the d^n-dimensional vector space $(\mathbb{C}^d)^{\otimes n} \cong \mathbb{C}^{d^n}$ together with

$$\mathcal{B}_n := \mathcal{B}_1^{\otimes n} = \{v_x = v_{x_1} \otimes \cdots \otimes v_{x_n} \mid x = (x_1, \ldots, x_n) \in R^n\}.$$

To generalize the bit-flip and the phase-flip errors one uses (7.1) and (7.2). Namely, for $a \in R$ define two linear transformations of $\mathbb{C}^d$ via

$$X(a) : v_x \longmapsto v_{x+a}$$
$$Z(a) : v_x \longmapsto \chi(ax)v_x$$

[1] Eventually we will work with commutative rings; see the paragraph preceding Definition 7.10.

Note that $X(a)$ is a permutation matrix for all $a \in R$ and thus unitary. Moreover, the matrix representation of $Z(a)$ with respect to $\mathcal{B}_1$ is $\mathrm{diag}(\chi(ax))_{x\in R}$. For all $a \in R$, $Z(a)$ is as well unitary since character values are roots of unity. Let

$$\mathcal{E}_1 = \{X(a)Z(b) \mid a, b \in R\}$$

For $a = (a_1, \ldots, a_n) \in R^n$ define the following unitary transformations of $\mathbb{C}^{d^n}$:

$$X(a) := X(a_1) \otimes \cdots \otimes X(a_n),$$
$$Z(a) := Z(a_1) \otimes \cdots \otimes Z(a_n).$$

This amounts to

$$X(a)(v_x) = v_{x+a} \text{ and } Z(a)(v_x) = \chi(a \cdot x)v_x \text{ for all } a, x \in R^n.$$

Remark 7.1. Since $X(a), Z(a)$ are unitary we have $X(a)^{-1} = X(a)^\dagger$ and $Z(a)^{-1} = Z(a)^\dagger$. In addition, the following are easily verifiable

$$X(a)^\ell = X(\ell a) \text{ and } Z(a)^\ell = Z(\ell a) \text{ for all } a \in R^n \text{ and } \ell \in \mathbb{Z}, \tag{7.3}$$

$$X(a)Z(b) = X(a')Z(b') \iff (a, b) = (a', b') \tag{7.4}$$

for all $(a, b), (a', b') \in R^{2n}$.

Recall that the Pauli group in the binary case was the multiplicative group generated by the Pauli matrices and was **the** error basis. In our case we need to be more careful. The error basis (out of which we will construct the Pauli group) is

$$\mathcal{E}_n := \{X(a)Z(b) \mid a, b \in R^n\} = \{X(a_1)Z(b_1) \otimes \ldots \otimes X(a_n)Z(b_n) \mid (a, b) \in R^{2n}\}.$$

The intuitive thing to do is to consider the group generated by $\mathcal{E}_n$. However, as we will see, this will be the right approach precisely when the characteristic of R is odd. That is, in general, we will need a group that contains $\langle \mathcal{E}_n \rangle$. The following gives the multiplication and commutativity rules for elements of $\mathcal{E}_n$

Proposition 7.2 ([43, Prop. 4])**.** *Let $E = X(a)Z(b), E' = X(a')Z(b') \in \mathcal{E}_n$. Then,*

$$EE' = \chi(b \cdot a')X(a + a')Z(b + b'),$$
$$E'E = \chi(b' \cdot a)X(a + a')Z(b + b').$$

In particular, E and E' commute iff $\chi(b \cdot a' - b' \cdot a) = 1 = \chi(b' \cdot a - b \cdot a')$.

The following is an immediate corollary. It points out how the characteristic comes into play and helps computing the order of elements of $\mathcal{E}_n$.

Corollary 7.3. *Let $(a, b) \in R^{2n}$. Then $\big(X(a)Z(b)\big)^{-1} = \chi(ba)X(-a)Z(-b)$ and more generally*

$$\big(X(a)Z(b)\big)^\ell = \chi\Big(\frac{\ell(\ell-1)}{2}ba\Big)X(\ell a)Z(\ell b) \text{ for all } \ell \in \mathbb{Z}.$$

Theorem 7.4. *Let* $\mathrm{char}(R) = c$ *and define* $N := \mathrm{lcm}\big\{|X(a)Z(b)| \,\big|\, (a,b) \in R^{2n}\big\}$, *where* $|\bullet|$ *denotes the order of the given matrix in the unitary group* $\mathcal{U}(d^n)$. *Then*

$$N = \begin{cases} c, & \text{if } c \text{ is odd,} \\ 2c, & \text{if } c \text{ is even.} \end{cases}$$

Proof. It is clear from Corollary 7.3 that $c \mid N$. Now if c is odd then $c(c-1)/2 = 0$ and the statement follows again from Corollary 7.3. Assume now that c is even. Then $2c(2c-1)/2 = 0$, and making use if Corollary 7.3 one more time we obtain $N \mid 2c$. To conclude the proof it remains to find $(a,b) \in R^{2n}$ such that $(X(a)Z(b))^c \neq I$. Indeed, since $c/2$ is an integer, the character $(c/2)\cdot\chi$ cannot be the trivial character. Thus there exists $\alpha \in R$ such that $\chi((c/2)\alpha) \neq 1$. Now it is easy to check that $a = (\alpha, 0, \ldots, 0)$ and $b = (1, 0, \ldots, 0)$ do the job. □

Definition 7.5. Let $\mathrm{char}(R) = c$, N be as in Theorem 7.4, and let $\omega \in \mathbb{C}^*$ be a primitive N-th root of unity. The n-**qudit Pauli group associated with the error basis** $\mathcal{E}_n$ is

$$\mathcal{P}_n := \{\omega^\ell X(a)Z(b) \mid \ell \in \mathbb{Z},\, a, b \in R^n\} \leq \mathcal{U}(d^n).$$

The elements of $\mathcal{P}_n$ are called **Pauli operators**.

Note that $\chi(a) \in \langle\, \omega \,\rangle = \{1, \omega, \ldots, \omega^{N-1}\}$ for all $a \in R$ implies that $\mathcal{P}_n$ is indeed a group. In addition, using a primitive N-th root of unity is absolutely crucial. For instance, if we use $\omega = -1$ for the binary case $R = \mathbb{F}_2$ we leave out all the complex phases; see also Example 7.13 for a more detailed description.

Remark 7.6. Let $E = \omega^\ell X(a)Z(b) \in \mathcal{P}_n$, where $\ell \in \mathbb{Z}$, $a, b \in R^n$. Then the trace of the matrix E is

$$\mathrm{Tr}(E) = \begin{cases} \omega^\ell d^n, & \text{if } (a,b) = (0,0), \\ 0, & \text{otherwise.} \end{cases}$$

Indeed, assume first that $a \neq 0$. In this case, since $X(a)$ is a permutation matrix, its diagonal elements are zero. And since $Z(b)$ is a diagonal matrix for any b, so are the entries of $X(a)Z(b)$. For $a = 0$ we have $X(a) = I_{d^n}$. Thus

$$\mathrm{Tr}(E) = \mathrm{Tr}(\omega^\ell Z(b)) = \omega^\ell \sum_{x \in R^n} \chi(xb) = \omega^\ell \sum_{x \in R^n} (b\chi)(x) = \omega^\ell d^n,$$

where the last equality follows by the orthogonality relations (2.1). Moreover, the set $\mathcal{E}_n$ is an orthonormal basis of $\mathcal{M}_{d^n}(\mathbb{C})$ with respect to the hermitian inner product

$$\langle\, E_1 \,|\, E_2 \,\rangle := \frac{1}{d^n}\mathrm{Tr}(E_1 E_2^\dagger). \tag{7.5}$$

In the language of Knill [35], the set $\mathcal{E}_n$ forms a **nice unitary error basis**.

Clearly, the self-adjoint operator X can be defined over any ring. In fact the same is true even for Z, where one uses any non-trivial character. However, the resulting $\mathcal{E}_n$ will be a nice error basis precisely when R is Frobenius; see [33, Lem. 2].

We have a surjective group homomorphism

$$\Psi : \mathcal{P}_n \longrightarrow R^{2n}, \quad \omega^\ell X(a)Z(b) \longmapsto (a,b), \tag{7.6}$$

with kernel $\ker \Psi = \{\omega^\ell I \mid \ell \in \mathbb{Z}\}$. The latter is also the center of $\mathcal{P}_n$. We will use this to transfer the study to R^{2n}. But first we give the definition of stabilizers and quantum stabilizer codes in this new setting.

Definition 7.7.
(1) An abelian subgroup $S \leq \mathcal{P}_n$ is called a **stabilizer** if $S \cap \ker \Psi = \{I_{d^n}\}$.
(2) A subspace $\mathcal{Q} \leq \mathbb{C}^{d^n}$ is called a **quantum stabilizer code** if there exists a stabilizer $S \leq \mathcal{P}_n$ such that

$$\mathcal{Q} = \mathfrak{Q}(S) := \{v \in \mathbb{C}^{d^n} \mid Ev = v \text{ for all } E \in S\} = \bigcap_{E \in S} \operatorname{eig}(E, 1).$$

(3) A linear code $\mathcal{C} \leq R^{2n}$ is called **stabilizer code** if there exists a stabilizer S such that $\mathcal{C} = \Psi(S)$.

Theorem 7.8. *Let $S \leq \mathcal{P}_n$ be a stabilizer and $\mathcal{Q} = \mathfrak{Q}(S) \leq \mathbb{C}^{d^n}$ be the corresponding quantum stabilizer code. Then* $\dim \mathcal{Q} = d^n/|S|$.

Proof. Set $P := \frac{1}{|S|} \sum_{E \in S} E$. Since S is a group we have $E'P = P$ for all $E' \in S$, and therefore $P^2 = P$. One easily shows that $\mathcal{Q} = \operatorname{im} P$ and hence

$$\dim_{\mathbb{C}} \mathcal{Q} = \dim_{\mathbb{C}}(\operatorname{im} P) = \operatorname{Tr}(P) = q^n/|S|,$$

where the last step follows from Remark 7.6 along with the fact that $S \cap \{\lambda I_{d^n} \mid \lambda \in \mathbb{C}\} = \{I_{d^n}\}$. □

Corollary 7.9. *For a stabilizer code $\mathcal{Q} = \mathfrak{Q}(S)$ we have $S = \mathfrak{S}(\mathcal{Q})$.*

Proof. As in (6.7) we have $S \leq \mathfrak{S}(\mathfrak{Q}(S))$. Thanks to Theorem 7.8 and (6.8) we have equality due to cardinality reasons. □

To keep track of the commutativity of Pauli operators we use the following symplectic bilinear form; see also Definition 3.2. In order to attain bilinearity we will need to work with a commutative Frobenius ring, and that is what we assume from now on.

Definition 7.10. The **symplectic inner product** on $\langle \bullet \mid \bullet \rangle_{\mathrm{s}} : R^{2n} \times R^{2n} \longrightarrow R$ is defined as

$$\langle (a,b) \mid (a',b') \rangle_{\mathrm{s}} := \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} \begin{pmatrix} a' \\ b' \end{pmatrix} = ba' - b'a.$$

For $A \subseteq R^{2n}$ we define $A^\perp := \{v \in R^{2n} \mid \langle v \mid w \rangle_{\mathrm{s}} = 0 \text{ for all } w \in A\}$. If $\mathcal{C} \leq R^{2n}$ is a linear code then $\mathcal{C}^\perp$ is the dual code as in Definition 3.3 As usual, $\mathcal{C}$ is called **self-orthogonal** (resp., **self-dual**) if $\mathcal{C} \subseteq \mathcal{C}^\perp$ (resp., $\mathcal{C} = \mathcal{C}^\perp$).

We have the following special instance of Proposition 3.4.

Proposition 7.11. *Let $\mathcal{C} \leq R^{2n}$ be a linear code. Then*

$$\mathcal{C}^\perp = \{v \in R^{2n} \mid \chi(\langle v \,|\, w \rangle_s) = 1 \text{ for all } w \in \mathcal{C}\}.$$

Theorem 7.12 ([19, Thm. 3.12])**.** *Let $\mathcal{C} \leq R^{2n}$ be a submodule. Then $\mathcal{C}$ is a stabilizer code iff $\mathcal{C} \subseteq \mathcal{C}^\perp$. Thus, the stabilizer codes are exactly the self-orthogonal linear codes of R^{2n} with respect to the symplectic inner product.*

Proof. "⇒" Let $\mathcal{C} = \Psi(S)$ for some stabilizer $S \leq \mathcal{P}_n$. We have to show that $\mathcal{C} \subseteq \mathcal{C}^\perp$. Let $v = (a, b)$, $w = (a', b') \in \mathcal{C}$. Since $E = \Psi^{-1}(v), E' = \Psi^{-1}(w) \in S$, they commute. Write $E = \omega^\ell X(a)Z(b)$, $E' = \omega^{\ell'} X(a')Z(b')$. Then Proposition 7.2 and the definition of the symplectic inner product yield $\chi\big(\langle v \,|\, w \rangle_s\big) = 1$. Now Proposition 7.11 implies $v \in \mathcal{C}^\perp$, and thus $\mathcal{C} \subseteq \mathcal{C}^\perp$.
"⇐" Recall N and ω from Definition 7.5. Let now $\mathcal{C} \leq R^{2n}$ be a self-orthogonal linear code. Consider the subset

$$\mathcal{G} = \{\omega^\ell X(a)Z(b) \mid \ell \in \mathbb{Z}, (a, b) \in C\} \tag{7.7}$$

of the Pauli group $\mathcal{P}_n$. Again, Proposition 7.2 implies that $\mathcal{G}$ is an abelian subgroup of $\mathcal{P}_n$. Let ξ be a character of $(\mathcal{G}, \cdot)$ such that $\xi(\omega^\ell I) = \omega^\ell$ for all $\ell \in \mathbb{Z}$. Such character ξ does indeed exist thanks to Remark 2.1(6). Define

$$S \coloneqq \{\xi\big(\chi(ab)X(-a)Z(-b)\big)X(a)Z(b) \mid (a, b) \in \mathcal{C}\} \subseteq \mathcal{G}. \tag{7.8}$$

We show first that S is a group. Let (a, b), $(a', b') \in \mathcal{C}$. With the aid of Proposition 7.2 the following computation implies that S is closed under multiplication:

$$\begin{aligned}
&\xi\big(\chi(ab)X(-a)Z(-b)\big)X(a)Z(b)\xi\big(\chi(a'b')X(-a')Z(-b')\big)X(a')Z(b') \\
&\quad = \xi\big(\chi(ab + a'b')X(-a)Z(-b)X(-a')Z(-b')\big)\chi(ba')X(a + a')Z(b + b') \\
&\quad = \xi\big(\chi(ab + a'b' + ba')X(-a - a')Z(-b - b')\big)\chi(ba')X(a + a')Z(b + b') \\
&\quad = \xi\big(\chi(ab + a'b' + ba')X(-a - a')Z(-b - b')\big)\xi\big(\chi(ba')I\big)X(a + a')Z(b + b') \\
&\quad = \xi\big(\chi(ab + a'b' + ba' + b'a)X(-a - a')Z(-b - b')\big)X(a + a')Z(b + b') \\
&\quad = \xi\big(\chi((a + a')(b + b'))X(-a - a')Z(-b - b')\big)X(a + a')Z(b + b')
\end{aligned}$$

where in the third step we used that $\xi\big(\chi(ba')I\big) = \chi(ba')$ and in the fourth step that $ba' = b'a$ for all (a, b), $(a', b') \in \mathcal{C}$. Next, using $(a', b') = (-a, -b)$ we also obtain closedness with respect to taking inverses. Finally, S is an abelian group such that $S \cap \ker \Psi = \{I\}$ and $\mathcal{C} = \Psi(\mathcal{C})$. □

We include linearity in the definition of stabilizer codes precisely because of the above theorem for otherwise we would not get a one-to-one correspondence; see [19, Ex. 3.11]. We next present an example that summaries the notions introduced so far.

Example 7.13. Let $R = \mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ with $\alpha^2 = \alpha + 1$, and let $n = 1$. Take the generating character χ on $\mathbb{F}_4$ defined by $\chi(1) = 1$ and $\chi(a) = -1$ for $a \in \mathbb{F}_4 \setminus \{0, 1\}$. We use the orthonormal basis

$$\mathcal{B} = \{v_0 = (1, 0, 0, 0)^\mathsf{T}, v_1 = (0, 1, 0, 0)^\mathsf{T}, v_\alpha = (0, 0, 1, 0)^\mathsf{T}, v_{\alpha^2} = (0, 0, 0, 1)^\mathsf{T}\}.$$

Consider the stabilizer code $\mathcal{C} = \operatorname{im}(1,1) \subseteq \mathbb{F}_4^2$. We use the fourth root of unity $\omega = i$, Then (7.7) reads as

$$\mathcal{G} = \{i^\ell X(a)Z(a) \mid \ell \in \mathbb{Z}_4,\, a \in \mathbb{F}_4\}$$

A character $\xi \in \widehat{\mathcal{G}}$ that satisfies $\xi(i^\ell I) = i^\ell$ is given by

$$\xi(i^\ell X(\alpha^t)Z(\alpha^t)) = \xi(i^\ell I)\xi(X(\alpha^t)Z(\alpha^t)) = i^{\ell + \frac{t(t+1)}{2}}.$$

Then, the stabilizer of (7.8) reads as

$$S = \{I_4,\, X(1)Z(1),\, -iX(\alpha)Z(\alpha),\, iX(\alpha^2)Z(\alpha^2)\},$$

which of course satisfies $\Psi(S) = \mathcal{C}$.

What is the appropriate weight function to endow a stabilizer code with? Recall the weight of a Pauli operator from Definition 6.16. Let $v = (a,b) \in R^{2n}$. Since the weight disregards the phases, we can use $\operatorname{wt}(\Psi^{-1}(v))$, making Ψ an isometry. This amounts to the following.

Definition 7.14. The **symplectic weight** of a vector $(a,b) = (a_1,\ldots,a_n,b_1,\ldots,b_n) \in R^{2n}$ is defined as

$$\operatorname{wt}_s(a,b) := |\{i \mid (a_i,b_i) \neq (0,0)\}|.$$

Note that the symplectic weight of $(a_1,\ldots,a_n,b_1,\ldots,b_n) \in R^{2n}$ is the same as the Hamming weight of the rearranged vector $(a_1,b_1,a_2,b_2,\ldots,a_n,b_n) \in (R^2)^n$, where (a_i,b_i) are considered as elements of R^2. We will rely heavily on this simple remark when discussing the equivalence of stabilizer codes is Section 7.3.

Of course, one would want a stabilizer code $\mathcal{C}$ to have the same error-correcting capabilities as the associated quantum stabilizer code.

Definition 7.15. The **minimum distance** of a stabilizer code $\mathcal{C} = \Psi(S)$ is

$$\operatorname{dist}(\mathcal{C}) = \begin{cases} \min\{\operatorname{wt}_s(v) \mid v \in \mathcal{C}^\perp - \mathcal{C}\}, & \text{if } \mathcal{C} \subsetneq \mathcal{C}^\perp \\ \min\{\operatorname{wt}_s(v) \mid v \in \mathcal{C} - \{0\}\}, & \text{if } \mathcal{C} = \mathcal{C}^\perp \end{cases}.$$

We will discuss the minimum distance and general structural results in details in the next section.

7.2 Minimum Distance

In this section we will discuss stabilizer codes over commutative local Frobenius rings. We will use the same notation as in Section 3.4. The symplectic weight is very similar to the Hamming weight and many of the results will hold true even in this new setting. If $\mathcal{C}$ is a stabilizer code then the reduction $\overline{\mathcal{C}}$ is a stabilizer code over the residue field $\mathbb{F} = R/\mathfrak{m}$. If $\mathcal{C}$ is a free stabilizer code then $\mathcal{C}$ and $\overline{\mathcal{C}}$ have the same rate due to Theorem 3.23. However, $\mathcal{C}$ deals with a much larger error basis. How does the

minimum distance of $\mathcal{C}$ compare with the minimum distance of $\overline{\mathcal{C}}$? First, a notation. For a subset X of R^{2n} or $\mathbb{F}^{2n}$ we define

$$\mathrm{d_s}(X) := \min\{\mathrm{wt_s}(x) \mid x \in X - \{0\}\}. \tag{7.9}$$

In [43] the authors consider free stabilizer codes over chain rings, and give[2] an upper bound using the reduction of $\mathcal{C}^\perp - \mathcal{C}$. Namely, they show

$$\mathrm{dist}(\mathcal{C}) \leq \mathrm{d_s}\left(\overline{\mathcal{C}^\perp - \mathcal{C}}\right). \tag{7.10}$$

In order to compare the performance of $\mathcal{C}$ and $\overline{\mathcal{C}}$ the respective minimum distances should be compared instead. Moreover, the quantity on the right hand side of (7.10) behaves unpredictably, especially for non-free stabilizer codes.

In Section 3.4 we considered linear codes with respect to the Hamming weight. As in Theorem 3.25, for a stabilizer code $\mathcal{C}$ one obtains

$$\mathrm{d_s}(\mathcal{C}) = \mathrm{d_s}\left(\overline{(\mathcal{C} : \alpha)}\right) \leq \mathrm{d_s}(\overline{\mathcal{C}}). \tag{7.11}$$

Lemma 3.26 played a crucial role in the proof of Theorem 3.27 to obtain equality for free linear codes. Finding a generating matrix on standard form was trivial in that case since we could simply permute the columns without changing the minimum distance. In this new setting, permuting the columns of a generating matrix may change the symplectic weight, and even worse, it may destroy self-orthogonality. Thus, in order to obtain a standard form we need to establish first the according allowed operations.

Definition 7.16. Let $\mathcal{C} \leq R^{2n}$ be a linear[3] code and $f : \mathcal{C} \longrightarrow R^{2n}$ be a linear map. Then f is called a **symplectic isometry** if $\mathrm{wt_s}(a) = \mathrm{wt_s}(f(a))$ and $\langle a \,|\, b \rangle_\mathrm{s} = \langle f(a) \,|\, f(b) \rangle_\mathrm{s}$ for all $a, b \in R^{2n}$. Two linear codes $\mathcal{C}, \mathcal{C}' \leq R^{2n}$ are called **symplectically isometric** if there exists a symplectic isometry $f : \mathcal{C} \longrightarrow R^{2n}$ such that $f(\mathcal{C}) = \mathcal{C}'$.

Example 7.17. We have two particularly nice symplectic isometries. For every permutation $\sigma \in S_n$ define the map $\tau_\sigma : R^{2n} \longrightarrow R^{2n}$ given by

$$(a_1, \ldots, a_n, b_1, \ldots, b_n) \longmapsto (a_{\sigma(1)}, \ldots, a_{\sigma(n)}, b_{\sigma(1)}, \ldots, b_{\sigma(n)}).$$

For every $i \in [n]$ we define the map $\tau_i : R^{2n} \longrightarrow R^{2n}$ given by

$$(a_1, \ldots, a_n, b_1, \ldots, b_n) \longmapsto (a_1, \ldots, a_{i-1}, b_i, a_{i+1}, \ldots, a_n, b_1, \ldots, b_{i-1}, -a_i, b_{i+1}, \ldots, b_n).$$

It is clear that τ_σ and τ_i preserve the symplectic weight as well as the symplectic inner product.

[2] This is for the case when $\mathcal{C}$ is not self-dual. As we will see, the self-dual case is much easier to deal with.

[3] Although we give this general definition, we will be mainly focusing on symplectic isometries of stabilizer codes.

The following characterizes the structure of free stabilizer codes. To achieve the normal form τ_σ and τ_i are sufficient.

Theorem 7.18 ([19, Thm. 4.7, Prop. 4.9])**.** *Let $\mathcal{C} \leq R^{2n}$ be a free stabilizer code of dimension k. Then $\mathcal{C}$ is symplectically isometric to a free code $\mathcal{C}'$ of the form*

$$\mathcal{C}' = \operatorname{im} \begin{pmatrix} I_k & M & N_1 & N_2 \end{pmatrix} \leq R^{2n}, \tag{7.12}$$

where $M \in \mathcal{M}_{k\times(n-k)}(R)$, $N_1 \in \mathcal{M}_k(R)$, $N_2 \in \mathcal{M}_{k\times(n-k)}(R)$ such that $N_1 + N_2M^\intercal \in \mathcal{M}_k(R)$ is a symmetric matrix. Furthermore, if $\mathcal{C}'$ is as in (7.12), then $\mathcal{C}'$ is self-orthogonal iff $N_1 + N_2M^\intercal$ is symmetric. In addition, the symplectic dual is given by

$$\mathcal{C}^\perp = \operatorname{im} \begin{pmatrix} I_k & 0 & N_1^\intercal & 0 \\ 0 & I_{n-k} & N_2^\intercal & 0 \\ 0 & 0 & M^\intercal & -I_{n-k} \end{pmatrix} = \operatorname{im} \begin{pmatrix} I_k & M & N_1 & N_2 \\ 0 & I_{n-k} & N_2^\intercal & 0 \\ 0 & 0 & M^\intercal & -I_{n-k} \end{pmatrix}.$$

The above theorem, as in Theorem 3.27, implies equality on (7.11). We have the following.

Theorem 7.19. *Let $\mathcal{C} \leq R^{2n}$ be a self-dual stabilizer code. Then $\operatorname{dist}(\mathcal{C}) \leq \operatorname{dist}(\overline{\mathcal{C}})$, with equality if $\mathcal{C}$ is free.*

Proof. When $\mathcal{C}$ is self-dual we have $\operatorname{dist}(\mathcal{C}) = \mathrm{d_s}(\mathcal{C})$. Similarly for $\overline{\mathcal{C}}$. In analogy with the Hamming weight we have $\mathrm{d_s}(\mathcal{C}) \leq \mathrm{d_s}(\overline{\mathcal{C}})$, with equality if $\mathcal{C}$ is free. □

From now on we focus on stabilizer codes that are not self-dual. In such case we have

$$\operatorname{dist}(\mathcal{C}) = \mathrm{d_s}(\mathcal{C}^\perp - \mathcal{C}).$$

The difficulties dealing with non self-dual stabilizer codes arise mainly from the fact that $\mathcal{C}^\perp - \mathcal{C}$ is not a submodule (in fact is not even closed under multiplication). However the necessary machinery is already developed in Section 3.4. Let $\alpha \in R$ be such that

$$\alpha R = \operatorname{soc}(R) = \mathfrak{m}^\perp,$$

as in (3.21) and (3.22), and $\rho : R^{2n} \longrightarrow \mathbb{F}^{2n}$ be as in (3.25). Thanks to (3.26) ρ preserves the symplectic weight.

Theorem 7.20. *Let $\mathcal{C}$ be a free stabilizer code. Then $\operatorname{dist}(\mathcal{C}) \leq \operatorname{dist}(\overline{\mathcal{C}})$.*

Proof. Note first that since ρ preserves the symplectic weight it is enough to show that

$$\rho^{-1}\left(\overline{\mathcal{C}}^\perp - \overline{\mathcal{C}}\right) \subseteq \mathcal{C}^\perp - \mathcal{C}. \tag{7.13}$$

To this end, let $\overline{x} \in \overline{\mathcal{C}}^\perp - \overline{\mathcal{C}}$ for some $x \in R^{2n}$. Thanks to Remark 3.29 we may assume that $x \in \mathcal{C}^\perp$. Then $\rho^{-1}(\overline{x}) = \alpha x \in \mathcal{C}^\perp$. Suppose $\alpha x \in \mathcal{C}$. Then $x \in (\mathcal{C} : \alpha)$, and thus $\overline{x} \in \overline{(\mathcal{C} : \alpha)} = \overline{\mathcal{C}}$, where the latter follows from Theorems 3.27 and 7.18, and we arrive at a contradiction. Thus $\rho^{-1}(\overline{x}) = \alpha x \notin \mathcal{C}$. □

We continue with various sufficient conditions that imply equality in the above theorem. It is precisely the nature of such conditions, along with computational data that motivate the following Conjecture

Conjecture 7.21. $\mathrm{dist}(\mathcal{C}) = \mathrm{dist}(\overline{\mathcal{C}})$ for any free stabilizer code $\mathcal{C} \leq R^{2n}$.

A stabilizer code $\mathcal{C}$ is called **pure** if $\mathrm{dist}(\mathcal{C}) = \mathrm{d_s}(\mathcal{C}^\perp)$. Otherwise, $\mathcal{C}$ is called **impure**. Note that a self-dual stabilizer code is automatically pure. If $\mathcal{C}$ is a free stabilizer code such that the reduced stabilizer code $\overline{\mathcal{C}}$ is pure then (7.11) implies

$$\mathrm{dist}(\overline{\mathcal{C}}) = \mathrm{d_s}(\overline{\mathcal{C}}^\perp) = \mathrm{d_s}(\mathcal{C}^\perp) \leq \mathrm{d_s}(\mathcal{C}^\perp - \mathcal{C}) = \mathrm{dist}(\mathcal{C}),$$

where the in-between inequality follows by the obvious containment $\mathcal{C}^\perp - \mathcal{C} \subseteq \mathcal{C}^\perp$. Along with Theorem 7.20 we have the following.

Theorem 7.22. *Let $\mathcal{C}$ be a free stabilizer code such that $\overline{\mathcal{C}}$ is pure. Then* $\mathrm{dist}(\mathcal{C}) = \mathrm{dist}(\overline{\mathcal{C}})$.

Example 7.23. We provide an example of a free impure stabilizer code for which Conjecture 7.21 holds true. Let $R = \mathbb{Z}_4$, $n = 7$, and $\mathcal{C} = \mathrm{im}\, G$, where

$$G = \left(\begin{array}{ccccccc|ccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 3 & 3 & 2 & 3 & 2 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 3 & 3 & 3 & 3 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 3 & 1 & 3 & 0 & 2 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 3 & 2 & 3 & 1 & 3 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 3 & 1 & 0 & 3 & 2 & 0 \end{array}\right).$$

One checks that $\mathcal{C}$ is a free stabilizer code with dual code $\mathcal{C}^\perp = \mathrm{im}\, H$, where

$$H = \left(\begin{array}{ccccccc|ccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 3 & 3 & 2 & 3 & 2 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 3 & 3 & 3 & 3 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 3 & 1 & 3 & 0 & 2 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 3 & 2 & 3 & 1 & 3 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 3 & 1 & 0 & 3 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 3 & 3 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 0 & 2 & 1 & 2 & 3 \end{array}\right).$$

One computes $\mathrm{d_s}(\mathcal{C}) = \mathrm{d_s}(\mathcal{C}^\perp) = 2$, and $\mathrm{dist}(\mathcal{C}) = 3$ since

$$(0,1,1,0,0,0,1,0)H = (0,1,1,0,0,0,0,0,1,0,0,1,0,0) \in \mathcal{C}^\perp - \mathcal{C}.$$

To obtain the corresponding reductions we simply multiply codewords by 2 modulo 4 and replace the 2s with 1s. Also for the reductions, one computes

$$\mathrm{d_s}(\overline{\mathcal{C}}) = \mathrm{d_s}(\overline{\mathcal{C}}^\perp) = 2, \text{ and } \mathrm{dist}(\overline{\mathcal{C}}) = 3.$$

For $x = (a, b)$ in R^{2n} or $\mathbb{F}^{2n}$ define $\operatorname{supp}(x) := \{i \mid (a_i, b_i) \neq (0, 0)\}$. It is clear that $\operatorname{wt}_s(x) = |\operatorname{supp}(x)|$. For a subset X of R^{2n} or $\mathbb{F}^{2n}$ define

$$\operatorname{supp}(X) := \{\operatorname{supp}(x) \mid x \in X - \{0\}\}.$$

Let $\mathrm{S}(X)$ be the set of all minimal elements of $\operatorname{supp}(X)$ under inclusion. Now let X, Y be any subsets of R^{2n} or $\mathbb{F}^{2n}$. It follows directly by the definitions that

$$\mathrm{S}(X) \subseteq \mathrm{S}(Y) \implies \mathrm{d}_s(Y) \leq \mathrm{d}_s(X).$$

Thus, by taking the contrapositive we obtain

$$\mathrm{d}_s(X) < \mathrm{d}_s(Y) \implies \mathrm{S}(X) \nsubseteq \mathrm{S}(Y). \tag{7.14}$$

Theorem 7.24. *Let $\mathcal{C}$ be a free stabilizer code such that $\mathrm{S}(\mathcal{C}^\perp - \mathcal{C}) \subseteq \operatorname{supp}(\overline{\mathcal{C}}^\perp - \overline{\mathcal{C}})$. Then $\operatorname{dist}(\mathcal{C}) = \operatorname{dist}(\overline{\mathcal{C}})$*

Proof. Assume $\operatorname{dist}(\mathcal{C}) \neq \operatorname{dist}(\overline{\mathcal{C}})$. Thanks to Theorem 7.20 this actually means $\operatorname{dist}(\mathcal{C}) < \operatorname{dist}(\overline{\mathcal{C}})$, and (7.14) implies that there exists $x \in \mathcal{C}^\perp - \mathcal{C}$ such that $\operatorname{supp}(x) \in \mathrm{S}(\mathcal{C}^\perp - \mathcal{C})$ but $\operatorname{supp}(x) \notin \mathrm{S}(\overline{\mathcal{C}}^\perp - \overline{\mathcal{C}})$. The assumption implies that $\operatorname{supp}(x) \in \operatorname{supp}(\overline{\mathcal{C}}^\perp - \overline{\mathcal{C}})$. This implies that $\operatorname{supp}(x)$ is not minimal on $\overline{\mathcal{C}}^\perp - \overline{\mathcal{C}}$. We show next that the latter cannot happen, arriving thus to a contradiction. Indeed, assume there exists $\overline{y} \in \overline{\mathcal{C}}^\perp - \overline{\mathcal{C}}$ such that $\operatorname{supp}(\overline{y}) \subsetneq \operatorname{supp}(x)$. Then (7.13) implies $\rho^{-1}(\overline{y}) \in \mathcal{C}^\perp - \mathcal{C}$. But ρ preserves the symplectic weigh, which in particular yields

$$\operatorname{supp}(\rho^{-1}(\overline{y})) = \operatorname{supp}(\overline{y}) \subsetneq \operatorname{supp}(x).$$

But the latter cannot happen since $\operatorname{supp}(x) \in \mathrm{S}(\mathcal{C}^\perp - \mathcal{C})$. Contradiction! □

We now give an example of non-free stabilizer code. It is worth pointing out that we do not even have an example of **non-free** codes that disprove Conjecture 7.21. When dealing with non-free stabilizer codes one needs to be aware of the strict containment $\overline{\mathcal{C}^\perp} \subsetneq \overline{\mathcal{C}}^\perp$; see also Theorem 3.30(2).

Example 7.25. Let $R = \mathbb{Z}_8$ and let $\mathcal{C} = \operatorname{im} G$, where

$$G := \left(\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 0 & 3 & 0 & 0 & 2 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & 0 & 7 & 7 & 0 \\ 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 2 & 0 & 6 & 6 & 0 & 0 & 0 \end{array}\right).$$

Then $|\mathcal{C}| = 8^3 \cdot 2$ and thus $|\mathcal{C}^\perp| = 8^6 \cdot 4$. The dual code is given by $\mathcal{C}^\perp = \operatorname{im} H$, where

$$H := \left(\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 0 & 3 & 0 & 0 & 2 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & 0 & 7 & 7 & 0 \\ 0 & 0 & 1 & 0 & 0 & 7 & 4 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 7 & 3 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 \end{array}\right).$$

The last row of H shows that $\operatorname{dist}(\mathcal{C}) = 1$. One computes $\mathrm{d_s}(\overline{\mathcal{C}^\perp - \mathcal{C}}) = 2$ whereas $\operatorname{dist}(\overline{\mathcal{C}}) = 1$. In this case (7.10) is strict.

We end this section with a comment. When a stabilizer code $\mathcal{C}$ is free we have $\overline{\mathcal{C}}^\perp - \overline{\mathcal{C}} \subseteq \overline{\mathcal{C}^\perp - \mathcal{C}}$. This yields

$$\mathrm{d_s}\left(\overline{\mathcal{C}^\perp - \mathcal{C}}\right) \leq \operatorname{dist}(\overline{\mathcal{C}}).$$

Thus, Conjecture 7.21 implies equality on (7.10). Example 7.25 shows that freeness is a necessary condition for (7.10). Yet, we are not able to find (should this be possible) a non-free stabilizer code that disproves the conjecture.

7.3 Symplectic Isometries

In this section we discuss symplectic isometries introduced in Definition 7.16. The study will be twofold. We first consider a stronger version of MacWilliams Extension Theorem for symplectic isometries, and then discuss isometry groups of stabilizer codes. The question is, does a symplectic isometry $f : \mathcal{C} \leq R^{2n} \longrightarrow R^{2n}$ extend to a symplectic isometry of R^{2n} for any linear code $\mathcal{C}$? In this case both the symplectic weight and the symplectic inner product have to be preserved. So we are simultaneously also dealing with Witt's Extension Theorem [67] where a bilinear form has to be preserved during the extension. As usual, in order to understand the structure of symplectic isometries, we start with the extremal case $\mathcal{C} = R^{2n}$. Stabilizer codes, that is self-orthogonal codes of R^{2n} differ from this scenario. This is due to the fact that R^{2n} **is not** a stabilizer code and hence symplectic isometries of the extremal case $\mathcal{C} = R^{2n}$ have a much richer structure. However, this case still gives insight on what to expect and aim. We mentioned that the symplectic weight on R^{2n} can be viewed as the Hamming weight on $(R^2)^n$. This allows us to invoke Theorem 3.16(1). We make use of this explicitly via the change of coordinates

$$\gamma : R^{2n} \longrightarrow (R^2)^n, \quad (a_1, \ldots, a_n \,|\, b_1, \ldots, b_n) \longmapsto (a_1, b_1 \,|\, a_2, b_2 \,|\, \ldots \,|\, a_n, b_n). \tag{7.15}$$

For a linear map $f : R^{2n} \longrightarrow R^{2n}$ we define $\tilde{f} := \gamma \circ f \circ \gamma^{-1} : (R^2)^n \longrightarrow (R^2)^n$; see the following commutative diagram.

$$\begin{array}{ccc} R^{2n} & \xrightarrow{\;f\;} & R^{2n} \\ \Big\downarrow{\scriptstyle \gamma} & & \Big\downarrow{\scriptstyle \gamma} \\ (R^2)^n & \xrightarrow[\;\tilde{f}\;]{} & (R^2)^n \end{array} \tag{7.16}$$

Thus for $x = (a_1, b_1 \,|\, \ldots \,|\, a_n, b_n)$ we have $\mathrm{wt_H}(x) = \mathrm{wt_s}(\gamma^{-1}(x))$, that is, the Hamming weight on $(R^2)^n$ is the pullback of the symplectic weight on R^{2n}. In order to transfer the problem completely to $(R^2)^n$ we need to also pull back the symplectic inner product. Namely, define

$$\langle\, x \,|\, y \,\rangle := \langle\, \gamma^{-1}(x) \,|\, \gamma^{-1}(y) \,\rangle_{\mathrm{s}} = \sum_{i=1}^{n} x_i J y_i^{\mathsf{T}}, \tag{7.17}$$

for all $x, y \in (R^2)^n$, where

$$J = XZ = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{7.18}$$

To resume, we obtain the following equivalences

$$f \text{ is } \mathrm{wt_s}\text{-isometry} \iff \tilde{f} \text{ is } \mathrm{wt_H}\text{-isometry} \tag{7.19}$$

and

$$f \text{ preserves } \langle \bullet \,|\, \bullet \rangle_{\mathrm{s}} \iff \tilde{f} \text{ preserves } \langle \bullet \,|\, \bullet \rangle. \tag{7.20}$$

We call $\tilde{f}$ as well a symplectic isometry. With this notation we obtain the structure of symplectic isometries of R^{2n}.

Theorem 7.26. *Let $f : R^{2n} \longrightarrow R^{2n}$ be a linear map. Then f is a symplectic isometry iff the matrix representation of $\tilde{f}$ in $\mathcal{M}_{2n}(R)$ is a block matrix of the form*

$$\mathrm{diag}(A_1, \ldots, A_n)(P \otimes I_2), \tag{7.21}$$

where $A_i \in \mathrm{SL}_2(R)$ and $P \in S_n$ is a permutation matrix.

Proof. For the "if part" note that (7.21) clearly preserves the Hamming weight on $(R^2)^n$. Note also that (7.21) also preserves $\langle \bullet \,|\, \bullet \rangle$. Indeed, for all $A \in \mathcal{M}_2(R)$, we have $AJA^{\mathsf{T}} = \det(A) \cdot J$, and thus

$$AJA^{\mathsf{T}} = J \iff A \in \mathrm{SL}_2(R). \tag{7.22}$$

Now the statement follows by (7.17). For the "only-if part", the existence of A_i and P follows by Theorem 3.16(1). Now assume that $\tilde{f} = \mathrm{diag}(A_1, \ldots, A_n)(P \otimes I_2)$ preserves $\langle \bullet \,|\, \bullet \rangle$. We want to show $A_i \in \mathrm{SL}_2(R)$. Indeed, thanks to (7.17) we have

$$\langle \tilde{f}(x) \,|\, \tilde{f}(y) \rangle = \langle x \,|\, y \rangle \implies \sum_{i=1}^{n} x_i A_i J A_i^{\mathsf{T}} y_i^{\mathsf{T}} = \sum_{i=1}^{n} x_i J y_i^{\mathsf{T}} \tag{7.23}$$

for all $x, y \in (R^2)^n$. Then (7.23) implies $A_i J A_i^{\mathsf{T}} = J$ for all i. Now the statement follows by (7.22). □

Note that (7.21) is precisely an element of $\mathrm{Mon}_{\mathrm{SL}_2(R),n}(\mathcal{M}_2(R))$ from (3.13). This motivates the following definitions.

Definition 7.27. The map $\widetilde{f}$ as in (7.21) is called a $\mathrm{SL}_2(R)$-**monomial map**. We will denote $\mathrm{Mon_{SL}}((R^2)^n)$ the group of $\mathrm{SL}_2(R)$-monomial maps of $(R^2)^n$. The group of $\mathrm{SL}_2(R)$-monomial maps of R^{2n} is given by

$$\mathrm{Mon_{SL}}(R^{2n}) := \{\gamma^{-1} \widetilde{f} \gamma \mid \widetilde{f} \in \mathrm{Mon_{SL}}((R^2)^n)\}.$$

The map $\widetilde{f}$ is called a **monomial map** if $A_i \in \mathrm{GL}_2(R)$ in (7.21). We will denote $\mathrm{Mon}((R^2)^n)$ and $\mathrm{Mon}(R^{2n})$ the groups of monomial maps of $(R^2)^n$ and R^{2n} respectively. If two stabilizer codes are symplectially isometric via a $\mathrm{SL}_2(R)$-monomial map we call them **monomially equivalent**.

We will be using the term "($\mathrm{SL}_2(R)$-) monomial map" interchangeably and it should be clear from context whether we work over $(R^2)^n$ or R^{2n}. Theorem 7.26 implies that all the symplectic isometries of R^{2n} are $\mathrm{SL}_2(R)$-monomial maps. On the the other hand, again thanks to Theorem 7.26, we have that monomial maps preserve the symplectic weight, but not necessarily the symplectic inner product.

Example 7.28. Recall the symplectic isometries of Example 7.17. One easily verifies that the isometry τ_σ transforms to $\widetilde{\tau_\sigma}$ with matrix representation $P_\sigma \otimes I_2$. The isometry τ_i transforms to $\widetilde{\tau_i}$ with matrix representation $\mathrm{diag}(I, \ldots, I, J, I, \ldots, I) \in \mathrm{GL}_{2n}(R)$, with J at the ith diagonal position.

In Section 5.1 we saw that a Hamming isometry $f : \mathcal{C} \leq (R^2)^n \longrightarrow (R^2)^n$ cannot be a monomial map in general. This is due to the fact that the R-module R^2 does not have a cyclic socle; see also Theorem 5.3. What about Hamming isometries that preserve $\langle \bullet \,|\, \bullet \rangle$? Are they given by (7.21)? The following example shows that the answer is still no.

Example 7.29. Let $\mathcal{C} = \mathrm{im}\, G \leq (\mathbb{F}_2^2)^4$ be the $\mathbb{F}_2$-linear code given by

$$\mathcal{C} = \mathrm{im} \left(\begin{array}{cc|cc|cc|cc} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right).$$

Let x_i be the ith row of the above matrix. Consider the linear map $f : \mathcal{C} \longrightarrow (\mathbb{F}_2^2)^n$ given by

$$\begin{array}{rl} x_1 \longmapsto & (1 \;\; 1 \,|\, 1 \;\; 0 \,|\, 1 \;\; 0 \,|\, 1 \;\; 1) \\ x_2 \longmapsto & (0 \;\; 0 \,|\, 0 \;\; 1 \,|\, 1 \;\; 0 \,|\, 1 \;\; 0) \\ x_3 \longmapsto & (0 \;\; 0 \,|\, 0 \;\; 0 \,|\, 0 \;\; 1 \,|\, 0 \;\; 1) \\ x_4 \longmapsto & (0 \;\; 1 \,|\, 0 \;\; 0 \,|\, 1 \;\; 0 \,|\, 1 \;\; 0) \end{array}$$

One checks that f is a Hamming isometry that preserves $\langle \bullet \,|\, \bullet \rangle$. Let G' be the matrix whose ith row is $f(x_i)$. Note that G' has 2×2 zero blocks whereas G does not. It follows easily from this observation that f cannot be extended to a $\mathrm{SL}_2(\mathbb{F}_2)$-monomial map.

Of course we are interested on stabilizer codes. Note that $\mathcal{C}$ from the previous examples is a self-orthogonal code with respect to $\langle \bullet \,|\, \bullet \rangle$ and thus corresponds to a stabilizer code in R^{2n}. Whenever the Extension Property fails the structure of isometries (symplectic isometries in this case) is yet to be discovered. To this end, we start by defining two **isometry groups** of a linear code $\mathcal{C} \leq R^{2n}$:

$$\begin{aligned} \mathrm{Mon}_{\mathrm{SL}}(\mathcal{C}) &:= \{f \in \mathrm{Aut}(\mathcal{C}) \mid f \text{ is the restriction of an } \mathrm{SL}_2(R)\text{-monomial map}\}, \\ \mathrm{Symp}(\mathcal{C}) &:= \{f \in \mathrm{Aut}(\mathcal{C}) \mid f \text{ is a symplectic isometry}\}. \end{aligned} \tag{7.24}$$

Example 7.30. Consider the $\mathbb{F}_2$-linear code $\mathcal{C} \leq (\mathbb{F}_2^2)^4$, generated by either of matrices

$$N_1 = \left(\begin{array}{cc|cc|cc|cc} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right), \quad N_2 = \left(\begin{array}{cc|cc|cc|cc} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right),$$

and the map $\tilde{f} : \mathcal{C} \longrightarrow \mathcal{C}$ that sends the ith row of H_1 to the ith row of H_2. One checks straightforwardly that $\tilde{f}$ is a symplectic isometry. Moreover, $\tilde{f}$ cannot be a $\mathrm{SL}_2(\mathbb{F}_2)$-monomial map due to the fact that there are 2×2 zero blocks in H_2 whereas no zero blocks in H_1.

Thanks to Theorem 7.26 we have $\mathrm{Mon}_{\mathrm{SL}}(\mathcal{C}) \subseteq \mathrm{Symp}(\mathcal{C})$. However, Example 7.30 shows that the containment is strict in general. In what follows we show that the gap can be as big as possible when $R = \mathbb{F}_q$. We then make use of the latter to create stabilizer codes over commutative local Frobenius ring with arbitrarily big isometry groups, answering in this way [19, Q. 7.4]. We heavily rely on the work of Wood [71] on linear codes over matrix modules. We use the very same language and techniques. Thanks to (7.19) and (7.20) it is enough to consider $\mathbb{F}_q$-linear codes over $\mathbb{F}_q^2$ endowed with the Hamming weight and that are self-orthogonal with respect to $\langle \bullet \,|\, \bullet \rangle$. First we set up some notations.

Let $\mathcal{C} \leq \mathbb{F}_q^{2n}$ be a stabilizer code of dimension k, and let G be a generating matrix. Then G is a full-rank $k \times 2n$ matrix over $\mathbb{F}_q$. View G as the linear map $\mathbb{F}_q^k \longrightarrow \mathbb{F}_q^{2n}$, $x \longmapsto xG$ with inputs on the left[4]. Thus

$$\mathcal{C} = \{xG \mid x \in \mathbb{F}_q^k\} = \mathrm{im}\, G = (\mathbb{F}_q^k)G. \tag{7.25}$$

This allows us to think of $\mathcal{C}$ as an embedding of $\mathbb{F}_q^k$ in $\mathbb{F}_q^{2n}$ via G. That is, we can identify $\mathcal{C}$ with the pair $(\mathbb{F}_q^k, G)$. In this way, if $xG \longmapsto yG$ is an automorphism of $\mathcal{C}$ then so is $xG \longmapsto yBG$ for any $B \in \mathrm{GL}_k(\mathbb{F}_q)$. Conversely, for any $f \in \mathrm{Aut}(\mathcal{C})$ there exists (a unique) $B \in \mathrm{GL}_k(\mathbb{F}_q)$ such that the following diagram commutes.

$$\begin{array}{ccccc} \mathbb{F}_q^k & \xrightarrow{G} & \mathcal{C} & \xrightarrow{f} & \mathcal{C} \\ & \searrow^{\exists! B_f} & & & \uparrow G \\ & & & & \mathbb{F}_q^k \end{array} \tag{7.26}$$

In other words, we may make the following identification

$$\{BG \mid B \in \mathrm{GL}_k(\mathbb{F}_q)\} = \mathrm{Aut}(\mathcal{C}). \tag{7.27}$$

Under this identification, we obtain an isomorphism of groups

$$\Phi : \mathrm{Aut}(\mathcal{C}) \longrightarrow \mathrm{GL}_k(\mathbb{F}_q), \;\; f \longmapsto B_f, \tag{7.28}$$

[4]To avoid ambiguities, all inputs in this section will be on the left and we precompose.

where B_f is the unique invertible matrix such that $f = B_f G$. An automorphism of a stabilizer code trivially preserves $\langle \bullet \,|\, \bullet \rangle_s$. With the above identification the second part of (7.24) reads as

$$\mathrm{Symp}(\mathcal{C}) = \{B \in \mathrm{GL}_k(\mathbb{F}_q) \mid \mathrm{wt}_s(xBG) = \mathrm{wt}_s(xG) \text{ for all } x \in \mathbb{F}_q^k\}. \tag{7.29}$$

Next, we address the group $\mathrm{Mon}_{\mathrm{SL}}(\mathcal{C})$. Let $f \in \mathrm{Mon}_{\mathrm{SL}}(\mathcal{C})$. As before, there exists a unique $B_f \in \mathrm{GL}_k(\mathbb{F}_q)$ such that $f = B_f G$. On the other hand, f is the restriction of a $\mathrm{SL}_2(\mathbb{F}_q)$-monomial map M. Thus we have $B_f G = f = M_{|\mathcal{C}}$. Denote[5] by

$$\mathrm{rMon}_{\mathrm{SL}}(\mathcal{C}) := \Phi(\mathrm{Mon}_{\mathrm{SL}}(\mathcal{C})) \leq \mathrm{GL}_k(\mathbb{F}_q). \tag{7.30}$$

Thus, in $\mathrm{GL}_k(\mathbb{F}_q)$ we have two subgroups that we can compare: $\mathrm{rMon}_{\mathrm{SL}}(\mathcal{C})$ and $\mathrm{Symp}(\mathcal{C})$. Of course we have $\mathrm{rMon}_{\mathrm{SL}}(\mathcal{C}) \leq \mathrm{Symp}(\mathcal{C})$. We will show that given $H_1 \leq H_2 \leq \mathrm{GL}_k(\mathbb{F}_q)$ that satisfy some necessary conditions[6], there exists a stabilizer code $\mathcal{C}$ such that $\mathrm{rMon}_{\mathrm{SL}}(\mathcal{C}) \subseteq H_1$ and $H_2 = \mathrm{Symp}(\mathcal{C})$, with equality $\mathrm{rMon}_{\mathrm{SL}}(\mathcal{C}) = H_1$ when $q = 2$. We discuss first the necessary conditions following the line [71]. First we need the notion of closure from group theory. For more details we refer the reader to [65] and [71, Sec. 4].

Definition 7.31. Let a group $\mathcal{G}$ act on a set X from the left and let $H \leq \mathcal{G}$ be a subgroup. For $x \in X$, define $\mathrm{orb}_H(x) := \{hx \mid h \in H\}$. Then the **closure** of H with respect to the action of $\mathcal{G}$ on X is

$$\overline{H} = \{g \in \mathcal{G} \mid g \cdot \mathrm{orb}_H(x) = \mathrm{orb}_H(x) \text{ for all } x \in X\}. \tag{7.31}$$

The subgroup H is called **closed** if $H = \overline{H}$.

We fix the following notation for the remainder of this section.

Notation 7.32. Recall the change of coordinates γ from (7.15). Let $\mathcal{C} \leq \mathbb{F}_q^{2n}$ be a stabilizer code and put $C := \gamma(\mathcal{C}) \leq (\mathbb{F}_q^2)^n$. For a generating matrix G of $\mathcal{C}$ we also put $N = \gamma(G)$, where the latter means that we permute the columns of G according to γ. Clearly $\mathrm{GL}_2(\mathbb{F}_q)$ acts from the right on the matrix space $\mathcal{M}_{k\times 2}(\mathbb{F}_q)$ and $\mathbb{F}_q^\star$ acts from the left on $\mathbb{F}_q^k$. Denote $\mathcal{O}^\#$ and $\mathcal{O}$ the respective orbit spaces. The group $\mathrm{GL}_k(\mathbb{F}_q)$ acts on $\mathcal{O}^\#$ from the left and on $\mathcal{O}$ from the right in an obvious way.

Remark 7.33. Let $C \leq (\mathbb{F}_q^2)^n$ be an $\mathbb{F}_q$-linear code with generating matrix N. In this case we think of N as $k \times n$ matrix whose columns are $k \times 2$ matrices. Similarly as in (7.29) we may define the isometry group of C as

$$\mathrm{Iso}(C) := \{B \in \mathrm{GL}_k(\mathbb{F}_q) \mid \mathrm{wt}_H(xBN) = \mathrm{wt}_H(xN) \text{ for all } x \in \mathbb{F}_q^k\}. \tag{7.32}$$

Next, let $\mathrm{Mon}(C) := \{f \in \mathrm{Aut}(C) \mid f \text{ is the restriction of a monomial map}\}$. We define $\mathrm{rMon}(C) := \Phi(\mathrm{Mon}(C)) \leq \mathrm{GL}_k(\mathbb{F}_q)$. If C is self-orthogonal we naturally put

$$\mathrm{Mon}_{\mathrm{SL}}(C) := \{\widetilde{f} = \gamma \circ f \circ \gamma^{-1} \mid f \in \mathrm{Mon}_{\mathrm{SL}}(\mathcal{C})\} \leq \mathrm{Mon}_{\mathrm{SL}}((\mathbb{F}_q^2)^n), \tag{7.33}$$

[5] We use the same notation as Wood [71] where the extra "r" stand for "restriction" since we may identify B_f with $M_{|\mathcal{C}}$.

[6] Not all subgroups of $\mathrm{GL}_k(\mathbb{F}_q)$ can be isometry groups.

where $\mathcal{C} \coloneqq \gamma^{-1}(C)$. Then $\mathrm{Mon}_{\mathrm{SL}}(C) \subseteq \mathrm{Mon}(C)$. Put $\mathrm{rMon}_{\mathrm{SL}}(C) \coloneqq \Phi(\mathrm{Mon}_{\mathrm{SL}}(C))$. It follows that $\mathrm{rMon}_{\mathrm{SL}}(\mathcal{C}) = \mathrm{rMon}_{\mathrm{SL}}(C)$.

Remark 7.34. Let $C \leq (\mathbb{F}_q^2)^n = \operatorname{im} N$ be a self-orthogonal $\mathbb{F}_q$-linear code and put $\mathcal{C} \coloneqq \gamma^{-1}(C) = \operatorname{im} G$. Then $\mathrm{wt}_{\mathrm{s}}(xG) = \mathrm{wt}_{\mathrm{H}}(xN)$ for all $x \in \mathbb{F}_q^k$. Comparing (7.29) and (7.32) we conclude that $\mathrm{Iso}(C) = \mathrm{Symp}(\mathcal{C})$. In addition, Remark 7.33 implies $\mathrm{rMon}_{\mathrm{SL}}(\mathcal{C}) = \mathrm{rMon}_{\mathrm{SL}}(C) \leq \mathrm{rMon}(C)$. When $q = 2$ we have $\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2)$ and thus $\mathrm{rMon}_{\mathrm{SL}}(\mathcal{C}) = \mathrm{rMon}(C)$.

Remarks 7.33 and 7.34 point out the importance of the isomorphism Φ from (7.28). By considering the images under Φ of all the groups floating around we obtain a unified approach that is independent of the change of coordinates γ.

Example 7.35. Let $\mathcal{C} \leq \mathbb{F}_2^{2\cdot 5}$ be the stabilizer given by the following generating matrix

$$G = \left(\begin{array}{ccccc|ccccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \end{array}\right).$$

Using (7.29) one computes $\mathrm{Symp}(\mathcal{C}) = \mathrm{GL}_3(\mathbb{F}_2)$. On the other hand, only 8 of these symplectic isometries are restrictions of $\mathrm{SL}_2(\mathbb{F}_2)$-monomial maps.

Then, [71, Prop. 4.7] applied to our specific scenario reduces to the following.

Proposition 7.36. *Let $C \leq (\mathbb{F}_q^2)^n$ be a $\mathbb{F}_q$-linear self-orthogonal code of dimension k. Then $\mathrm{rMon}(C)$ is closed with respect to the action of $\mathrm{GL}_k(\mathbb{F}_q)$ on $\mathcal{O}^{\#}$ and $\mathrm{Iso}(C)$ is closed with respect to the action of $\mathrm{GL}_k(\mathbb{F}_q)$ on $\mathcal{O}$.*

Theorem 7.37 ([71, Thm. 5.1])**.** *Let $H_1, H_2 \leq \mathrm{GL}_k(\mathbb{F}_q)$ be two subgroups such that H_1 is closed under the action of $\mathrm{GL}_k(\mathbb{F}_q)$ on $\mathcal{O}^{\#}$ and H_2 is closed under the action of $\mathrm{GL}_k(\mathbb{F}_q)$ on $\mathcal{O}$. Then there exists $n \in \mathbb{N}$ and a $\mathbb{F}_q$-linear code $C \leq (\mathbb{F}_q^2)^n$ such that*

$$H_1 = \mathrm{rMon}(C) \text{ and } H_2 = \mathrm{Iso}(C).$$

Of course there is no reason for the linear code produced in Theorem 7.37 to be self-orthogonal. However, we make use of it to produce a self-orthogonal code of the same dimension without changing the isometry groups. To achieve this we make use of the concatenated code. That is, for a linear code C, the **concatenated code** is defined as

$$C \mid C \coloneqq \{(x \mid x) \mid x \in C\} \leq (\mathbb{F}_q^2)^{2n}. \tag{7.34}$$

Clearly, $C \mid C$ has the same dimension as C, but it is twice as long. In this sense C has a rate twice as large as the rate of $C \mid C$. So of course, achieving self-orthogonality will come with a high cost.

Lemma 7.38. *Let $C = \operatorname{im} N \leq (\mathbb{F}_q^2)^n$ be a $\mathbb{F}_q$-linear code. Then $\mathrm{rMon}(C \mid C) = \mathrm{rMon}(C)$ and $\mathrm{Iso}(C \mid C) = \mathrm{Iso}(C)$.*

Proof. The first statement is a corollary of [71, Prop. 3.7] along with the observation that $C \mid C = \operatorname{im} \widehat{N}$ where $\widehat{N} := N \mid N$ is the corresponding concatenated matrix. Next, by the very definition of the Hamming weight, for all $B \in \mathrm{GL}_k(\mathbb{F}_q)$ we have

$$\mathrm{wt}_{\mathrm{H}}(xN \mid xN) = \mathrm{wt}_{\mathrm{H}}(xBN \mid xBN) \iff \mathrm{wt}_{\mathrm{H}}(xN) = \mathrm{wt}_{\mathrm{H}}(xBN).$$

The second statement then follows. □

Lemma 7.39. *Fix $q = 2^\ell$. Let $C \leq (\mathbb{F}_q^2)^n$ be a $\mathbb{F}_q$-linear code. Then $C \mid C \leq (\mathbb{F}_q^2)^{2n}$ is a self-orthogonal $\mathbb{F}_q$-linear code.*

Proof. Let $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in (\mathbb{F}_q^2)^n$. Then

$$\langle\, (x \mid x) \,|\, (y \mid y) \,\rangle = \sum_{i=1}^{n} x_i J y_i^{\mathsf{T}} + \sum_{i=1}^{n} x_i J y_i^{\mathsf{T}} = 0,$$

since $\mathrm{char}(\mathbb{F}_q) = 2$. Thus $C \mid C$ is self-orthogonal. □

Corollary 7.40. *Let $C \leq (\mathbb{F}_q^2)^n$ be a $\mathbb{F}_q$-linear code where $q = p^\ell$ for some prime p. Then the pth concatenated code $\widetilde{C} := C \mid \cdots \mid C \leq (\mathbb{F}_q^2)^{pn}$ is self-orthogonal code such that $\mathrm{rMon}(C) = \mathrm{rMon}(\widetilde{C})$ and $\mathrm{Iso}(C) = \mathrm{Iso}(\widetilde{C})$.*

We are now ready to prove the main theorem.

Theorem 7.41. *Let $H_1, H_2 \leq \mathrm{GL}_k(\mathbb{F}_q)$ be two subgroups such that H_1 is closed under the action of $\mathrm{GL}_k(\mathbb{F}_q)$ on $\mathcal{O}^{\#}$ and H_2 is closed under the action of $\mathrm{GL}_k(\mathbb{F}_q)$ on $\mathcal{O}$. Then there exists $n \in \mathbb{N}$ and a stabilizer code $\mathcal{C} \leq \mathbb{F}_q^{2n}$ such that*

$$\mathrm{rMon}_{\mathrm{SL}}(\mathcal{C}) \subseteq H_1 \text{ and } H_2 = \mathrm{Symp}(\mathcal{C}), \tag{7.35}$$

with equality $H_1 = \mathrm{rMon}_{\mathrm{SL}}(\mathcal{C})$ if $q = 2$.

Proof. Applying Corollary 7.40 to Theorem 7.37 we can produce a self-orthogonal code $C \leq (\mathbb{F}_q^2)^n$, for some n, such that

$$H_1 = \mathrm{rMon}(C) \text{ and } H_2 = \mathrm{Iso}(C).$$

Now $\mathcal{C} := \gamma^{-1}(C) \leq \mathbb{F}_q^{2n}$ is a stabilizer code that satisfies (7.35), thanks to Remark 7.34. The equality for the case $q = 2$ was also discussed in Remarks 7.33 and 7.34. □

We now address the general case of stabilizer codes over a local commutative Frobenius R. In this case we obtain a weaker version of Theorem 7.41.

Remark 7.42. Let $\mathfrak{m}$ be the maximal ideal of the local ring R and let α a generator of the socle. Recall from Section 3.4 that thanks to (3.22) we obtain a well-defined multiplication

$$\overline{r} \cdot x = rx, \text{ for all } \overline{r} \in \mathbb{F}_q \text{ and } x \in \alpha R, \tag{7.36}$$

which makes αR a $\mathbb{F}_q$-vector space. Let $X \leq R^{2n}$ be a submodule. We denote $\alpha X := \{\alpha x \mid x \in X\}$ and $\overline{X} := \{\overline{x} \mid x \in X\} \leq \mathbb{F}_q^{2n}$. Note that αX is trivially self-orthogonal. Thus, αX is a stabilizer code for any submodule $X \leq R^{2n}$. Recall also

that we have an isomorphism $\rho : \alpha R^{2n} \longrightarrow \mathbb{F}_q^{2n}$ as in (3.25). In addition $\alpha X \cong \overline{X}$ for any submodule $X \leq R^{2n}$, where the isomorphism is R-linear and $\mathbb{F}_q$-linear. In particular, for any $n \in \mathbb{N}$, $\mathbb{F}_q$-linear maps and R-linear maps of $(\alpha R)^n$ coincide.

Theorem 7.43. *Let $H \leq \mathrm{GL}_k(\mathbb{F}_q)$ be a closed subgroup under the action of $\mathrm{GL}_k(\mathbb{F}_q)$ on $\mathcal{O}$. Then there exists $n \in \mathbb{N}$ and a stabilizer code $\mathcal{C} \leq R^{2n}$ such that $H = \mathrm{Symp}(\mathcal{C})$.*

Proof. Let $\widetilde{\mathcal{C}} \leq \mathbb{F}_q^{2n}$ be the stabilizer code produced by Theorem 7.41 that satisfies $H = \mathrm{Symp}(\widetilde{\mathcal{C}})$. Write $\widetilde{\mathcal{C}} = \mathrm{im}\, G$, and let $\overline{g_i}$ be the ith row of G. Then $\mathcal{C} := \rho^{-1}(\widetilde{\mathcal{C}}) \subseteq (\alpha R)^{2n} \leq R^{2n}$ is a stabilizer code over R thanks to Remark 7.42. Let G' be the matrix whose ith row is αg_i. Thanks to (7.36) we have

$$\mathcal{C} = \{xG' \mid \overline{x} \in \mathbb{F}_q^k\} = \mathrm{im}_{\mathbb{F}_q} G'.$$

Furthermore, we mentioned in Remark 7.42 that $\mathbb{F}_q$-linear automorphisms of $\mathcal{C}$ and R-linear automorphisms coincide. This implies $\mathrm{Symp}(\mathcal{C}) = \mathrm{Symp}(\widetilde{\mathcal{C}}) = H$. □

So far we have been comparing symplectic isometries of stabilizer codes with the symplectic isometries of the entire ambient space. But for a stabilizer code $\mathcal{C}$ we have $\mathcal{C} \subseteq \mathcal{C}^\perp$. How do symplectic isometries of $\mathcal{C}$ relate to symplectic isometries of $\mathcal{C}^\perp$? We end this section with an example that addresses this. See also Questions 7.5 and 7.6 in [19].

Example 7.44. Consider the stabilizer code $\mathcal{C} := \gamma^{-1}(C)$ where $C \leq (\mathbb{F}_2^2)^4$ is the self-orthogonal code generated by the matrix

$$G = \left(\begin{array}{cc|cc|cc|cc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right).$$

It is easy to see that $\mathcal{C}^\perp$ is generated by the matrix

$$H = \left(\begin{array}{cc|cc|cc|cc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right).$$

Let g_i be the ith row of G and $f : C \longrightarrow (\mathbb{F}_2^2)^4$ be the symplectic isometry given by

$$\begin{aligned} g_1 &\longmapsto \left(\begin{array}{cc|cc|cc|cc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right) \\ g_2 &\longmapsto \left(\begin{array}{cc|cc|cc|cc} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right) \\ g_3 &\longmapsto \left(\begin{array}{cc|cc|cc|cc} 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \end{aligned}$$

Clearly, there are exactly three self-dual codes C_i such that $C \subsetneq C_i \subsetneq C^\perp$. Namely, if h_i is the ith row of H, they are $C \oplus \langle h_4 \rangle, C \oplus \langle h_5 \rangle$, and $C \oplus \langle h_4 + h_5 \rangle$. We claim that f cannot be extended to a symplectic isometry of $C^\perp$. To that end, assume f extends to a linear map $C^\perp \longrightarrow \mathbb{F}_2^8$ that preserves orthogonality with respect to $\langle \bullet \mid \bullet \rangle$,

called again f. Since C_i's are self-dual so are $f(C_i)$'s. Put $\widetilde{C} := f(C)$. Then $\widetilde{C}^{\perp}$ has generating matrix

$$\widetilde{H} = \left(\begin{array}{cc|cc|cc|cc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right).$$

Similarly, there are three self-dual codes $\widetilde{C}_j$ such that $\widetilde{C} \subsetneq \widetilde{C}_j \subsetneq \widetilde{C}^{\perp}$. Namely, if $\widetilde{h}_i$ is the ith row of $\widetilde{H}$, they are $\widetilde{C} \oplus \langle \widetilde{h}_4 \rangle, \widetilde{C} \oplus \langle \widetilde{h}_5 \rangle$, and $\widetilde{C} \oplus \langle \widetilde{h}_4 + \widetilde{h}_5 \rangle$. Thus $f(C_i) = \widetilde{C}_j$ for some j, and $f(C_i - C) = \widetilde{C}_j - \widetilde{C}$. By comparing the weight-distributions of $C_i - C$ and $\widetilde{C}_j - \widetilde{C}$ for all i, j, we must have $f(C_1) = \widetilde{C}_1$ in order to preserve the Hamming weight. By the same argument f cannot be extended any further.

Table 7.1: Weight distributions of $C_i - C$

C \ C_i	01|00|00|10 (2)	01|00|01|01 (3)	00|00|01|11 (2)
10|00|00|11	11|00|00|01 (2)	11|00|01|10 (3)	10|00|01|00 (2)
00|10|00|00	01|10|00|10 (3)	01|10|01|01 (4)	00|10|01|11 (3)
01|00|10|10	00|00|10|00 (1)	00|00|11|11 (2)	01|00|11|01 (3)
10|10|00|11	11|10|00|01 (3)	11|10|01|10 (4)	10|10|01|00 (3)
01|10|10|10	00|10|10|00 (2)	00|10|11|11 (3)	01|10|11|01 (4)
11|00|10|01	10|00|10|11 (3)	10|00|11|00 (2)	11|00|11|10 (3)
11|10|10|01	10|10|10|11 (4)	10|10|11|00 (3)	11|10|11|10 (4)

Table 7.2: Weight distributions of $\widetilde{C}_j - \widetilde{C}$

$\widetilde{C}$ \ $\widetilde{C}_j$	01|00|00|01 (2)	10|00|01|00 (2)	11|00|01|00 (2)
10|00|00|10	11|00|00|11 (2)	00|00|01|10 (2)	01|00|01|10 (3)
00|01|00|00	01|01|00|01 (3)	10|01|01|00 (3)	11|01|01|00 (3)
01|00|10|01	00|00|10|00 (1)	11|00|11|01 (3)	10|00|11|01 (3)
10|01|00|10	11|01|00|11 (3)	00|01|01|10 (3)	01|01|01|10 (4)
01|01|10|01	00|01|10|00 (2)	11|01|11|01 (4)	10|01|11|01 (4)
11|00|10|11	10|00|10|10 (3)	10|00|11|11 (3)	00|00|11|11 (2)
11|01|10|11	10|01|10|10 (4)	01|01|11|11 (4)	00|01|11|11 (3)

7.4 Applications to the LU-LC Conjecture

In this section we connect symplectic isometries of stabilizer codes with automorphisms of the Pauli group. This naturally brings into play the normalizer of the Pauli group, which is known in literature as the Clifford group. Loosely speaking, we will be discussing quantum gates that preserve the Pauli group.

Recall that for a quantum gate $U \in \mathcal{U}(d^n)$ we have $U^\dagger = U^{-1}$. Thus the normalizer of the Pauli group is given by

$$\mathcal{N}(\mathcal{P}_n) := \{U \in \mathcal{U}(d^n) \mid U\mathcal{P}_n U^\dagger = \mathcal{P}_n\}.$$

Definition 7.45. The n-**qudit Clifford group** is $\mathcal{C}_n := \mathcal{N}(\mathcal{P}_n)/\{e^{i\theta} I\}$.

Note that the Clifford group is simply the normalizer where we disregard the phases. The latter is of course justified by the phase principle. Throughout this section we will pay special attention to the subgroup $\mathcal{C}_1^{\otimes n} \leq \mathcal{C}_n$. We call $U \in \mathcal{C}_n$ a **Clifford operator** whereas $U \in \mathcal{C}_1^{\otimes n}$ a **locally Clifford** (LC) operator. Recall the surjective group homomorphism Ψ from (7.6), with kernel $\ker \Psi = \{\omega^\ell I \mid \ell \in \mathbb{Z}\}$. We will denote $\mathcal{P}_n^* := \mathcal{P}_n / \ker \Psi$. Thus we have an induced isomorphism

$$\Psi^* : \mathcal{P}_n^* \longrightarrow R^{2n}. \tag{7.37}$$

Then Ψ and Ψ^* agree when restricted to stabilizers. The normalizer $\mathcal{N}(\mathcal{P}_n)$ acts on $\mathcal{P}_n$ via conjugation. This induces a well-defined action of $\mathcal{C}_n$ on $\mathcal{P}_n^*$. Stated differently, for all $U \in \mathcal{C}_n$ we obtain a group homomorphism

$$\phi_U : \mathcal{P}_n^* \longrightarrow \mathcal{P}_n^*,\ E \longmapsto UEU^\dagger, \tag{7.38}$$

which in turn is an automorphism of $\mathcal{P}_n^*$.

Remark 7.46. Similarly as above, using the action of $\mathcal{N}(\mathcal{P}_n)$ on $\mathcal{P}_n$ we also obtain a group homomorphism

$$\Phi : \mathcal{N}(\mathcal{P}_n) \longmapsto \mathrm{Aut}(\mathcal{P}_n),\ U \longmapsto \begin{cases} \Phi_U : \mathcal{P}_n & \longrightarrow & \mathcal{P}_n \\ E & \longmapsto & UEU^\dagger \end{cases}. \tag{7.39}$$

Note that $U \in \ker \Phi$ iff U commutes with every Pauli operator. Since the Pauli operators span[7] the matrix space $\mathcal{M}_{d^n}(\mathbb{C})$, we may conclude that

$$\begin{aligned} U \in \ker \Phi &\iff UM = MU \text{ for all } M \in \mathcal{M}_{d^n}(\mathbb{C}) \\ &\iff U \in \{e^{i\theta} I \mid \theta \in \mathbb{R}\}. \end{aligned}$$

Hence $\mathcal{C}_n = \mathcal{N}(\mathcal{P}_n)/\ker \Phi$ can be thought of as a subgroup of $\mathrm{Aut}(\mathcal{P}_n)$. Namely,

$$\mathcal{C}_n \cong \{\Phi_U \mid U \in \mathcal{N}(\mathcal{P}_n)\} \leq \mathrm{Aut}(\mathcal{P}_n). \tag{7.40}$$

Although Remark 7.46 gives a natural connection of the Clifford group with automorphisms of the Pauli group, we focus only on (7.37) and (7.38). Thanks to (7.37) we clearly have $\mathrm{Aut}(\mathcal{P}_n^*) \cong \mathrm{Aut}(R^{2n})$. Moreover, the map $\Psi_U := \Psi^{*-1} \circ \phi_U \circ \Psi^*$ is an automorphism of the additive group $(R^{2n}, +)$ for any $U \in \mathcal{C}_n$. Since Ψ^* and ϕ_U are only group isomorphisms, it is impossible to say anything about R-linearity of Ψ_U. For this reason we restrict ourselves to the Frobenius ring $R := \mathbb{Z}/d\mathbb{Z}$. With this

[7] See (6.4) for the binary case. For the general case see, for instance, [19, Rem. 3.6] and the references therein.

restriction, Ψ_U is R-linear and it is given by right matrix multiplication. Namely, for a matrix $M \in \mathrm{GL}_{2n}(R)$ denote $L_M : x \longmapsto xM$ its induced linear map. Then for every $U \in \mathcal{C}_n$ there exists $M(U) \in \mathrm{GL}_{2n}(R)$ such that the following diagram

$$\begin{array}{ccc} \mathcal{P}_n^* & \xrightarrow{\phi_U} & \mathcal{P}_n^* \\ \Psi^* \downarrow & & \downarrow \Psi^* \\ R^{2n} & \xrightarrow[L_{M(U)}]{} & R^{2n} \end{array} \tag{7.41}$$

Recall N from Theorem 7.4. We will slightly change the notation to the following

$$\overline{c} = \begin{cases} c, & \text{if } c \text{ is odd,} \\ 2c, & \text{if } c \text{ is even.} \end{cases} \tag{7.42}$$

Remark 7.47. Consider (7.41) for $n = 1$ and recall that we have fixed $R := \mathbb{Z}/d\mathbb{Z}$. We will see in Theorem 7.49 below that Ψ_U is a wt_{s}-isometry for every $U \in \mathcal{C}_1$. Theorem 7.26 implies $M(U) \in \mathrm{SL}_2(R)$. The converse is also true, that is,

$$\text{for every } M \in \mathrm{SL}_2(R), \text{ there exists } U(M) \in \mathcal{C}_1 \text{ such that (7.41) commutes.} \tag{7.43}$$

In here we will need only the existence, thus, for the details of the existence we refer the reader to [1, 28]. It is worth mentioning that in these references the arithmetic is modulo $\overline{d}$ where $\overline{d}$ is as in (7.42). Then one shows that the same holds true modulo d; see [2, Lemma A.1], for instance. Hence, (7.43) holds regardless of whether d is odd or even. Now let $U = U_1 \otimes \cdots \otimes U_n \in \mathcal{C}_1^{\otimes n}$. Then

$$M(U) = \mathrm{diag}(M(U_i))_i \tag{7.44}$$

is a $2n \times 2n$ block diagonal matrix, where $M(U_i) \in \mathrm{SL}_2(R)$. In other words, $M(U)$ is a $\mathrm{SL}_2(R)$-monomial map for every $U \in \mathcal{C}_1^{\otimes n}$.

Remark 7.48. Let $S \leq \mathcal{P}_n$ be a stabilizer. By definition $S \cap \ker \Psi = \{I\}$ and thus $\Psi(S) = \Psi^*(S)$ gives rise to a stabilizer code $\mathcal{C} \leq R^{2n}$. It is easy to see that for any $U \in \mathcal{C}_n$ the group

$$\phi_U(S) = USU^\dagger := \{UEU^\dagger \mid E \in S\} \tag{7.45}$$

is again a stabilizer. Thus $\Psi(USU^\dagger)$ also defines a stabilizer code $\mathcal{C}_U \leq R^{2n}$. Moreover, we obtain a quantum stabilizer code $\mathcal{Q}(USU^\dagger)$. It is straightforward to verify that $\mathcal{Q}(USU^\dagger) = U\mathcal{Q}(S) := \{Uv \mid v \in \mathcal{Q}(S)\}$.

Theorem 7.49. *Let $U \in \mathcal{C}_1^{\otimes n}$. Then $\mathcal{C}$ and $\mathcal{C}_U$ as in Remark 7.48. are symplectically isometric.*

Proof. Write $U = U_1 \otimes \cdots \otimes U_n$ with $U_i \in \mathcal{C}_1$. Consider the map $\Psi_U := \Psi^{*-1}\phi_U\Psi^*$. By Remark 7.48 we have $\Psi_U(\mathcal{C}) = \mathcal{C}_U$. Thus, Ψ_U trivially preserves the symplectic inner product on $\mathcal{C}$. To complete the proof we need to show that Ψ_U also preserves the

symplectic weight. Since Ψ is a weight preserving map, it is enough to show that ϕ_U is weight preserving for any $U = U_1 \otimes \cdots \otimes U_n \in \mathcal{C}_1^{\otimes n}$. Indeed, let $E = E_1 \otimes \cdots \otimes E_n \in S$. Recall from Definition (6.16) that $\mathrm{wt}(E) = |\{i \mid E_i \neq I\}|$. Moreover, we have

$$\phi_U(E) = UEU^\dagger = U_1 E_1 U_1^\dagger \otimes \cdots \otimes U_n E_n U_n^\dagger,$$

which in turn implies $\mathrm{wt}(E) = \mathrm{wt}(\phi_U(E))$. □

Notation 7.50. We fix the following notation. A permutation $\sigma \in S_n$ acts on R^n by permuting the coordinates. For $E = \omega^\ell X(a)Z(b)$ we will denote $\sigma(E) := \omega^\ell X(\sigma(a))Z(\sigma(b))$ and for $X \subseteq \mathcal{P}_n$ we will denote $\sigma(X) := \{\sigma(x) \mid x \in X\}$. It is easy to see that $S \leq \mathcal{P}_n$ is a stabilizer iff $\sigma(S) \leq \mathcal{P}_n$ is a stabilizer.

Definition 7.51.

(1) Two quantum stabilizer codes $\mathcal{Q} = \mathcal{Q}(S)$ and $\mathcal{Q}' = \mathcal{Q}(S')$ are called **permutation equivalent** if there exists a permutation $\sigma \in S_n$ such that $S' = \sigma(S)$.

(2) Two quantum stabilizer codes $\mathcal{Q} = \mathcal{Q}(S)$ and $\mathcal{Q}' = \mathcal{Q}(S')$ are called **Clifford permutation equivalent** (CP) (resp., **locally Clifford permutation equivalent** (LCP)) if there exists a permutation $\sigma \in S_n$ and $U \in \mathcal{C}_n$ (resp., $U \in \mathcal{C}_1^{\otimes n}$) such that $S' = U\sigma(S)U^\dagger$.

(3) Two quantum stabilizer codes $\mathcal{Q}$ and $\mathcal{Q}'$ are called **unitary equivalent** (resp., **locally unitary equivalent** (LU)) if there exists $U \in \mathcal{U}(d^n)$ (resp., $U \in \mathcal{U}(d)^{\otimes n}$) such that $\mathcal{Q}' = U\mathcal{Q}$.

If we take σ to be the identity permutation in Definition 7.51(2) then we are dealing with LC equivalent quantum stabilizer codes. It is obvious that two LC equivalent quantum stabilizer codes are also LU equivalent. Is the converse true? This is known in the literature as the LU-LC conjecture [56]. The conjecture was reduced to various subclasses of quantum stabilizer codes [24, 45, 46, 72], to finally be proven incorrect in [31]. One of these subclasses is that of quantum stabilizer states, that is, quantum stabilizer codes of dimension one. Thanks to Theorem 7.12, quantum stabilizer states correspond to self-dual stabilizer codes. The counterexample provided in [31] is randomly generated. Thus the structure of such counterexamples is yet to be discovered. In [55] the authors show that there exist infinitely many stabilizer states that disprove the LU-LC conjecture. A sufficient condition for spotting LU quantum stabilizer states that are not LC is of interest.

Remark 7.52. Note that we defined CP and LCP equivalence of quantum stabilizer codes via their stabilizer groups. This is possible due to Remark 7.48 and Corollary 7.9. Indeed, two quantum stabilizer $\mathcal{Q} = \mathcal{Q}(S)$ and $\mathcal{Q}' = \mathcal{Q}(S')$ codes are LC equivalent iff there exists $U \in \mathcal{C}_1^{\otimes n}$ such that $\mathcal{Q}' = U\mathcal{Q}$. The same cannot be done (local) unitary equivalence. Indeed, if $U \notin \mathcal{C}_n$ then $USU^\dagger \notin \mathcal{P}_n$ and thus $\mathcal{Q}(USU^\dagger)$ no longer makes sense.

The following result characterizes LCP quantum stabilizer codes (and thus LC quantum stabilizer states) using the language of Section 7.3.

Theorem 7.53. *Let $\mathcal{C} = \Psi(S)$ and $\mathcal{C}' = \Psi(S')$ be two stabilizer codes. Then $\mathcal{C}$ and $\mathcal{C}'$ are monomially equivalent iff the quantum stabilizer codes $\mathcal{Q}(S)$ and $\mathcal{Q}(S')$ are LCP equivalent.*

Proof. We show the forward direction, with the other one being similar. Let

$$M = \operatorname{diag}(M_1, \dots, M_n)(P_\sigma \otimes I_2)$$

be a $\mathrm{SL}_2(R)$-monomial map as in (7.21) that maps $\mathcal{C}$ to $\mathcal{C}'$. Let $U_i := U(M_i) \in \mathcal{C}_1$ be as in Remark 7.47 and consider $U := U_1 \otimes \cdots \otimes U_n \in \mathcal{C}_1^{\otimes n}$. Recall the change of coordinates γ from (7.15). For $(a, b) \in \mathcal{C}$ we have

$$\gamma(a, b) =: x = (x_1, \dots, x_n) \in \gamma(\mathcal{C}) =: C \leq (R^2)^n,$$

where $x_i = (a_i, b_i) \in R^2$. Put $E_i = \Psi^{*-1}(x_i)$. Then $E = E_1 \otimes \cdots \otimes E_n \in S$, and every element of S can be written in such way. With this notation we have

$$\begin{aligned} U\sigma(E)U^\dagger &= U_1 E_{\sigma(1)} U_1^\dagger \otimes \cdots \otimes U_n E_{\sigma(n)} U_n^\dagger \\ &= \phi_{U_1}(E_{\sigma(1)}) \otimes \cdots \otimes \phi_{U_n}(E_{\sigma(n)}) \\ &= \phi_{U_1}(\Psi^{*-1}(x_{\sigma(1)})) \otimes \cdots \otimes \phi_{U_n}(\Psi^{*-1}(x_{\sigma(n)})) \\ &= \Psi^{*-1}(x_{\sigma(1)} M_1) \otimes \cdots \otimes \Psi^{*-1}(x_{\sigma(n)} M_n) \\ &\in S', \end{aligned}$$

because $(x_{\sigma(1)}M_1, \dots, x_{\sigma(n)}M_n) \in \gamma(\mathcal{C}')$. Thus $U\sigma(S)U^\dagger \subseteq S'$. Since $|S'| = |\mathcal{C}'| = |\mathcal{C}| = |S| = |U\sigma(S)U^\dagger|$, equality follows. □

We end this section with two examples that relate all the equivalence notions discussed. Throughout we will use $R = \mathbb{F}_2$ and $X := X(1)$, $Z := Z(1)$.

Example 7.54. Let $\mathcal{C} \leq \mathbb{F}_2^{2\cdot 3}$ be the stabilizer code given by the following generating matrix

$$G = \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{array}\right),$$

and consider the $\mathrm{SL}_2(\mathbb{F}_2)$-monomial map given by $M = \operatorname{diag}(M_1, M_2, M_3)(P_\sigma \otimes I_2)$ where we take the permutation to be the cycle $\sigma = (123)$, and

$$M_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, M_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, M_3 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then, $\mathcal{C}' := \{xM \mid x \in \mathcal{C}\}$ is the stabilizer code given the following generating matrix

$$G' = \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{array}\right).$$

Then the corresponding stabilizers are $S = \langle XZX, ZXX, ZZZ\rangle$ and $S' = \langle YZY, XZZ, YXZ\rangle$. To M_i correspond the following Clifford operators that make (7.41) commute:

$$U_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, U_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, U_3 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

One easily verifies $S' = U\sigma(S)U^\dagger$ where $U = U_1 \otimes U_2 \otimes U_3$. The corresponding quantum stabilizer states $\mathcal{Q}(S)$ and $\mathcal{Q}(S')$ are the one-dimensional complex spaces generated by vectors $v = (1,0,0,-1,0,1,1,0)^\intercal$ and $v' = (1,1,-i,i,1,-1,-i,-i)^\intercal$ respectively. By Theorem 7.53 and Remark 7.48 we have

$$\mathcal{Q}(S') = \mathcal{Q}(U\sigma(S)U^\dagger) = U\mathcal{Q}(\sigma(S)). \tag{7.46}$$

Note that $\sigma(S) = \langle ZXX, XXZ, ZZZ\rangle$ and $\mathcal{Q}(\sigma(S))$ is generated by $v'' = (1,0,0,1,0,-1,1,0)^\intercal$. One could also verify (7.46) directly by noting that Uv and v'' differ only by the scalar $(1+i)/2$.

Example 7.55. We revisit Example 7.30 with this new language. So let $\mathcal{C} = \operatorname{im} G$ and $\mathcal{C}' = \operatorname{im} G'$ be the self-dual stabilizer codes where G and G' are as follows

$$G = \left(\begin{array}{cccc|cccc} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right), \quad G' = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{array}\right).$$

The map $f : \mathcal{C} \longrightarrow \mathcal{C}'$ that maps the ith row of G to the ith row of G' is a symplectic isometry and thus $\mathcal{C}$ and $\mathcal{C}'$ are symplectially equivalent. On the other hand, it is easy to see that there cannot exist a $\mathrm{SL}_2(\mathbb{F}_2)$-monomial map between the two. The associated stabilizers are

$$S = \langle XZXX, ZXIX, ZIZI, ZZIZ\rangle,$$
$$S' = \langle YXXY, IZXX, IIZZ, ZIXX\rangle.$$

Then, the respective quantum stabilizer states are

$$\begin{aligned} \mathcal{Q}(S) &= \operatorname{span}_{\mathbb{C}}\{(1,0,0,0,0,0,0,-1,0,0,1,0,0,1,0,0)^\intercal\}, \\ \mathcal{Q}(S') &= \operatorname{span}_{\mathbb{C}}\{(1,0,0,1,0,0,0,0,0,0,0,0,1,0,0,-1)^\intercal\}. \end{aligned} \tag{7.47}$$

Since f is not a $\mathrm{SL}_2(\mathbb{F}_2)$-monomial map Theorem 7.53 implies that $\mathcal{Q}(S)$ and $\mathcal{Q}(S')$ are not LCP equivalent. In fact, they are not even LU equivalent. To show this we make use of the **vectorization** of matrix, that is, $\operatorname{vec}(X)$ of a matrix X is the column vector where we stack the columns of X. Let $X, X' \in \mathcal{M}_4(\mathbb{F}_2)$ be the matrices whose vectorization gives the vectors in (7.47). Namely

$$X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \text{ and } X' = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}.$$

Assume that there exists $U = U_1 \otimes U_2 \otimes U_3 \otimes U_4 \in \mathcal{U}(2)^{\otimes 4}$ such that $\mathcal{Q}(S') = U\mathcal{Q}(S)$. From elementary properties of the Kronecker Product, this is equivalent with

$$(U_3 \otimes U_4)X(U_1^{\mathsf{T}} \otimes U_2^{\mathsf{T}}) = X'.$$

Clearly this is impossible since the right-hand-side has rank 2 whereas the left hand side has rank 4.

7.5 MacWilliams Identities

In this section we will describe MacWilliams Identities [40, Chapter 5] for stabilizer codes over (commutative[8]) Frobenius rings. We will use the famous Gleason's approach [5, §1.12] via the Poisson Summation Formula described in Theorem 2.7, which is in line with the main theme of this thesis. But first we start with a few conventions. Let W be a complex vector space and denote W^R the set of all maps $R \longrightarrow W$. Then one may define the Fourier Transform of $f \in W^R$ to be the map $\widehat{f} \in W^{\widehat{R}}$ similarly as in Definition 2.3. Recall that for Frobenius rings the map $R \longrightarrow \widehat{R}$, $r \longmapsto r\chi$ is an isomorphism. Under this isomorphism and with a slight abuse of notation we will think of $\widehat{f}$ as taking $r \in R$ as an input instead of $r\chi \in \widehat{R}$. In other words, we will think of $\widehat{f}$ as an element of W^R:

$$\widehat{f}(r) \coloneqq \widehat{f}(r\chi) = \sum_{s \in R} f(s)\overline{\chi(rs)}.$$

We will first discuss the MacWilliams Identity with respect the symplectic weight. Let $\mathcal{C} \leq R^{2n}$ be a stabilizer code and put

$$A_i = |\{(a,b) \in \mathcal{C} \mid \mathrm{wt}_{\mathrm{s}}(a,b) = i\}| \text{ and } B_i = |\{(a,b) \in \mathcal{C}^{\perp} \mid \mathrm{wt}_{\mathrm{s}}(a,b) = i\}|. \tag{7.48}$$

Then the **symplectic weight enumerator** of $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are given by the following homogeneous polynomials:

$$\mathrm{WE}_{\mathcal{C}}(U,V) = \sum_{i=1}^{n} A_i U^{n-i} V^i \in \mathbb{C}[U,V],$$
$$\mathrm{WE}_{\mathcal{C}^{\perp}}(U,V) = \sum_{i=1}^{n} B_i U^{n-i} V^i \in \mathbb{C}[U,V].$$

The following result is well-known for additive codes endowed with the Hamming weight. Since the symplectic weight in R^{2n} is the Hamming weight in $(R^2)^n$, the very same proof works for our case, which we include for completeness.

Theorem 7.56. *Let R be a (commutative) Frobenius ring with d elements, and let $\mathcal{C} \leq R^{2n}$ be a stabilizer code. Then*

$$\mathrm{WE}_{\mathcal{C}}(U,V) = \frac{1}{|\mathcal{C}^{\perp}|}\mathrm{WE}_{\mathcal{C}^{\perp}}(U + (d^2-1)V, U - V).$$

[8] The only reason we assume commutativity is so that Theorem 7.12 holds.

Proof. Set $W = \mathbb{C}[U,V]$ and consider $x = (a,b) = (a_1,\ldots,a_n,b_1,\ldots,b_n) \in R^{2n}$. Define $f_i : R^2 \longrightarrow W$, $x_i := (a_i,b_i) \longmapsto U^{1-\mathrm{wt_s}(x_i)}V^{\mathrm{wt_s}(x_i)}$ and put

$$f(x) := \prod_{i=1}^{n} f_i(x_i) = \prod_{i=1}^{n} U^{n-\mathrm{wt_s}(x)}V^{\mathrm{wt_s}(x)}.$$

Note that $x_i\chi = (a_i,b_i)\chi = (a_i\chi, b_i\chi)$ is the trivial character iff $\mathrm{wt_s}(x_i) = 0$. This fact along with the orthogonality relations (2.1) implies

$$\widehat{f}_i(x_i) = \begin{cases} U + (d^2-1)V, & \text{if } x_i = (0,0), \\ U - V, & \text{if } x_i \neq (0,0). \end{cases} \tag{7.49}$$

Now we compute

$$\begin{aligned}
\mathrm{WE}_{\mathcal{C}}(U,V) &= \sum_{x\in\mathcal{C}} f(x) && \text{(by definition)} \\
&= \frac{1}{|\mathcal{C}^\perp|}\sum_{c\in\mathcal{C}^\perp} \widehat{f}(x) && \text{(by Theorem 2.7)} \\
&= \frac{1}{|\mathcal{C}^\perp|}\sum_{c\in\mathcal{C}^\perp}\prod_{i=1}^{n} \widehat{f}_i(x_i) && \text{(by Remark 2.5)} \\
&= \frac{1}{|\mathcal{C}^\perp|}\sum_{c\in\mathcal{C}^\perp}(U+(d^2-1)V)^{n-\mathrm{wt_s}(x)}(U-V)^{\mathrm{wt_s}(x)} && \text{(by (7.49))} \\
&= \frac{1}{|\mathcal{C}^\perp|}\mathrm{WE}_{\mathcal{C}^\perp}(U+(d^2-1)V, U-V) && \text{(by definition).}
\end{aligned}$$

□

We point out in here that Theorem 7.56 applies exclusively to quantum stabilizer codes for which the symplectic weight enumerators can be defined via the stabilizer groups. Weight enumerators for general quantum codes were defined by Shor and Laflamme [58]. For a quantum code $\mathcal{Q} \leq \mathbb{C}^{d^n}$ of dimension K and orthogonal projector $P : \mathbb{C}^{d^n} \longrightarrow \mathcal{Q}$, instead of (7.48) one uses

$$A_i^{\mathrm{SL}} = \frac{1}{K^2}\sum_{\substack{E\in\mathcal{P}_n \\ \mathrm{wt}(E)=i}} \mathrm{Tr}(E^\dagger P)\mathrm{Tr}(EP) \text{ and } B_i^{\mathrm{SL}} = \frac{1}{K}\sum_{\substack{E\in\mathcal{P}_n \\ \mathrm{wt}(E)=i}} \mathrm{Tr}(E^\dagger PEP). \tag{7.50}$$

Then the corresponding MacWilliams Identity along with other generalizations were established in [52, 53, 58]. As pointed out in [32, Lem. 22], the quantities in (7.50) are just scalar multiples of the quantities in (7.48) for quantum stabilizer codes, and thus they encode the same information. In turn, this fact allows for a much pleasant approach. In [32, Thm. 23] the authors show a MacWilliams Identity for quantum stabilizer codes over finite fields where they use a slightly different symplectic weight enumerator (they use a polynomial in one variable instead a homogeneous polynomial in two variables).

Next, we consider an asymmetric case. It is known from [30] that a quantum channel is asymmetric with respect to errors. Namely, X-errors are much more likely to occur than the Z-errors or the combined XZ-errors. This motivates the

study/construction of quantum codes that can correct X-errors in a much higher rate than the Z-errors. Although this is a very active area of research, in here we will consider only a MacWillimas-type Identity. To that end, for $x = (a, b) \in R^{2n}$ denote

$$\mathrm{wt}_{\mathrm{s,X}}(x) := \mathrm{wt}_{\mathrm{H}}(a) \text{ and } \mathrm{wt}_{\mathrm{s,Z}}(x) := \mathrm{wt}_{\mathrm{H}}(b). \tag{7.51}$$

The above quantities capture the capability of a quantum stabilizer code to correct the respective error. Then, the **asymmetric symplectic weight enumerator** of $\mathcal{C}$ is defined as

$$\mathrm{AWE}_{\mathcal{C}}(U_1, V_1, U_2, V_2) := \sum_{i,j=1}^{n} A_{i,j} U_1^{n-i} V_1^i U_2^{n-j} V_2^j,$$

where $A_{i,j} = |\{x \in \mathcal{C} \mid \mathrm{wt}_{\mathrm{s,X}}(x) = i \text{ and } \mathrm{wt}_{\mathrm{s,Z}}(x) = j\}|$. Similarly, one puts $B_{i,j} = |\{x \in \mathcal{C}^\perp \mid \mathrm{wt}_{\mathrm{s,X}}(x) = i \text{ and } \mathrm{wt}_{\mathrm{s,Z}}(x) = j\}|$ and $\mathrm{AWE}_{\mathcal{C}^\perp}$.

Theorem 7.57. *Let R be a (commutative) Frobenius ring with d elements, and let $\mathcal{C} \leq R^{2n}$ be a stabilizer code. Then*

$$\mathrm{AWE}_{\mathcal{C}}(U_1, V_1, U_2, V_2) = \frac{1}{|\mathcal{C}^\perp|} \mathrm{AWE}_{\mathcal{C}^\perp}(U_1 + (d-1)V_1, U_1 - V_1, U_2 + (d-1)V_2, U_2 - V_2).$$

Proof. As one might have already guessed, the proof is very similar with that of Theorem 7.56, and thus we will only sketch a proof. Consider $x = (a, b) = (a_1, \ldots, a_n, b_1, \ldots, b_n)$. Define

$$f_{1,i}(a_i) := U_1^{1-\mathrm{wt}_{\mathrm{H}}(a_i)} V_1^{\mathrm{wt}_{\mathrm{H}}(a_i)} \text{ and } f_{2,j}(b_j) := U_2^{1-\mathrm{wt}_{\mathrm{H}}(b_j)} V_2^{\mathrm{wt}_{\mathrm{H}}(b_j)}.$$

Then put

$$f(x) = \left(\prod_{i=1}^{n} f_{1,i}(a_i) \right) \left(\prod_{j=1}^{n} f_{2,j}(b_j) \right),$$

and proceed as in the proof of Theorem 7.56. □

Note that the weights defined in (7.51) do not capture the capability of the quantum stabilizer code to independently correct the combined XZ-errors. We end this section by briefly discussing this scenario for the binary case $d = 2$. Let $x = (a, b) \in \mathbb{F}_2^{2n}$. For $c \in \mathbb{F}_2^2$ define

$$\mathrm{wt}_c(x) := |\{i \mid (a_i, b_i) = c\}|. \tag{7.52}$$

Note that, for instance, $\mathrm{wt}_{(1,1)}$ will capture the $Y = iXZ$-errors independently. Then one defines the **complete weight enumerator** of $\mathcal{C} \leq \mathbb{F}_2^{2n}$ as

$$\mathrm{CWE}_{\mathcal{C}}(U_{(0,0)}, U_{(1,0)}, U_{(1,1)}, U_{(0,1)}) := \sum_{x \in \mathcal{C}} \prod_{c \in \mathbb{F}_2^2} U_c^{\mathrm{wt}_c(x)}, \tag{7.53}$$

which as well satisfies a MacWilliams identity. For the details we refer the reader to [69, Section 13.2]. Similar ideas for general binary quantum codes and asymmetric Shor-Laflamme weights are discussed in the recent work [29].

Chapter 8 Conclusion and Future Research

In this thesis we discuss classical and quantum codes over Frobenius alphabets. We provide a unified approach to equivalence related questions. As a preparatory step, we develop a character-theoretic approach to Frobeniusness which does not resort to quasi-Frobeniusness. Equivalence of classical codes is studied via MacWilliams Extension Theorem and isometry groups. We determine the structure of ω-isometries by studying the corresponding induced partition $\mathcal{P}_\omega$. Similarities are drown between the equivalence of classical codes and quantum codes. We introduced the notion of symplectic isometries as a tool to study the equivalence of quantum stabilizer codes. Finally, we discussed the performance of quantum stabilizer codes over Frobenius rings and conjectured that they are as good as quantum stabilizer codes over fields. We established the isometry groups of stabilizer codes and applied the results to LU-LC conjecture. We also discussed MacWilliams Identities for stabilizer codes with respect to the symplectic weight.

We pointed out that whenever a MacWilliams Equivalence Theorem does not hold, the two isometry groups $\mathrm{Mon}_\omega \subsetneq \mathrm{Iso}_\omega$ are different. In this case one wonders how different they could be. However, there is another quite interesting approach one could take. Recall the MacWilliams Extension Property (EP) from Definition 5.1. Theorem 5.3 characterizes alphabets that have EP with respect to the Hamming weight. Consider now a proper field extension E/F. Theorem 5.13 implies that the alphabet ${}_FE$ has EP with respect to the RT weight. Yet, since E does not have a cyclic socle over F, the alphabet does not have EP with respect to the Hamming weight. In [13] Dyshko shows that a "partial" EP holds true. Namely, for any $n \leq |F|$ and code $\mathcal{C} \leq E^n$, every Hamming isometry $f : \mathcal{C} \longrightarrow E^n$ extends to a Hamming isometry of E^n. Moreover, for $N = |F|+1$, there exists a code $\mathcal{C} \leq E^N$ and a Hamming isometry $f : \mathcal{C} \longrightarrow E^N$ that does not extend to a Hamming isometry of E^N. This motivates the following definition and open problem.

Definition 8.1. A left R-module A is of type (N, ω)-EP (or N-EP if the weight is pre-specified) if all the ω-isometries between codes of length at most N extend. An alphabet that has EP with respect to ω is of type ∞-EP.

Problem 8.2. Given a natural number N, a weight function ω, and a left R-module A, under what conditions is A of type N-EP?

We have mentioned that techniques developed in this thesis also apply to weights like RT and poset weight that are not additively extended from the alphabet to the ambient space. There is a very interesting and important instance that fits this scenario: the **rank weight** in **linear network coding**. Consider $\mathbb{F}_{q^m}$, $d \in \{1, \ldots, n\}$ where $n < m$, and put $k = n - d + 1$. Fix a vector $g = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ such that

$\{g_1, \ldots, g_n\}$ is linearly independent over $\mathbb{F}_q$. Define

$$G = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^q & g_2^q & \cdots & g_n^q \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & g_n^{q^{k-1}} \end{pmatrix}.$$

Then $\mathcal{C}_{g,k} \coloneqq \operatorname{im}_{\mathbb{F}_{q^m}} G$ is called a **Gabidulin code** [15]. One endows $\mathcal{C}_{g,k}$ with the rank weight. Namely, for $v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$ define

$$\mathrm{wt}_{\mathrm{rk}}(v) = \dim_{\mathbb{F}_q}(\operatorname{span}_{\mathbb{F}_q}\{v_1, \ldots, v_n\}). \tag{8.1}$$

$\mathbb{F}_{q^m}$-linear $\mathrm{wt}_{\mathrm{rk}}$-isometries of $\mathbb{F}_{q^m}^n$ are well-known in the network coding community [8]. As usual, we have two associated isometry groups: $\mathrm{Mon}_{\mathrm{wt}_{\mathrm{rk}}}(\mathcal{C}_{g,k}) \subseteq \mathrm{Iso}_{\mathrm{wt}_{\mathrm{rk}}}(\mathcal{C}_{g,k})$ (see (1.1)) where the containment is strict as it can be seen from a modified version of [6, Ex. 2.9(a)].

Problem 8.3. How big can the gap $\mathrm{Mon}_{\mathrm{wt}_{\mathrm{rk}}}(\mathcal{C}_{g,k}) \subsetneq \mathrm{Iso}_{\mathrm{wt}_{\mathrm{rk}}}(\mathcal{C}_{g,k})$ be?

Next, we list some future directions in quantum computation. Of course, an obvious future direction would be to settle Conjecture 7.21. As we mentioned, we are not able to construct non-free stabilizer codes that disprove the conjecture.

Problem 8.4. Prove Conjecture 7.21. Determine whether or not the conjecture holds true for non-free stabilizer codes.

Problem 8.5. Is Theorem 7.20 true for any stabilizer code?

In Theorem 7.41 we showed that the gap between the isometry groups of stabilizer codes can be as big as possible. However, the stabilizer codes constructed with predetermined isometry groups are asymptotically bad. Indeed, the rate goes to zero as the characteristic of the alphabet goes to infinity.

Problem 8.6. Construct asymptotically good stabilizer codes that satisfy Theorem 7.41.

For the general case over local Frobenius rings a partial result is presented. In this case, the group $\mathrm{Symp}(\mathcal{C})$ is easily understood and related with the case of stabilizer codes over fields. Whereas, since $\mathrm{SL}_2(R) \neq \mathrm{SL}_2(\mathbb{F}_q)$ (R finite local Frobenius ring and $\mathbb{F}_q = R/\mathfrak{m}$ the residue field), the techniques presented in this thesis do not help toward understanding $\mathrm{Mon}_{\mathrm{SL}}(\mathcal{C})$.

Problem 8.7. Establish an analogous result as in Theorem 7.41 for stabilizer codes over Frobenius rings.

In Section 7.4 we related equivalence notions of quantum stabilizer codes with symplectic isometries. In particular, Theorem 7.53 characterizes LCP equivalence in terms of $\mathrm{SL}_2(R)$-monomial maps. We view this as the first step toward systematically constructing LU equivalent stabilizer states that are not LC. Of course, much more

work is needed to understand the structure of counterexamples of LU-LC conjecture. The strategy for searching for such counterexamples was already pointed out in Example 7.55. Let us make this precise. Let $\mathcal{C} = \operatorname{im} G$, $\mathcal{C}' = \operatorname{im} G' \subseteq \mathbb{F}_q^{2n}$ be two stabilizer codes of the same dimension. Define two isometry groups

$$\operatorname{rMon}(\mathcal{C}, \mathcal{C}') := \{B \in \mathrm{GL}_k(\mathbb{F}_q) \mid GM_{|\mathcal{C}} = BG', M \text{ is an } \mathrm{SL}_2(\mathbb{F}_q)\text{-monomial map}\},$$
$$\operatorname{Symp}(\mathcal{C}, \mathcal{C}') := \{B \in \mathrm{GL}_k(\mathbb{F}_q) \mid \mathrm{wt}_{\mathrm{s}}(xG) = \mathrm{wt}_{\mathrm{s}}(xBG') \text{ for all } x \in \mathbb{F}_q^k\}.$$

Example 7.55 shows that $\operatorname{rMon}(\mathcal{C}, \mathcal{C}') \subsetneq \operatorname{Symp}(\mathcal{C}, \mathcal{C}')$ in general. Let $f \in \operatorname{Symp}(\mathcal{C}, \mathcal{C}') - \operatorname{rMon}(\mathcal{C}, \mathcal{C}')$. Since $f \notin \operatorname{rMon}(\mathcal{C}, \mathcal{C}')$, Theorem 7.53 guarantees that $\mathcal{Q}(\Psi^{-1}(\mathcal{C}))$ and $\mathcal{Q}(\Psi^{-1}(\mathcal{C}'))$ cannot be LCP stabilizer codes. So if they are LU equivalent to start with, we have a counterexample. Unfortunately it is not clear how LU equivalence fits into the language of Section 7.3. Thus more work is needed for understanding what symplectic isometries produce LU equivalent quantum stabilizer codes. As far as LU-LC conjecture is concerned we may restrict ourselves on quantum stabilizer states, to which correspond self-dual stabilizer codes.

Problem 8.8. Let $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_q^{2n}$ be two self-dual stabilizer codes. Establish how different $\operatorname{rMon}(\mathcal{C}, \mathcal{C}')$ and $\operatorname{Symp}(\mathcal{C}, \mathcal{C}')$ can be. That is, let $H, K \leq \mathrm{GL}_n(\mathbb{F}_q)$ be two groups that satisfy some reasonable necessary conditions. Is it possible to construct two self-dual stabilizer codes $\mathcal{C}$ and $\mathcal{C}'$ such that $H = \operatorname{rMon}(\mathcal{C}, \mathcal{C}')$ and $K = \operatorname{Symp}(\mathcal{C}, \mathcal{C}')$?

Problem 8.9. Let $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_q^{2n}$ be two self-dual stabilizer codes, and $f : \mathcal{C} \longrightarrow \mathcal{C}'$ be a symplectic isometry. Find sufficient conditions for the existence of $U \in \mathcal{U}(q)^{\otimes n}$ with $\mathcal{Q}(\Psi^{-1}(\mathcal{C}')) = U\mathcal{Q}(\Psi^{-1}(\mathcal{C}))$.

Note that a rather weak necessary condition for symplectic isometries that produce LU states was mentioned in Example 7.55. Namely, if v and v' are generators of two quantum stabilizer states, then the $n \times n$ matrices X, X' with $v = \text{vectorization}(X)$ and $v' = \text{vectorization}(X')$ must have the same rank.

Continuing with the line of Problem 8.9 we introduce the following group:

$$\operatorname{LUSymp}(\mathcal{C}) := \{f \in \operatorname{Symp}(\mathcal{C}, \mathcal{C}') \mid f \text{ corresponds to a LU map}\}. \tag{8.2}$$

It follows that $\operatorname{Mon}_{\mathrm{SL}}(\mathcal{C}, \mathcal{C}') \subseteq \operatorname{LUSymp}(\mathcal{C}, \mathcal{C}') \subseteq \operatorname{Symp}(\mathcal{C}, \mathcal{C}')$. The latter containment is also strict, as one can see from Example 7.55. Since the LU-LC conjecture is false, it follows that the former containment is also strict.

Problem 8.10. Characterize the group $\operatorname{LUSymp}(\mathcal{C}, \mathcal{C}')$. How big can the differences between the three groups be?

Bibliography

[1] D. M. Appleby, *Symmetric informationally complete-positive operator valued measures and the extended Clifford group*, J. Math. Phys. **46** (2005), no. 5, 052107, 29.

[2] D. M. Appleby, Ingemar Bengtsson, Stephen Brierley, Markus Grassl, David Gross, and Jan-Ake Larsson, *The monomial representations of the Clifford group*, Quantum Inf. Comput. **12** (2012), no. 5-6, 404–431.

[3] Alexei Ashikhmin and Emanuel Knill, *Nonbinary quantum stabilizer codes*, IEEE Trans. Inform. Theory **47** (2001), no. 7, 3065–3072.

[4] E. F. Assmus Jr., *The category of linear codes*, IEEE Trans. Inform. Theory **44** (1998), no. 2, 612–629.

[5] E. F. Assmus Jr. and H. F. Mattson Jr., *Coding and combinatorics*, SIAM Rev. **16** (1974), 349–388.

[6] Aleams Barra and Heide Gluesing-Luerssen, *MacWilliams extension theorems and the local-global property for codes over Frobenius rings*, J. Pure Appl. Algebra **219** (2015), no. 4, 703–728.

[7] H. Bass, *K-theory and stable algebra*, Inst. Hautes Études Sci. Publ. Math. **22** (1964), 5–60.

[8] Thierry P. Berger, *Isometries for rank distance and permutation group of Gabidulin codes*, IEEE Trans. Inform. Theory **49** (2003), no. 11, 3016–3019.

[9] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, *Quantum error correction and orthogonal geometry*, Phys. Rev. Lett. **78** (1997), no. 3, 405–408.

[10] A. Robert Calderbank, Eric M. Rains, P. W. Shor, and Neil J. A. Sloane, *Quantum error correction via codes over* GF(4), IEEE Trans. Inform. Theory **44** (1998), no. 4, 1369–1387.

[11] H. L. Claasen and R. W. Goldbach, *A field-like property of finite rings*, Indag. Math. (N.S.) **3** (1992), no. 1, 11–26.

[12] Hai Quang Dinh and Sergio R. López-Permouth, *On the equivalence of codes over finite rings*, Appl. Algebra Engrg. Comm. Comput. **15** (2004), no. 1, 37–50.

[13] Serhii Dyshko, *On extendability of additive code isometries*, Adv. Math. Commun. **10** (2016), no. 1, 45–52.

[14] Noha ElGarem, Nefertiti Megahed, and Jay A. Wood, *The extension theorem with respect to symmetrized weight compositions*, Coding theory and applications, 2015, pp. 177–183.

[15] Ernst M. Gabidulin, *Theory of codes with maximal rank distance. Probl. Inf. Transm.*, 21:1-12, 1985.

[16] Heide Gluesing-Luerssen, *Partitions of Frobenius rings induced by the homogeneous weight*, Adv. Math. Commun. **8** (2014), no. 2, 191–207.

[17] ———, *Fourier-reflexive partitions and MacWilliams identities for additive codes*, Des. Codes Cryptogr. **75** (2015), no. 3, 543–563.

[18] ———, *The homogeneous weight partition and its character-theoretic dual*, Des. Codes Cryptogr. **79** (2016), no. 1, 47–61.

[19] Heide Gluesing-Luerssen and Tefjol Pllaha, *On quantum stabilizer codes derived from local Frobenius rings*. Submitted. arXiv:1710.09884.

[20] ———, *Extension theorems for various weight functions over Frobenius bimodules*, J. Algebra Appl. **17** (2018), no. 3, 1850052, 28.

[21] Daniel Gottesman, *Stabilizer codes and quantum error correction.* PhD Thesis. arXiv:quant-ph/9705052v1.

[22] M. Greferath and S. E. Schmidt, *Finite-ring combinatorics and MacWilliams' equivalence theorem*, J. Combin. Theory Ser. A **92** (2000), no. 1, 17–28.

[23] Marcus Greferath, Alexandr Nechaev, and Robert Wisbauer, *Finite quasi-Frobenius modules and linear codes*, J. Algebra Appl. **3** (2004), no. 3, 247–272.

[24] David Gross and Maarten Van den Nest, *The LU-LC conjecture, diagonal local operations and quadratic forms over* GF(2), Quantum Inf. Comput. **8** (2008), no. 3-4, 263–281.

[25] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Sole, *The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals, and related codes*, IEEE Transactions on Information Theory **40** (1994), no. 2, 301–319 (eng).

[26] Günther Hauger and Wolfgang Zimmermann, *Quasi-Frobenius-Moduln*, Arch. Math. (Basel) **24** (1973), 379–386.

[27] Thomas Honold, *Characterization of finite Frobenius rings*, Arch. Math. (Basel) **76** (2001), no. 6, 406–415.

[28] E. Hostens, J. Dehaene, and B. de Moor, *Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic*, Phys. Rev. A **71** (2005), no. 4, 042315.

[29] Chuangqiang Hu, Shudi Yang, and Stephen S.-T Yau, *Complete weight distribution and MacWilliams identities for asymmetric quantum codes.* arXiv:1810.11969.

[30] Lev Ioffe and Marc Mézard, *Asymmetric quantum error-correcting codes*, Phys. Rev. A (3) **75** (2007), no. 3, 032345, 4.

[31] Zhengfeng Ji, Jianxin Chen, Zhaohui Wei, and Mingsheng Ying, *The LU-LC conjecture is false*, Quantum Inf. Comput. **10** (2010), no. 1-2, 97–108.

[32] Avanti Ketkar, Andreas Klappenecker, Santosh Kumar, and Pradeep Kiran Sarvepalli, *Nonbinary stabilizer codes over finite fields*, IEEE Trans. Inform. Theory **52** (2006), no. 11, 4892–4914.

[33] A. Klappenecker, *Nice nearrings*, IEEE International Symposium on Information Theory Proceedings, 2012, pp. 170–173.

[34] Emanuel Knill, *Group representations, error bases and quantum codes.* Los Alamos National Laboratory Report LAUR-96-2807; arXiv:quant-ph/9608049, August 1996.

[35] ———, *Non-binary unitary error bases and quantum codes.* Los Alamos National Laboratory Report LAUR-96-2717; arXiv:quant-ph/9608048, 1996.

[36] I. Konstantinesku and V. Khaĭze, *A metric for codes over residue class rings of integers*, Problemy Peredachi Informatsii **33** (1997), no. 3, 22–28.

[37] R. Laflamme, C. Miquel, J.P. Paz, and W.H. Zurek, *Perfect quantum error correcting code*, Physical Review Letters **77** (1996), no. 1, 198–201 (English).

[38] T. Y. Lam, *Lectures on modules and rings*, Graduate Texts in Mathematics, vol. 189, Springer-Verlag, New York, 1999.

[39] ———, *A first course in noncommutative rings*, Second, Graduate Texts in Mathematics, vol. 131, Springer-Verlag, New York, 2001.

[40] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, 1977.

[41] Florence Jessie MacWilliams, *Combinatorial problems of elementary abelian groups*, ProQuest LLC, Ann Arbor, MI, 1962. Thesis (Ph.D.)–Radcliffe College.

[42] Edgar Martínez-Moro and Steve Szabo, *On codes over local Frobenius non-chain rings of order 16*, Noncommutative rings and their applications, 2015, pp. 227–241.

[43] S. Nadella and A. Klappenecker, *Stabilizer codes over frobenius rings*, IEEE International Symposium on Information Theory Proceedings, 2012, pp. 165–169.

[44] A. A. Nechaev and T. Khonol′ d, *Fully weighted modules and representations of codes*, Problemy Peredachi Informatsii **35** (1999), no. 3, 18–39.

[45] Maarten Van den Nest, Jeroen Dehaene, and Bart De Moor, *Graphical description of the action of local Clifford transformations on graph states*, Physical Review A **69** (2005), no. 2, 062323.

[46] ———, *Local unitary versus local Clifford equivalence of stabilizer states*, Phys. Rev. A (3) **71** (2005), no. 6, 062323, 7.

[47] Michael A. Nielsen and Isaac L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.

[48] Graham H. Norton and Ana Sălăgean, *On the Hamming distance of linear codes over a finite chain ring*, IEEE Trans. Inform. Theory **46** (2000), no. 3, 1060–1067.

[49] ———, *On the structure of linear and cyclic codes over a finite chain ring*, Appl. Algebra Engrg. Comm. Comput. **10** (2000), no. 6, 489–506.

[50] Luciano Panek, Marcelo Firer, Hyun Kwang Kim, and Jong Yoon Hyun, *Groups of linear isometries on poset structures*, Discrete Math. **308** (2008), no. 18, 4116–4123.

[51] Tefjol Pllaha, *Symplectic isometries of stabilizer codes*. To appear in J. Algebra Appl. arXiv:1807.09107.

[52] Eric M. Rains, *Quantum weight enumerators*, IEEE Trans. Inform. Theory **44** (1998), no. 4, 1388–1394.

[53] ———, *Quantum shadow enumerators*, IEEE Trans. Inform. Theory **45** (1999), no. 7, 2361–2366.

[54] M. Yu. Rozenblyum and M. A. Tsfasman, *Codes for the m-metric*, Problemy Peredachi Informatsii **33** (1997), no. 1, 55–63.

[55] P Sarvepalli and R Raussendorf, *Local equivalence, surface-code states, and matroids*, Physical Review A **82** (2010), no. 2, 022304.

[56] D. Schlingemann, *Local equivalence of graph states. In O. Krueger and R. F. Werner, Some Open Problems in Quantum Information Theory*. arXiv: quant-ph/0504166.

[57] D. Schlingemann, *Stabilizer codes can be realized as graph codes*, Quantum Inf. Comput. **2** (2002), no. 4, 307–323.

[58] P. Shor and R. Laflamme, *Quantum analog of the MacWilliams identities for classical coding theory*, Physical Review Letters **78** (1997), no. 8, 1600–1602.

[59] Peter W. Shor, *Scheme for reducing decoherence in quantum computer memory*, Phys. Rev. A **52** (1995Oct), R2493–R2496.

[60] M. M. Skriganov, *On linear codes with large weights simultaneously for the Rosenbloom-Tsfasman and Hamming metrics*, J. Complexity **23** (2007), no. 4-6, 926–936.

[61] A. M. Steane, *Error correcting codes in quantum theory*, Phys. Rev. Lett. **77** (1996), no. 5, 793–797.

[62] ———, *Simple quantum error-correcting codes*, Phys. Rev. A **54** (1996Dec), 4741–4751.

[63] Audrey Terras, *Fourier analysis on finite groups and applications*, London Mathematical Society Student Texts, vol. 43, Cambridge University Press, Cambridge, 1999.

[64] Harold N. Ward and Jay A. Wood, *Characters and the equivalence of codes*, J. Combin. Theory Ser. A **73** (1996), no. 2, 348–352.

[65] Helmut Wielandt, *Finite permutation groups.*, Academic paperbacks. Mathematics, Academic Press, New York, 1964.

[66] Robert Wisbauer, *Foundations of module and ring theory*, German, Algebra, Logic and Applications, vol. 3, Gordon and Breach Science Publishers, Philadelphia, PA, 1991. A handbook for study and research.

[67] Ernst Witt, *Theorie der quadratischen Formen in beliebigen Körpern*, J. Reine Angew. Math. **176** (1937), 31–44.

[68] Jay A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), no. 3, 555–575.

[69] ———, *Foundations of linear codes defined over finite modules: the extension theorem and the MacWilliams identities*, Codes over rings, 2009, pp. 124–190.

[70] ———, *Relative one-weight linear codes*, Des. Codes Cryptogr. **72** (2014), no. 2, 331–344.

[71] ———, *Isometry groups of additive codes over finite fields*, J. Algebra Appl. **17** (2018), no. 10, 1850198, 39.

[72] Bei Zeng, Hyeyoun Chung, Andrew W. Cross, and Isaac L. Chuang, *Local unitary versus local Clifford equivalence of stabilizer and graph states*, Physical Review A **75** (2006), no. 3, 032325.

Vita

Tefjol Pllaha

Place of Birth

- Korçë, Albania

Education

- Universiteti i Tiranës, Tiranë, Albania
  Master of Science in Mathematics. July 2011.
- Universiteti i Tiranës, Tiranë, Albania
  Bachelor of Science in Mathematics. July 2009.

Professional Positions

- Postdoctoral Researcher, Aalto University, Espoo, Finland. February 2019 - .
- Research and Teaching Assistant, University of Kentucky, Lexington, KY, USA. August 2013 - December 2018.

Publications

- Marie Meyer and **Tefjol Pllaha**, *Laplacian simplices II: A coding theoretic approach*, Submitted, arXiv:1809.02960.
- Heide Gluesing-Luerssen and **Tefjol Pllaha**, *On quantum stabilizer codes derived from local Frobenius rings*, Submitted, arXiv:1710.09884.
- **Tefjol Pllaha**, *Symplectic isometries of stabilizer codes*, To appear in J. Algebra Appl. arXiv:1807.09107.
- Heide Gluesing-Luerssen and **Tefjol Pllaha**, *Extension theorems for various weight functions over Frobenius bimodules*, J. Algebra Appl. **17** (2018), no. 3, 1850052, 28.