Generalizations of the MacWilliams Extension Theorem

Serhii Dyshko

UNIVERSITÉ DE TOULON

ÉCOLE DOCTORALE Mer et Sciences (ED548)

Institut de Mathématiques de Toulon

THÈSE présentée par :

Serhii DYSHKO

soutenue le : **15 Décembre 2016**

pour obtenir le grade de Docteur en Mathématiques

Généralisations du Théorème d'Extension de MacWilliams

THÈSE dirigée par :

M. LANGEVIN Philippe	Professeur, Université de Toulon

JURY :

M. AUBRY Yves	Maître de conférence HDR, Université de Toulon
M. GREFERATH Marcus	Professeur, Aalto University
M. LEROY André	Professeur, Université d'Artois
M. RANDRIAMBOLOLONA Hugues	Maître de conférence, Telecom ParisTech
M. WOOD Jay	Professeur, Western Michigan University
M. ZEMOR Gilles	Professeur, Université de Bordeaux

CONTENTS

INTRODUCTION

This work is dedicated to investigations of generalizations of one famous result for classical linear codes obtained by a pioneer of coding theory, Florence Jessie MacWilliams. In her thesis, she proved the following extension theorem: "*each linear map of a linear code that preserves the Hamming distance extends to a monomial map.*" Recall that a linear map is called monomial if it acts by permutation of the coordinates and multiplication of each coordinate by a nonzero scalar. The original proof of MacWilliams was refined by Bogart, Goldberg and Gordon. It was later simplified by Ward and Wood using a character-theoretic approach. As it was noted by Goldberg, the MacWilliams Extension Theorem is itself an analogue of the famous Witt's Extension Theorem for quadratic forms. Indeed, the group of monomial maps coincide with the group of linear Hamming isometries of the whole Hamming space.

In the past decades many researches studied linear codes over various module alphabets. In this context an alphabet is a finite module over a ring with identity, a code is a module and maps are module homomorphisms. Varying the ring and the alphabet one gets such important classes of codes as: codes over a ring alphabet, classical linear codes, additive codes. Many other cases covered by the general settings are observed by Greferath in [32] and Schmidt in [36], Hammons, Kumar, Calderbank, Sloane and Solé in [38], Satyanarayana in [53].

However, analogues of the MacWilliams Extension Theorem do not always exist in general. Unlike the classical linear codes, there exist linear codes over a module alphabet with unextendable linear Hamming isometries.

In this thesis I consider the general context of linear codes over a module alphabet and study the extendability of weight preserving maps of the codes.

Let us observe several known results on extension properties of linear codes over a module alphabet. In [64] Wood proved that an extension property holds for codes over Frobenius ring alphabets, using a character-theoretic approach. The same result was also proved in [35] by Greferath and Schmidt, using a combinatorial approach.

The extension problem for module alphabets was partially translated to the case of matrix rings and matrix modules in [16] by Dinh and López-Permouth. There the authors proved the necessary conditions for the existence of a code over a matrix module alphabet with an unextendable Hamming isometry. An explicit construction appeared in the work of Wood [61]. The author developed the ideas of [16] and he found sufficient and necessary conditions under which

an alphabet has an extension property.

Besides the Hamming distance, the properties of codes equipped with other distances and weights are often studied. A general weight is a function defined on an alphabet with numeric values. A weight of a codeword is a sum of weights of each coordinate. The Hamming weight is a particular example of such a weight function, as well as the Lee weight (introduced in [45]), the Euclidean weight and the homogeneous weight, defined by Constantinescu and Heise in [14].

In the present thesis I also study extension properties of general weight preserving maps on linear codes over a module alphabet. By the analogy with the case of the Hamming weight, extendability to monomial maps is studied. Below, a brief description of known results concerning the extension theorem for general weights is given.

The first universal extension criterion for finite ring alphabets equipped with a general weight function was proved in [65] by Wood, where he characterizes an extension property in terms of determinant of a special matrix. The subject was developed by Barra in [5] where various properties and examples are introduced.

Of a particular interest is a special weight, the symmetrized weight composition, which is built on a subgroup of the group of alphabet automorphisms. This weight was introduced by Goldberg in [31] (as a coset weight) for classical linear codes, where he proved an analogue of the extension theorem. The definition of symmetrized weight composition was extended for the case of ring alphabets in [63] by Wood and in [28] by ElGarem and Megahed for module alphabets. The authors found sufficient conditions for an extension property to hold for module alphabets equipped with the symmetrized weight composition. Later, in [2], Assem proved that under several additional assumptions the found conditions are also necessary.

Some other interesting result of Greferath, Langevin, Honold, Fadden and Wood, concerning extension properties of general weights and some particular weights can be found in [26, 33, 44].

One of results of the present work is related to extension problems for combinatorial codes, i.e., codes without any algebraic structure. In these settings I study extendability of Hamming isometries to monomial maps, which are defined in a similar to the classical case way. Despite the fact that for none of the set alphabets an extension property holds, for some classes of combinatorial codes analogue of the extension theorem exist. For example, in [4], [41] and [55] Avgustinovich, Solov'eva, Kovalevskaya, Honold and Heise described several families of combinatorial codes with all Hamming isometries extendable. There they also observed various classes of codes that have unextendable isometries. Among the studied families there are some subclasses of codes that achieve the Singleton bound, some subclasses of equidistant codes and some perfect codes.

The present thesis is organized in the following way. Chapter 1 contains a collection of basic facts of ring and module theories, character theory and coding theory.

Chapter 2 explains a new geometric approach to an extension property of linear codes over a module alphabet. It also contains the known results and our improvements concerning extension properties of module alphabets equipped with the Hamming weight. In Chapter 3 I prove an extension theorem for short linear codes over a matrix module alphabet and give examples for additive codes. It appears that to have an unextendable Hamming isometry, a code should have its length to be greater than some frontier value. The exact bound on the code length is found. Chapter 4 deals with extension properties of special type of codes: MDS codes. Strong geometric properties of MDS codes in many cases are sufficient for the extension property to hold. Some of the results presented in Chapter 2, Chapter 3 and Chapter 4 are published in [19], [23] and [24].

The case of codes over alphabets equipped with symmetrized weight composition and general weight functions is observed in Chapter 5. In this context I improve the known results and I prove a new one. They are published in [22] and [25]. The main contribution of this chapter is a construction of a special linear code and a weight preserving map of the code with the following property: on every codeword the map acts by a permutation of coordinates but there is no monomial map that acts on the code in the same way.

Chapter 6 contains some results on the G-pseudo-injectivity of vector spaces, which is defined in the precedent chapters. The solved problem is related to the extension properties of additive codes. These results can be found in [22].

In Chapter 8 my attention is focused on combinatorial codes. A group of isometries of a classical linear code is the group of those linear bijections from the code to itself that preserve the Hamming distance. For the case of combinatorial codes, along with the group of isometries of a code there is observed the subgroup of those isometries that extend to monomial maps. The two groups may not be the same. In [62] Wood investigated the question of how different the two groups of a linear code over a matrix module alphabet can be. He showed, under certain assumptions, that there exists a linear code over a matrix module alphabet with predefined group of isometries and group of monomial isometries. The main result of the chapter characterizes two isometry groups of a combinatorial codes and is an analogue of the mentioned result of Wood. The material of this chapter appears in [20].

Chapter 7 is related to extension properties of quantum codes and Gabidulin codes.

LIST OF NOTATIONS

$\mathbb{F}_q$	*finite field* with q elements, where q is a prime power.
$\mathfrak{S}(X)$	group of all permutations of a set X.
$\mathfrak{S}_n$	the group $\mathfrak{S}(\{1,\ldots,n\})$.
$X \subseteq Y$	set X is a subset of Y.
$X \subset Y$	set X is a proper subset of Y.
$\mathrm{F}(X,Y)$	set of maps from a set X to a set Y.
$\mathbb{1}_Y$	*indicator function* of a subset $Y \subseteq X$, i.e., a map $\mathbb{1}_Y : X \to \{0,1\}$ such that $\mathbb{1}_Y(x) = 1$ if $x \in Y$ and $\mathbb{1}_Y(x) = 0$ if $x \notin Y$.
$\mathrm{M}_{a\times b}(\mathbb{F}_q)$	set of all $a \times b$ matrices over the finite field $\mathbb{F}_q$.
$\mathrm{GL}_n(\mathbb{F}_q)$	group of invertible $n \times n$ matrices over the finite field $\mathbb{F}_q$.
$\binom{n}{k}$	the binomial coefficient; the number of k-element subsets of an n-element set.
$\begin{bmatrix} n \\ k \end{bmatrix}_q$	the Gaussian binomial (q-binomial) coefficient, where q is a prime power, n and k are nonnegative integers (see Section 3.1).
$\mathrm{Hom}_R(M,N)$	set of R-linear homomorphisms from an R-module M to an R-module N.
$\mathrm{End}_R(M)$	set of R-linear endomorphisms of an R-module M; the same as $\mathrm{Hom}_R(M,M)$.
$\mathrm{Aut}_R(M)$	group of R-linear automorphisms of an R-module M.
$\mathrm{ann}(M)$	annihilator of an R-module M.
$\mathrm{soc}(M)$	socle of an R-module M, see Definition 2.1.3.
$\ker\sigma$	kernel of the map σ.
$\mathrm{im}\,\sigma$	image of the map σ.
ρ_H	the Hamming distance.
wt_H	the Hamming weight.
swc_G	symmetrized weight composition, see Definition 5.0.1.
$H \leq G$	group H is a subgroup of G.
$H < G$	group H is a proper subgroup of G.
$\mathcal{F}$	the Fourier transform, see Section 1.2.
$\widehat{G}$	group of characters of a group G, see Section 1.2.
$\widehat{M}$	character right(left) R-module of a left(right) R-module M, see Section 1.2.
$H^\perp$	group annihilator of a group H, see Section 1.2.
$\overline{G}$	closure of a group G, see Section 5.1.

1. PRELIMINARIES

1.1 Rings and modules

Definition 1.1.1. A *ring* is a non-empty set R with two operations $+, \cdot : R \times R \to R$ with the properties:

- $(R, +)$ is an abelian group (zero element 0);
- $(R, \cdot)$ is a semigroup, i.e., the multiplication is associative;
- for all $a, b, c \in R$ the distributivity rules are valid:

$$(a + b)c = ac + bc, \quad a(b + c) = ab + ac.$$

If there exists an element 1 in a ring R such that for all $a \in R$, $1a = a1 = a$, then R is called a *ring with identity*. In the present thesis we will only consider rings with identity.

Example 1.1.1. The set of all integer numbers $\mathbb{Z}$ with usual operations of multiplication and addition is a ring with identity. Any field is a ring. The set of $k \times k$ matrices over a field together with the operations of matrix addition and matrix multiplication is a ring with the identity I_k, where I_k is a diagonal $k \times k$ matrix with 1s on the diagonal and 0s elsewhere.

Let R be a ring with identity.

Definition 1.1.2. A left *R-module* M is an abelian group together with a multiplication $\cdot : R \times M \to M$, such that, for all $m, m_1, m_2 \in M$ and $r, r_1, r_2 \in R$,

- $r(m_1 + m_2) = rm_1 + rm_2$;
- $(r_1 + r_2)m = r_1m + r_2m$;
- $1m = m$;
- $r_1(r_2m) = (r_1r_2)m$.

A right R-module M is defined similarly, except that the ring acts on the right.

Example 1.1.2. A left *ideal* I of a ring R is an abelian subgroup of $(R,+)$ such that for all $r \in R$ and $a \in I$, $ra \in I$. A left ideal $I \subseteq R$ is a left R-module.

Any abelian group is both left and right $\mathbb{Z}$-module. The set $M = \mathrm{M}_{k\times m}(\mathbb{F}_q)$ of $k \times m$ matrices over the finite field $\mathbb{F}_q$ with the operation of matrix addition is a left $\mathrm{M}_{k\times k}(\mathbb{F}_q)$-module and a right $\mathrm{M}_{m\times m}(\mathbb{F}_q)$-module.

The basic properties of rings, ideals and modules can be found in chapters II and III of [43] and in [60]. All the R-modules observed in the thesis are left R-modules, except the cases where it is stated explicitly. All the definitions, statements and results remain correct if "left" is substituted in place of "right" and "right" is substituted in place of "left".

1.2 Characters and the Fourier transform

Consider the abelian group of nonzero complex numbers with complex multiplication, $(\mathbb{C}^*, \times)$. Let G be a finite abelian group. Recall that an abelian group is a $\mathbb{Z}$-module. Denote by

$$\widehat{G} := \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{C}^*)$$

the *group of characters* of G. The isomorphism holds, $\widehat{G} \cong G$, see [39, Theorem 5.1].

The *Fourier transform* of a map $f : G \to \mathbb{C}$ is a map $\mathcal{F}(f) : \widehat{G} \to \mathbb{C}$ defined as

$$\mathcal{F}(f)(\chi) = \sum_{g\in G} f(g)\chi(g).$$

For a subgroup $H \leq G$,

$$\mathcal{F}(\mathbb{1}_H) = |H|\mathbb{1}_{H^\perp}, \tag{1.1}$$

where the *group annihilator* $H^\perp \leq \widehat{G}$ is defined as

$$H^\perp = \{\chi \in \widehat{G} \mid \forall g \in H, \chi(g) = 1\} = \{\chi \in \widehat{G} \mid \ker\chi \leq H\}.$$

Indeed, for every $\chi \in \widehat{G}$,

$$\mathcal{F}(\mathbb{1}_H)(\chi) = \sum_{g\in G} \mathbb{1}_H(g)\chi(g) = \sum_{g\in H} \chi(g) = |H|\mathbb{1}_{H^\perp},$$

where the last equality comes from [39, Lemma 5.4]. Note that the Fourier transform is invertible, see [57, p. 168]. In [39, Theorem 5.6] the following two facts were proven. For all subgroups $H \leq G$, $N \leq \widehat{G}$,

$$H^{\perp\perp} \cong H, \quad N^{\perp\perp} \cong N.$$

For all subgroups $H_1, H_2 \leq G$, $N_1, N_2 \leq \widehat{G}$,

$$(H_1 \cap H_2)^\perp = H_1^\perp + H_2^\perp, \quad (N_1 \cap N_2)^\perp = N_1^\perp + N_2^\perp. \tag{1.2}$$

From [39, Theorem 5.5], for two abelian groups $H \leq G$,

$$\widehat{H} \cong \widehat{G}/H^{\perp}. \tag{1.3}$$

Let R be a ring with identity. A finite left R-module M is an abelian group. The group of characters $\widehat{M}$ has a natural structure of a right R-module. The ring multiplication is defined as, $(\chi r)(m) = \chi(rm)$, for $\chi \in \widehat{M}$, $r \in R$ and $m \in M$ (see [34, Section 2.2]).

1.3 Hamming space and codes

An *alphabet* A is a finite set with at least two elements. Let n be a positive integer. The *Hamming distance* is the function $\rho_H : A^n \times A^n \to \{0, \ldots, n\}$, defined as, for $x, y \in A^n$,

$$\rho_H(x, y) = |\{i \mid x_i \neq y_i\}|.$$

The set A^n equipped with the Hamming distance is a metric space called the *Hamming space*. A *code* C is a nonempty subset of the Hamming space A^n. The elements of C are *codewords*.

A *Hamming isometry* is a map $f : C \to A^n$ such that for each two codewords $x, y \in C$, $\rho_H(x, y) = \rho_H(f(x), f(y))$, i.e., the map f preserves the Hamming distance.

The alphabet A and the code C may additionally have algebraic structures. For example, the classical coding theory study the case of a finite field alphabet A, where a code is a linear subspace of A^n.

If an alphabet A has the structure of a group, it is convenient to use the *Hamming weight* $\mathrm{wt}_H : A^n \to \{0, \ldots, n\}$, defined as, for $x \in A^n$,

$$\mathrm{wt}_H(x) = \{i \mid x_i \neq e\},$$

where e is the identity element of A. If A is an abelian group, then the identity element is denoted by 0, and the weight of a codewords counts the number of nonzero coordinates. Obviously, the equality holds, for every $x, y \in A^n$,

$$\rho_H(x, y) = \mathrm{wt}_H(xy^{-1}).$$

When A is abelian, the corresponding equality is $\rho_H(x, y) = \mathrm{wt}_H(x - y)$.

1.4 Categories of codes

In [3] Assmus introduced a categorical approach to the error-correcting codes. As it is mentioned before, a code is considered as a nonempty set with some algebraic structure (optional) and a structure of a metric space. An object of the category of codes is a code itself and a morphism $\psi : C \to D$ is a map between two codes that preserves the algebraic structure and for all $x, y \in$

C, $\rho_H(\psi(x), \psi(y)) \leq \rho_H(x, y)$. In such a way an isomorphism of codes is a Hamming isometry.

In the present thesis we consider the codes with the following algebraic structures.

Linear codes over a module alphabet. Let R be a ring with identity and let A be a finite R-module. A code C is a submodule of the R-module A^n. Consequently, a morphism of C is an R-linear Hamming isometry, $f \in \mathrm{Hom}_R(C, A^n)$.

Linear codes over a matrix module alphabet. A particular case of linear codes over a module alphabet with the matrix ring $R = \mathrm{M}_{k\times k}(\mathbb{F}_q)$ and the matrix module alphabet $A = \mathrm{M}_{k\times \ell}(\mathbb{F}_q)$, where k, ℓ are positive integers and q is a power of prime.

Linear codes over a vector space alphabet. A particular case of linear codes over a matrix module alphabet with $k = 1$.

Classical linears codes. A particular case of linear codes over a matrix module alphabet with $k = 1$ and $\ell = 1$.

Group codes over a group alphabet. An alphabet A is a finite group. A code C is a subgroup of A^n. Morphisms of group codes are the Hamming isometries that are the group homomorphisms.

Combinatorial codes. An alphabet A is a finite set. A code is a subset of A^n. A morphism of a code is a Hamming isometry.

Further in the text we will always specify the context that is used.

1.5 Additive codes

Consider the finite field alphabet $A = \mathbb{F}_q$, where $q = p^m$, p is a prime and m is a positive integer. A subset $C \subseteq \mathbb{F}_q^n$ is called an *additive* code if C contains the sum of any two its codewords, i.e., C is an abelian group under addition. Alternatively, C is additive if it is an $\mathbb{F}_p$-linear subspace in $\mathbb{F}_q^n$.

A finite field $\mathbb{F}_q$ is a vector space over $\mathbb{F}_p$ since it is a finite field extension of $\mathbb{F}_p$. Hence, additive codes can be observed as linear codes over a vector space alphabet, where the ground field is $\mathbb{F}_p$.

Remark 1.5.1. Let A be an $\mathbb{F}_q$-linear ℓ-dimensional vector space. There exists an extension field $\mathbb{F}_{q^\ell}$ of $\mathbb{F}_q$ of degree of extension ℓ, which is isomorphic to A as an $\mathbb{F}_q$-linear vector space. Thus, we can consider on A the structure of a finite field.

Let A be an $\mathbb{F}_q$-linear ℓ-dimensional vector space alphabet. A linear code $C \subseteq A^n$ can be seen as an $\mathbb{F}_q$-linear code in the Hamming space $\mathbb{F}_{q^\ell}^n$ and it is additive since it is an abelian group.

In such a way, additive codes and codes over a vector space alphabet represent the same set of codes. In the thesis we identify additive codes and linear codes over a vector space alphabet.

In the case $\ell = 1$, an $\mathbb{F}_q$-linear code is *linear* in the classical sense. If additionally $q = p$, where p is prime, the notions of additive and linear codes coincide.

Example 1.5.1. Let $q = 2$ and let $A = \mathbb{F}_4$ be a field extension of $\mathbb{F}_2$, where $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ and $\omega + 1 = \omega^2$. Note that A is a two-dimensional $\mathbb{F}_q$-linear vector space. Consider two $\mathbb{F}_2$-linear codes

$$C_1 = \{(0,0,0), (1,1,0), (\omega,0,1), (\omega^2,1,1)\},$$

$$C_2 = \{(0,0,0), (0,\omega^2,\omega), (1,0,1), (1,\omega^2,\omega^2)\},$$

in $\mathbb{F}_4^3$. Define a map $f : C_1 \to C_2$ in the following way: $f\big((0,0,0)\big) = (0,0,0)$, $f\big((1,1,0)\big) = (0,\omega^2,\omega)$, $f\big((\omega,0,1)\big) = (1,0,1)$ and $f\big((\omega^2,1,1)\big) = (1,\omega^2,\omega^2)$. Evidently, the map f is $\mathbb{F}_2$-linear and it preserves the Hamming distance. Therefore f is an $\mathbb{F}_2$-linear Hamming isometry of the $\mathbb{F}_2$-linear code C_1 in $\mathbb{F}_4^3$. Both codes C_1 and C_2 are not $\mathbb{F}_4$-linear.

2. EXTENSION CRITERION

2.1 MacWilliams Extension Theorem

Consider the context of classical linear codes with a finite field alphabet A. A map $h : A^n \to A^n$ that acts by permutation of coordinates and by multiplication of coordinates by nonzero scalars in A is called *monomial*. A monomial map is a linear Hamming isometry of the Hamming space. An essential question is whether all the linear code isometries act as monomial maps.

The MacWilliams Extension Theorem describes all the linear isometries of linear codes in A^n.

Theorem 2.1.1 (MacWilliams Extension Theorem, see [48] and [49])**.** *Let $C \subseteq \mathbb{F}_q^n$ be an $\mathbb{F}_q$-linear code. Each $\mathbb{F}_q$-linear Hamming isometry $f : C \to \mathbb{F}_q^n$ extends to a monomial map, i.e., there exist a permutation $\pi \in \mathfrak{S}_n$ and scalars $c_1, \ldots, c_n \in \mathbb{F}_q \setminus \{0\}$ such that, for all $a \in C$,*

$$f\big((a_1, \ldots, a_n)\big) = (c_1 a_{\pi(1)}, \ldots, c_n a_{\pi(n)}).$$

The proof of the theorem appeared in the Ph.D. thesis of F. J. MacWilliams. The original proof was later refined by other researchers in [8] and [58] using different approaches.

We give a definition of a monomial map for the contexts of a module alphabet observed in Section 1.4. Let R be a ring with identity and let A be a finite R-module alphabet. Let $\mathrm{Aut}_R(A)$ denote the group of all R-module automorphisms of A.

Definition 2.1.1. A map $h : A^n \to A^n$ is called *monomial* if there exist a permutation $\pi \in \mathfrak{S}_n$ and automorphisms $g_1, \ldots, g_n \in \mathrm{Aut}_R(A)$ such that, for any $a \in A^n$,

$$h\left((a_1, \ldots, a_n)\right) = \big(g_1(a_{\pi(1)}), \ldots, g_n(a_{\pi(n)})\big)\,.$$

The given definition generalizes the definition of a classical monomial map for linear codes. Indeed, for a finite field $\mathbb{F}_q$, the group $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q)$ consists of multiplications by nonzero elements of the field.

Remark 2.1.1. Note that the group $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q)$ of module automorphisms of a finite field and the group $\mathrm{Gal}(\mathbb{F}_q)$ of automorphisms of a finite field are different. In the first case we consider the bijections $\mathbb{F}_q \to \mathbb{F}_q$ that preserve addition and multiplication by scalars and in the second case we consider the bijections that preserve addition and multiplication. It is known that the group $\mathrm{Gal}(\mathbb{F}_q)$ consists of the Frobenius automorphisms, see [47, p. 113].

The set of monomial maps forms a group, isomorphic to the semi-direct product $(\mathrm{Aut}_R(A))^n \rtimes \mathfrak{S}_n$, which is equal, by definition, to the wreath product $\mathfrak{S}_n \wr \mathrm{Aut}_R(A)$, see [17, Section 2.6].

The definition of the monomial map for the contexts of group codes and combinatorial codes can be obtained from Definition 2.1.1 by replacing $\mathrm{Aut}_R(A)$ with the corresponding automorphism group: the group $\mathrm{Aut}(A)$ of group automorphisms of A for group codes, and the group $\mathfrak{S}(A)$ of permutations of A for combinatorial codes.

For the combinatorial codes, a full description of the Hamming isometries of A^n is given.

Theorem 2.1.2 (see [9, 13])**.** *Let A be a finite set alphabet and let n be a positive integer. A map $h : A^n \to A^n$ is a Hamming isometry if and only if h is a monomial map.*

An analogue of this theorem holds for the Hamming isometries of A^n in all the contexts. We formulate the statement and give the proof for the context of module alphabets. The same statement with a similar proof holds for group codes.

Proposition 2.1.1. *Let A be a finite R-module alphabet and let n be a positive integer. A map $h \in \mathrm{End}_R(A^n)$ is a Hamming isometry if and only if h is a monomial map.*

Proof. It is easy to see that a monomial map is R-linear and preserves the Hamming distance. Conversely, if h preserves the Hamming distance, then, considering A as a set, from Theorem 2.1.2, the map h acts by permutation of columns $\pi \in \mathfrak{S}_n$ and by permutation of coordinates $\sigma_1, \ldots, \sigma_n \in \mathfrak{S}(A)$. Since h is R-linear, each map $\sigma_i : A \to A$ is an R-linear automorphism of A. Hence, $\sigma_i \in \mathrm{Aut}_R(A)$. Therefore, h is a monomial map. □

Except for the case of classical linear codes, a general analogue of the MacWilliams Extension Theorem does not exist for other contexts. That is, there exists a code and there exists a Hamming isometry of this code that does not extend to a monomial map. The following example of an unextendable code isometry for combinatorial codes can be found in [4].

Example 2.1.1. Let $A = \{0, 1\}$. The two codes in A^4

$$C = \{(0,0,0,0), (1,1,0,0), (1,0,1,0), (0,1,1,0)\}$$

and

$$D = \{(0,0,0,0), (1,1,0,0), (1,0,1,0), (1,0,0,1)\}$$

are isometric, i.e. there exists a Hamming isometry $f : C \to D$. Indeed, in both codes the Hamming distance between two different codewords is 2, thus any bijection $f : C \to D$ is a Hamming isometry. For any position, there exist two different codewords in D that have different values in this position. But all the codewords in C have equal values on the fourth position. Hence, any Hamming isometry between these two codes cannot be extended to a monomial map.

In the thesis there are presented various examples of unextendable Hamming isometries for other contexts.

Definition 2.1.2. We say that an R-linear alphabet A has an *extension property* if for any positive integer n and for any R-linear code $C \subseteq A^n$ each R-linear Hamming isometry $f \in \mathrm{Hom}_R(C, A^n)$ extends to a monomial map.

One can easily get similar definitions of an extension property for group and combinatorial codes. Note that in the context of classical linear codes, the MacWilliams Extension Theorem can be formulated as follows: every finite field alphabet A has an extension property.

Despite the fact that in general an extension property does not always hold, for some alphabets it is still possible to prove an analogue of the extension theorem.

Theorem 2.1.3 (see [67])**.** *Let R be a finite ring with identity. A finite R-module A has an extension property if and only if A is pseudo-injective with a cyclic socle.*

The definition of pseudo-injective modules is given in Section 2.2. For the definition of the socle, recall that a nonzero R-submodule is called *simple* (or irreducible) if it does not contain any submodule other than 0 and itself, see [60, p. 38]. A nonzero R-submodule is called *semisimple* (or completely reducible) if it is a direct sum of simple submodules, see [60, p. 166].

Definition 2.1.3 ([60, p. 174])**.** The *socle* of a finite R-module M, denoted $\mathrm{soc}(M)$, is the sum of all simple submodules of M.

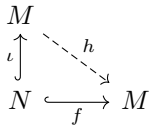
An R-module M is called *cyclic* if there exists $m \in M$ such that $M = Rm$. For elements $m_1, \ldots, m_r$ of an R-module M by $\langle m_1, \ldots, m_r \rangle$ we denote the R-submodule of M generated by $m_1, \ldots, m_r$, i.e., $\langle m_1, \ldots, m_r \rangle = Rm_1 + \cdots + Rm_r$.

Example 2.1.2. Consider the ring $R = \mathbb{Z}$ and let $M = \mathbb{Z}_4 \oplus \mathbb{Z}_2$ be a left R-module. Calculate $\mathrm{soc}(M)$. The R-module M has three simple submodules: $\langle (2,1) \rangle$, $\langle (0,1) \rangle$ and $\langle (2,0) \rangle$. The socle is equal to the sum of all the three simple submodules, $\mathrm{soc}(M) = \langle 2 \rangle \oplus \mathbb{Z}_2 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. The R-module $\mathrm{soc}(M)$ is not cyclic.

2.2 Pseudo-injective modules

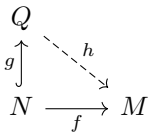
Following the original definition of [54], we give the following definition of pseudo-injectivity.

Definition 2.2.1. An R-module M is called *pseudo-injective*, if for each submodule $N \subseteq M$, each injective homomorphism $f \in \mathrm{Hom}_R(N, M)$ extends to an endomorphism $h \in \mathrm{End}_R(M)$.



There exists a connection between injective and pseudo-injective modules.

Example 2.2.1. Injective modules are pseudo-injective. Following the definition in [43, p. 782], a module M is called *injective*, if for every two R-modules N and Q, for every injective map $g \in \mathrm{Hom}_R(N, Q)$ and every map $f \in \mathrm{Hom}_R(N, M)$, there exists a map $h \in \mathrm{Hom}_R(Q, M)$ such that $hg = f$.



Put $Q = M$, $N \subseteq M$ and define $g = \iota \in \mathrm{Hom}_R(N, M)$ as a canonical embedding of N into M. If M is injective, then for every submodule $N \subseteq M$ and every map $f \in \mathrm{Hom}_R(N, M)$, there exists a map $h \in \mathrm{End}_R(M)$ such that $h\iota = f$, i.e., f extends to h. Hence M is pseudo-injective.

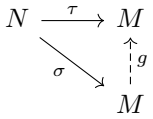
Example 2.2.2. Let $R = \mathbb{Z}$ be the ring of integer numbers. Consider the following $\mathbb{Z}$-module $M = \mathbb{Z}_4 \oplus \mathbb{Z}_2$ and $\mathbb{Z}$-submodule $N = \langle 2 \rangle \oplus \mathbb{Z}_2 \subset M$. The $\mathbb{Z}_2$-linear injective map $f : N \to M$, defined as $f(0,1) = (2,0)$ and $f(2,0) = (0,1)$, does not extend to a $\mathbb{Z}$-linear homomorphism $h : M \to M$. Indeed, defining $h(1,0) = (x,y)$ for some $x \in \mathbb{Z}_4$ and $y \in \mathbb{Z}_2$, $h(2,0) = (2x, 2y) = (2x, 0) \neq f(2,0)$. Therefore M is not pseudo-injective.

In [67], the author proved, based on the original proof for rings in [15] (where ring is considered a module over itself), the following fact.

Proposition 2.2.1 ([67, Proposition 5.1])**.** *A finite R-module M is pseudo-injective if and only if for every submodule $N \subseteq M$ each injective homomorphism $\sigma \in \mathrm{Hom}_R(N, M)$ extends to an automorphism $g \in \mathrm{Aut}_R(M)$.*

We prove the following property of pseudo-injective modules.

Lemma 2.2.1. *Let N be an R-module and let M be a finite pseudo-injective R-module. Let σ, τ be two maps in $\mathrm{Hom}_R(N, M)$. If $\ker \sigma = \ker \tau$, then there exists an automorphism $g \in \mathrm{Aut}_R(M)$ such that $\tau = g\sigma$.*



Proof. Since the kernels are equal, consider two canonical injective homomorphisms $\bar{\sigma}, \bar{\tau} : N/\ker \sigma \to M$. Note that $\mathrm{im}\, \sigma = \mathrm{im}\, \bar{\sigma}$ and $\mathrm{im}\, \sigma \cong N/\ker \sigma$ as R-modules. The map $\bar{\tau}\bar{\sigma}^{-1} : \mathrm{im}\, \sigma \to M$ is an injective homomorphism defined on the submodule $\mathrm{im}\, \sigma \subseteq M$. From pseudo-injectivity of M and Proposition 2.2.1, there exists $g \in \mathrm{Aut}_R(M)$ such that $\bar{\tau}\bar{\sigma}^{-1} = g$ on $\mathrm{im}\, \sigma$. It is easy to check that $\tau = g\sigma$. Indeed, for every $x \in N$, $\tau(x) = \bar{\tau}(\bar{x}) = g\bar{\sigma}(\bar{x}) = g\sigma(x)$, where $\bar{x} = x + \ker \sigma$, $\bar{x} \in N/\ker \sigma$. □

2.3 Extension criterion

Consider the context of a module alphabet. Let R be a ring with identity, let A be a finite R-module alphabet, let $C \subseteq A^n$ be an R-module code and let $f \in \mathrm{Hom}_R(C, A^n)$.

We use the following notations in this and the next three chapters.

Let M be an R-module isomorphic to C, called a *message set*. Let $\lambda \in \mathrm{Hom}_R(M, A^n)$ be *an encoding map of* C, i.e., an injective map such that $\mathrm{im}\,\lambda = C$, in the form

$$\lambda = (\lambda_1, \ldots, \lambda_n),$$

where $\lambda_i \in \mathrm{Hom}_R(M, A)$ is the projection on the ith coordinate, for $i \in \{1, \ldots, n\}$. Consider the following R-modules, for $i \in \{1, \ldots, n\}$,

$$V_i = \ker \lambda_i \subseteq M.$$

Define $\mu = f\lambda \in \mathrm{Hom}_R(M, A^n)$ and denote

$$U_i = \ker \mu_i \subseteq M.$$

Denote the *n-tuples of modules* $\mathcal{V} = (V_1, \ldots, V_n)$ and $\mathcal{U} = (U_1, \ldots, U_n)$.

We say that $\mathcal{V} = \mathcal{U}$ if they represent the same multiset of modules. In other words, $\mathcal{V} = \mathcal{U}$ if and only if there exists $\pi \in \mathfrak{S}_n$ such that for each $i \in \{1, \ldots, n\}$, $U_i = V_{\pi(i)}$.

The following proposition characterizes extendable Hamming isometries in terms of the n-tuples $\mathcal{V}$ and $\mathcal{U}$.

Proposition 2.3.1 (see [19])**.** *The map $f \in \mathrm{Hom}_R(C, A^n)$ is a Hamming isometry if and only if the equality below holds,*

$$\sum_{i=1}^{n} \mathbb{1}_{V_i} = \sum_{i=1}^{n} \mathbb{1}_{U_i}. \tag{2.1}$$

If f extends to a monomial map, then $\mathcal{V} = \mathcal{U}$. If A is pseudo-injective and $\mathcal{V} = \mathcal{U}$, then f extends to a monomial map.

Proof. It is easy to see that the map f is a Hamming isometry if and only if for each $x \in C$, $\mathrm{wt}_H(f(x)) = \mathrm{wt}_H(x)$, or, equivalently, for each $w \in M$, $\mathrm{wt}_H(\lambda(w)) = \mathrm{wt}_H(\mu(w))$. Note that for all $w \in M$,

$$n - \mathrm{wt}_H(\lambda(w)) = \sum_{i=1}^{n} (1 - \mathrm{wt}_H(\lambda_i(w))) = \sum_{i=1}^{n} \mathbb{1}_{\ker \lambda_i}(w),$$

and the same for the map μ. Hence, f is a Hamming isometry if and only if eq. (2.1) holds.

If f extends to a monomial map, then there exist a permutation $\pi \in \mathfrak{S}_n$ and automorphisms $g_i \in \mathrm{Aut}_R(A)$ such that $\lambda_i = g_i \mu_{\pi(i)}$, which implies $\ker \lambda_i = \ker \mu_{\pi(i)}$, for all $i \in \{1, \ldots, n\}$. Hence $\mathcal{V} = \mathcal{U}$.

Let $\mathcal{V} = \mathcal{U}$ and let A be a pseudo-injective module. There exists $\pi \in \mathfrak{S}_n$ such that $\ker \lambda_i = \ker \mu_{\pi(i)}$, for $i \in \{1, \dots, n\}$. From Lemma 2.2.1, there exists an automorphism $g_i \in \mathrm{Aut}_R(A)$ such that $\lambda_i = g_i \mu_{\pi(i)}$. Hence, f extends to a monomial map. □

Calculating the Fourier transform of eq. (2.1), using eq. (1.1), we get the equality of functions defined on the right R-module $\widehat{M}$,

$$\sum_{i=1}^{n} |V_i| \mathbb{1}_{V_i^\perp} = \sum_{i=1}^{n} |U_i| \mathbb{1}_{U_i^\perp}. \tag{2.2}$$

Since the Fourier transform is invertible, eq. (2.1) holds if and only if eq. (2.2) holds.

2.4 General extension theorem

The original proof of the "if part" of Theorem 2.1.3 is mainly character theoretical. In this section we show how to use a geometric approach and the Fourier transform to prove the theorem (the if part) in a different way. Also we show that the condition of the finiteness of the ring can be omitted.

Lemma 2.4.1. *Let n be a positive integer and let $a_1, \dots, a_n$, $b_1, \dots, b_n \in \mathbb{Q}$ be positive numbers. Let $X = (X_1, \dots, X_n)$ and $Y = (Y_1, \dots, Y_n)$ be two n-tuples of cyclic R-submodules of some ambient finite R-module M. Assume that $X_i = X_j$ implies $a_i = a_j$, $Y_i = Y_j$ implies $b_i = b_j$, and $X_i = Y_j$ implies $a_i = b_j$, for $i, j \in \{1, \dots, n\}$. If the equality*

$$\sum_{i=1}^{n} a_i \mathbb{1}_{X_i} = \sum_{j=1}^{n} b_j \mathbb{1}_{Y_j}$$

holds, then $X = Y$.

Proof. Simplify the equality by combining terms with equal modules in the left and right hand sides and eliminating terms with equal modules in different hand sides. After renaming the variables, the resulting equality have the following form,

$$\sum_{i=1}^{n_1} a'_i \mathbb{1}_{X'_i} = \sum_{j=1}^{n_2} b'_j \mathbb{1}_{Y'_j},$$

where $n_1, n_2 \geq 0$, $a'_i, b'_j > 0$, and all the modules $X'_i, Y'_j \subseteq M$, for $i \in \{1, \dots, n_1\}$ and $j \in \{1, \dots, n_2\}$, are distinct.

Assume that $n_1 > 0$ or $n_2 > 0$. Among the modules $X'_1, \dots, X'_{n_1}, Y'_1, \dots, Y'_{n_2}$ choose one that is maximal with respect to the inclusion, suppose it is X'_1. Then $X'_1 = \bigcup_{j=1}^{n_2} (X'_1 \cap Y'_j)$, where $\{0\} \subseteq X'_1 \cap Y'_j \subseteq X'_1$, $j \in \{1, \dots, n_2\}$. Since X'_1 is cyclic with a generator $x \in X'_1$, there exists $j \in \{1, \dots, n_2\}$ such that $x \in X'_1 \cap Y'_j$, which implies $X'_1 = Y'_j$. By contradiction, $n_1 = n_2 = 0$.

Hence, for every submodule $Z \subseteq M$, considering the assumption of the lemma on equal coefficients, the submodule Z appears in the n-tuples X and Y the same number of times, and thus $X = Y$. □

Let N and M be two finite R-modules. For a map $\sigma \in \mathrm{Hom}_R(M, N)$ define a map

$$\widehat{\sigma} : \widehat{N} \to \widehat{M}, \quad \chi \mapsto \chi\sigma.$$

Note that $\widehat{\sigma} \in \mathrm{Hom}_R(\widehat{N}, \widehat{M})$. The following fact appears in [64, Sections 2-3] and is related to Morita's theory of duality for modules (see [1, Chapter 6]).

Proposition 2.4.1. *Let R be a finite ring. The functor $\wedge$ on the category of finite R-modules is exact contravariant.*

Exact means that $\wedge$ preserves exact sequences, and *contravariant* means that it reverses the direction of arrows.

Proposition 2.4.2 ([67, Proposition 5.3])**.** *Let R be a finite ring with identity and let A be a finite R-module. The socle* $\mathrm{soc}(A)$ *is cyclic if and only if there exists an injective homomorphism of left R-modules $\iota : A \to \widehat{R}$.*

Note that for a finite ring R, both R and $\widehat{R}$ are R-bi-modules over itself.
Prove that for all $\sigma \in \mathrm{Hom}_R(M, N)$,

$$(\ker \sigma)^{\perp} = \mathrm{im}\, \widehat{\sigma}. \tag{2.3}$$

Indeed, consider the isomorphism of groups $\psi : N \to \widehat{\widehat{N}}$, defined as $\psi(x)(\chi) = \chi(x)$ for all $\chi \in \widehat{N}$, $x \in N$. Assume that for all $\chi \in \widehat{N}$, $\chi(x) = 1$ for some x. Then $\psi(x)(\chi) = 1$ for all $\chi \in \widehat{N}$ that means $\psi(x)$ is a trivial character in $\widehat{\widehat{N}}$. Therefore $x = \psi^{-1}(\psi(x)) = 0$. Calculate, $\ker \sigma = \{m \in M \mid \sigma(m) = 0\} = \{m \in M \mid \forall \chi \in \widehat{N}, \chi(\sigma(m)) = 1\} = (\mathrm{im}\, \widehat{\sigma})^{\perp}$. Hence, $(\ker \sigma)^{\perp} = (\mathrm{im}\, \widehat{\sigma})^{\perp\perp} = \mathrm{im}\, \widehat{\sigma}$.

Proof of Theorem 2.1.3, the if part. Let A be a finite pseudo-injective left R-module with a cyclic socle. From Proposition 2.4.2, there exists an injective homomorphism of left R-modules $\phi : A \to \widehat{R}$. From Proposition 2.4.1, the last is equivalent to the fact that the map $\widehat{\phi} : R \to \widehat{A}$ is a surjective homomorphism of right R-modules, i.e., $\widehat{A}$ is a cyclic right R-module.

Let $C \subset A^n$ be a code and let $f \in \mathrm{Hom}_R(C, A^n)$ be a Hamming isometry. Recall the notations of Section 2.3. Since $\widehat{A}$ is a cyclic right R-module, for all $i \in \{1, \ldots, n\}$ the right R-modules $V_i^{\perp} = \mathrm{im}\, \widehat{\lambda}_i$ and $U_i^{\perp} = \mathrm{im}\, \widehat{\mu}_i$ are cyclic. Applying Lemma 2.4.1 to eq. (2.2), there exists a permutation $\pi \in \mathfrak{S}_n$ such that $V_i^{\perp} = U_{\pi(i)}^{\perp}$, for all $i \in \{1, \ldots, n\}$. Equivalently, $\mathcal{V} = \mathcal{U}$. By Proposition 2.3.1, f extends to a monomial map. □

The proof of the only if part remains the same as in [67]. However, we can improve the statement of Theorem 2.1.3 by omitting the finiteness assumption on the ring R.

Let R be a ring with identity (not necessary finite). Let M be a finite R-module. The *annihilator* $\operatorname{ann}(M) = \{r \in R \mid rM = 0\}$ of M is a two-sided ideal in R. Denote the quotient ring $R_M = R/\operatorname{ann}(M)$.

Consider the canonical projection $R \to R_M$, $r \mapsto \bar{r}$, where $\bar{r}$ is the class of r in R_M. Any R-module $N \subseteq M$ can be seen as an R_M-module with the well-defined action $\bar{r}a = ra$, for $r \in R, a \in N$. Conversely, any R_M-module $N \subseteq M$ is an R-module, where the action is defined as $ra = \bar{r}a$ for all $r \in R$, $a \in N$.

For any positive integer n, it is easy to see that $\operatorname{ann}(M^n) = \operatorname{ann}(M)$, and hence, $R_M = R_{M^n}$. From the arguments above, any R-submodule $N \subseteq M^n$ is an R_M-module and vice versa. For any two R-modules $A, B \subseteq M$ ($A, B \subseteq M^n$), $\operatorname{Hom}_R(A, B) = \operatorname{Hom}_{R_M}(A, B)$.

Lemma 2.4.2. *The ring $R_M = R/\operatorname{ann}(M)$ is finite.*

Proof. For any element $\bar{r} \in R_M$, the map $h_{\bar{r}} : M \to M$, $a \mapsto \bar{r}a$ is an element of the ring of endomorphisms $\operatorname{End}_{\mathbb{Z}}(M)$. Prove that the map $R_M \to \operatorname{End}_{\mathbb{Z}}(M)$, $\bar{r} \mapsto h_{\bar{r}}$ is an injection. Assume that for some elements $\bar{r}_1, \bar{r}_2 \in R_M$, $h_{\bar{r}_1} = h_{\bar{r}_2}$, or equivalently, $\bar{r}_1 m = \bar{r}_2 m$, for all $m \in M$. Hence $\bar{r}_1 = \bar{r}_2$. Since R_M can be embedded into a finite set $\operatorname{End}_{\mathbb{Z}}(M)$, it is finite itself. □

Theorem 2.4.1 (see [19])**.** *Let R be a ring with identity, not necessary finite. A finite R-module A has an extension property if and only if A is a pseudo-injective R-module with a cyclic socle.*

Proof. By definition, an R-module A has an extension property if for every positive integer n, for every R-linear code $C \subseteq A^n$, each R-linear Hamming isometry $f \in \operatorname{Hom}_R(C, A^n)$ extends to an R-linear monomial map. Hence, the R-module A has an extension property if and only if the R_A-module A has an extension property, where $R_A = R/\operatorname{ann}(A)$.

In the same way, A is pseudo-injective as an R-module if and only if it is pseudo-injective R_A-module. The socle $\operatorname{soc}(A)$ is the same for the module A considered both as an R-module and as an R_A-module. It is cyclic as an R-module if and only if it is cyclic as an R_A-module.

From Lemma 2.4.2, the ring R_A is finite and thus from Theorem 2.1.3 and the arguments above, we have the statement of the theorem. □

Consider the context of linear codes over a vector space alphabet, see also Section 1.5. Since it is a particular example of linear codes over module alphabet, we placed below several valuable examples to help the reader to get familiar with the notions and objects defined in Section 2.3.

Let $\mathbb{F}_q$ be a finite field and let the alphabet A be a vector space over $\mathbb{F}_q$ of dimension ℓ. Consider a structure of a finite field $\mathbb{F}_{q^\ell}$ on A (see Remark 1.5.1).

Example 2.4.1. Let $q = 2$ and let $A = \mathbb{F}_4$. Let $M = \mathbb{F}_2^3$ and let $\lambda \in \mathrm{Hom}_{\mathbb{F}_2}(M, A^n)$ be defined as $\lambda(w) = wG$, for $w \in M$, where

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

Consider the 3-tuple of vector spaces $\mathcal{V} = (V_1, V_2, V_3)$ that corresponds to the map λ. The spaces are: $V_1 = \ker \lambda_1 = \langle (1,0,1) \rangle_{\mathbb{F}_2}$, $V_2 = \ker \lambda_2 = \langle (0,0,1) \rangle_{\mathbb{F}_2}$ and $V_3 = \ker \lambda_3 = \langle (1,0,0), (0,1,0) \rangle_{\mathbb{F}_2}$.

For vector space alphabets the last part of the statement of Proposition 2.3.1 can be refined.

Proposition 2.4.3 (see [24])**.** *Let $C \subseteq A^n$ be an $\mathbb{F}_q$-linear code and let $f : C \to A^n$ be an $\mathbb{F}_q$-linear map. The map f is a Hamming isometry if and only if the following equality holds,*

$$\sum_{i=1}^{n} \mathbb{1}_{V_i} = \sum_{i=1}^{n} \mathbb{1}_{U_i}. \qquad \text{(2.1 revisited)}$$

The map f is extendable if and only if $\mathcal{V} = \mathcal{U}$.

Proof. The proof follows directly from Proposition 2.3.1 and the fact that the vector space A, as a module over a finite field, is injective and hence pseudo-injective, see Example 2.2.1. □

To illustrate Proposition 2.4.3 we consider the following example.

Example 2.4.2. We continue Example 2.4.1. Define an $\mathbb{F}_2$-linear map $f : C \to \mathbb{F}_4^3$ on the generators in the following way: $f\big((1,1,0)\big) = (1,1,0)$, $f\big((\omega,\omega,0)\big) = (1,0,1)$ and $f\big((1,0,1)\big) = (\omega,\omega,0)$. Consider the following matrices G and G',

$$G = \begin{pmatrix} 1 & 1 & 0 \\ \omega & \omega & 0 \\ 1 & 0 & 1 \end{pmatrix} \xrightarrow{f} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ \omega & \omega & 0 \end{pmatrix} = G' .$$

The map $\mu = f\lambda$ can be presented as $\mu(w) = wG'$, $w \in M$. Calculate the 3-tuple of spaces $\mathcal{U} = (U_1, U_2, U_3)$. The spaces are: $U_1 = \langle (1,1,0) \rangle_{\mathbb{F}_2}$, $U_2 = \langle (0,1,0) \rangle_{\mathbb{F}_2}$, $U_3 = \langle (1,0,0), (0,0,1) \rangle_{\mathbb{F}_2}$. One can verify that the spaces V_1, V_2, V_3 and U_1, U_2, U_3 satisfy eq. (2.1). By Proposition 2.4.3, the map $f : C \to \mathbb{F}_4^3$ is an $\mathbb{F}_2$-linear Hamming isometry. Since $(V_1, V_2, V_3) \neq (U_1, U_2, U_3)$, the map f is unextendable.

The developed geometric representation can be used to prove the original extension theorem of MacWilliams even without the Fourier transform, which we used in the proof of Theorem 2.1.3. This proof also appears in [24].

Proof of the classical MacWilliams Extension Theorem 2.1.1. For classical $\mathbb{F}_q$-linear codes $\dim_{\mathbb{F}_q} A = 1$. Due to Proposition 2.4.3 it is enough to show that if the pair $(\mathcal{U}, \mathcal{V})$ satisfies eq. (2.1), then $\mathcal{U} = \mathcal{V}$. For all $i \in \{1, \dots, n\}$, $\dim_{\mathbb{F}_q} V_i = \dim_{\mathbb{F}_q} \ker \lambda_i \geq \dim_{\mathbb{F}_q} M - \dim_{\mathbb{F}_q} A = \dim_{\mathbb{F}_q} M - 1$. In the same way, $\dim_{\mathbb{F}_q} U_i \geq \dim_{\mathbb{F}_q} M - 1$. Therefore the spaces in $\mathcal{U}$ and $\mathcal{V}$ are either hyperplanes of M or the space M itself.

In eq. (2.1) eliminate equal terms from different sides. Then, group equal terms on each side and make a renumbering of the spaces on both sides of the equation. We did the same operations in the proof of Lemma 2.4.1. After this procedure we get the reduced equality,

$$\sum_{i=1}^{r} a_i \mathbb{1}_{U_i'} = \sum_{j=1}^{s} b_j \mathbb{1}_{V_j'},$$

where $U_i', V_j' \subseteq M$ are $\mathbb{F}_q$-linear spaces, $a_i, b_j > 0$, and the spaces U_i', V_j' are all different, for $i \in \{1, \dots, r\}$, $j \in \{1, \dots, s\}$. Note that $r, s \leq n$, and if $\mathcal{U} \neq \mathcal{V}$, then $r, s > 0$. Evaluated in $\{0\}$ the reduced equality gives the following, $\sum_{i=1}^{r} a_i = \sum_{j=1}^{s} b_j$.

Consider the reduced equality and assume that $\mathcal{U} \neq \mathcal{V}$. Without loss of generality, assume that U_1' is maximal with respect to inclusion among all the spaces that appear in the reduced equality. Calculate the restriction of the equality on the space U_1',

$$a_1 \mathbb{1}_{U_1'} + \sum_{i=2}^{r} a_i \mathbb{1}_{U_i' \cap U_1'} = \sum_{j=1}^{s} b_j \mathbb{1}_{V_j' \cap U_1'} \, .$$

Now calculate the sum over all the points in M of the left and the right side. Denote $k = \dim_{\mathbb{F}_q} U_1'$. Since U_1 is either M or a hyperplane of M we directly calculate the size of all the intersections,

$$a_1 q^k + \sum_{i=2}^{r} a_i q^{k-1} = \sum_{j=1}^{s} b_j q^{k-1} \, .$$

Note that in both cases the formula is the same. Thus, using the equality $\sum_{i=1}^{r} a_i = \sum_{j=1}^{s} b_j$, we get $a_1(q-1) = 0$, which is impossible. Therefore $\mathcal{U} = \mathcal{V}$. □

Remark 2.4.1. The MacWilliams Extension Theorem describes the linear isometries of classical linear codes but does not apply to additive isometries of classical linear codes. In other words, the classical linear code over a finite field $\mathbb{F}_{q^\ell}$ can be considered as an additive code over a finite field $\mathbb{F}_q$, where $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^\ell}$. We observe extension properties of such codes in Section 4.2.2.

2.5 Module alphabets over PIDs

A nonzero commutative ring in which a product of every two nonzero elements is nonzero is called an *integral domain* (or entire ring). A commutative ring R

is called a *principal ideal* ring if every ideal $I \subseteq R$ is of the form Rx for some $x \in R$. Combining these two definition, a ring R is called a PID (*principal integral domain*) if it is an integral domain and a principal ideal ring.

Examples of PIDs include fields, the ring of integers $\mathbb{Z}$ and the ring of polynomials in one variable with coefficients in a field. The ring of polynomials with integer coefficients or the ring of multi-variable polynomials with coefficients in a field are not PIDs.

Let R be a PID. To prove the extension theorem for R-module alphabets we need the following two lemmas.

Lemma 2.5.1. *A finite R-module M is cyclic if and only if* $\mathrm{soc}(M)$ *is cyclic.*

Proof. Since R is PID, if M is cyclic, then $\mathrm{soc}(M) \subseteq M$ is cyclic, so prove the converse. Let M be a finite R-module with a cyclic socle. For a prime $p \in R$, let $M(p)$ denote the set of those elements x in M such that there exists a positive integer t with $p^t x = 0$.

The R-module M is isomorphic to the sum $\bigoplus_p M(p)$ over all primes $p \in R$ with $M(p) \neq 0$ (see [43, p. 149]). From [60, p. 175], the socle of a direct sum of modules equals to the direct sum of socles of summands,

$$\mathrm{soc}(M) \cong \bigoplus_p \mathrm{soc}(M(p)).$$

Thus, $\mathrm{soc}(M)$ is cyclic if and only if each summand $\mathrm{soc}(M(p))$ is cyclic.

For a prime $p \in R$, the R-module $M(p)$ is isomorphic to a product of cyclic R-modules $R/(p^{t_1}) \oplus \cdots \oplus R/(p^{t_r})$, where $t_1, \ldots, t_r$ are positive integers, (see [43, p. 149]). Note that $\mathrm{soc}(R/(p^{t_i})) \cong R/(p)$, for $i \in \{1, \ldots, r\}$. Calculate the socle,

$$\mathrm{soc}(M(p)) \cong \underbrace{R/(p) \oplus \cdots \oplus R/(p)}_{r},$$

that is cyclic if and only if $r = 1$, i.e., $M(p) \cong R/(p^t)$ for some integer t. Therefore M is cyclic. □

Lemma 2.5.2. *A finite cyclic R-module M is pseudo-injective.*

Proof. Prove the statement for the R-module $M = R/(p^t)$. Let N be a submodule of M and let $f : N \to M$ be an injective R-linear homomorphism. All the divisors of p^t are of the form p^v for some integer $v < t$. There exists a correspondence between the submodules of M and divisors of p^t and therefore, there exists an integer $v < t$ such that $N \cong R/(p^v)$. Consider the canonical embedding $R/(p^v) \to M$, $1 + (p^v) \mapsto p^{t-v} + (p^t)$. Let $x \in R$ be such that $f(p^{t-v} + (p^t)) = x + (p^t)$. Since f is an injective R-linear homomorphism, there exists $y \in R$ coprime with p such that $x = yp^{t-v}$. The map $h : M \to M$, defined by $h(1+(p^t)) = y+(p^t)$ is then an endomorphism (moreover, an automorphism) of M and f extends to h.

Now, let M be arbitrary cyclic R-module. Then $M \cong R/(p_1^{t_1}) \oplus \cdots \oplus R/(p_r^{t_r})$, where $p_i \in R$ are different primes and t_i are positive integers. Let N be a

submodule of M. The R-module N is isomorphic to $R/(p_1^{s_1}) \oplus \cdots \oplus R/(p_r^{s_r})$, where $s_i \leq t_i$ for $i \in \{1, \ldots, r\}$. Let $f : N \to M$ be an injective homomorphism. The map f splits into the product of injective homomorphisms $f = f_1 \times \cdots \times f_r$, where $f_i : R/(p_i^{s_i}) \to R/(p_i^{t_i})$, $i \in \{1, \ldots, r\}$. We have already showed that each f_i extends to an automorphism h_i of $R/(p_i^{t_i})$, $i \in \{1, \ldots, r\}$, and therefore f extends to a map $h_1 \times \cdots \times h_r$, which is an automorphism of M. □

The following theorem for the case $R = \mathbb{Z}$ was proved in [19].

Theorem 2.5.1. *Let R be a PID. A finite R-module alphabet A has an extension property if and only if A is cyclic.*

Proof. From Lemma 2.5.1 and Lemma 2.5.2 the conditions of Theorem 2.4.1 are satisfied and thus the statement holds. □

3. SHORT CODES

In [16] Dinh and López-Permouth partially translated the extension problem for a module alphabet to the case of matrix rings and matrix modules. They proved the necessary conditions for the existence of a code over a matrix module alphabet with an unextendable Hamming isometry. An explicit construction appeared later in the proof of the following theorem. For a positive integer x define the integer N_x,

$$N_x = \prod_{i=1}^{x}(1+q^i).$$

Theorem 3.0.1 (see [67]). *Let $R = \mathrm{M}_{k\times k}(\mathbb{F}_q)$ and let $A = \mathrm{M}_{k\times \ell}(\mathbb{F}_q)$ be the left R-module.*
If $\ell \leq k$, then the alphabet A has an extension property.
If $\ell > k$, then there exist a linear code $C \subset A^n$ of the length $n = N_{\ell-1}$, and a map $f \in \mathrm{Hom}_R(C, A^n)$ that is a Hamming isometry, but there is no monomial map extending f.

Note that Theorem 3.0.1 does not claim if the code has the minimum possible length. We improve the result above by giving the exact bound for all k. That is, in the context of matrix modules, we found the minimum code length for which a code with an unextendable Hamming isometry exists.

Theorem 3.0.2 (see [19]). *Let $R = \mathrm{M}_{k\times k}(\mathbb{F}_q)$ and let $A = \mathrm{M}_{k\times \ell}(\mathbb{F}_q)$ be the left R-module. Let $n < N_k$ be a positive integer and let $C \subseteq A^n$ be an R-linear code. Each Hamming isometry $f \in \mathrm{Hom}_R(C, A^n)$ extends to a monomial map.*

If $\ell > k$ and $n \geq N_k$, then there exists a linear code $C \subset A^n$, and a map $f \in \mathrm{Hom}_R(C, A^n)$ that is a Hamming isometry, but there is no monomial map extending f.

Note that the code length $N_{\ell-1}$ in Theorem 3.0.1 depends on the dimension of the alphabet, whereas in Theorem 3.0.2 the code length N_k depends on the dimension of the ring, considered as a module over itself. If $\ell > k$, then $N_{\ell-1} \geq N_k$.

3.1 Matrix modules

Consider the matrix ring $R = \mathrm{M}_{k\times k}(\mathbb{F}_q)$ of $k \times k$ matrices over the finite field $\mathbb{F}_q$, where k is a positive integer and q is a prime power. The ring R is simple, i.e., it is a non-zero ring that has no two-sided ideals besides the zero ideal and

itself. Each simple R-module is isomorphic to the R-module $T = M_{k\times 1}(\mathbb{F}_q)$ (see [43, Theorem 5.5]). Each *matrix module* M is isomorphic to $\mathrm{M}_{k\times m}(\mathbb{F}_q)$ for some nonnegative integer m. In such a way,

$$M \cong mT = \underbrace{T \oplus T \oplus \cdots \oplus T}_{m}.$$

Call m the *dimension* of M and denote $\dim M = m$. For an m-dimensional R-module M,

$$|M| = q^{km}.$$

Remark 3.1.1. Recall the definition of a poset (partially ordered set, see Definition 5.4.1). Consider the poset of all submodules of M with the partial order "$\subseteq$". In [70, Lemma 6.2] the author proved that there exists an isomorphism between the poset of subspaces of an m-dimensional vector spaces and the poset of submodules of an m-dimensional matrix module. For example, one such poset isomorphism can be obtained by identifying an R-module $N \subseteq M$ with the sum of row spaces of all matrices in N.

In such a way the defined poset isomorphism maps t-dimensional submodules of M to t-dimensional subspaces of an m-dimensional vector space. When $k = 1$, $R = \mathrm{M}_{1\times 1}(\mathbb{F}_q) = \mathbb{F}_q$ and R-modules are vector spaces, so the defined dimension of an R-module and the dimension of a vector space are identical.

Recall the definition of a *q-ary Gaussian binomial coefficient*, for nonnegative integers $u \le v$,

$$\begin{bmatrix} v \\ u \end{bmatrix}_q = \prod_{i=0}^{u-1} \frac{q^{v-i}-1}{q^{u-i}-1}.$$

Lemma 3.1.1. *Let V be a v-dimension submodule of an m-dimensional matrix module M. Then,*

$$|\{U \subseteq M \mid U \cap V = \{0\},\ \dim U = u\}| = q^{vu} \begin{bmatrix} m-v \\ u \end{bmatrix}_q.$$

In particular,

$$|\{U \subseteq M \mid \dim U = u\}| = \begin{bmatrix} m \\ u \end{bmatrix}_q.$$

Proof. See [11, Lemma 9.3.2] and [70, Lemma 6.2]. □

3.2 Codes over a matrix module alphabet

Lemma 3.2.1. *For any positive integer t the following equalities hold,*

$$\sum_{i=0}^{t-1} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} t \\ i \end{bmatrix}_q = (-1)^{t-1} q^{\binom{t}{2}},$$

$$\sum_{i=0}^{t} q^{\binom{i}{2}} \begin{bmatrix} t \\ i \end{bmatrix}_q = \prod_{i=0}^{t-1} (1+q^i).$$

Proof. Use the q-binomial theorem, see [56, p. 74],

$$\sum_{i=0}^{t} q^{\binom{i}{2}} \begin{bmatrix} t \\ i \end{bmatrix}_q x^i = \prod_{i=0}^{t-1} (1 + xq^i).$$

To get the equalities in the statement, put $x = -1$ and $x = 1$. □

Let $R = \mathrm{M}_{k\times k}(\mathbb{F}_q)$ and let M be a left m-dimensional R-module. For a positive integer n, consider the equation

$$\sum_{i=1}^{n} \mathbb{1}_{X_i} = \sum_{i=1}^{n} \mathbb{1}_{Y_i}, \tag{3.1}$$

where the unknowns are n-tuples $X = (X_1, \ldots, X_n)$, $Y = (Y_1, \ldots, Y_n)$ of submodules of M. Recall that $X = Y$ if there exists a permutation $\pi \in \mathfrak{S}_n$ such that $X_i = Y_{\pi(i)}$ for all $i \in \{1, \ldots, n\}$. We prove the following.

Lemma 3.2.2. *If a pair of n-tuples (X, Y) satisfies eq. (3.1) and $X \neq Y$, then $n \geq N_k$.*

Proof. To prove the statement of the lemma we consider a pair of n-tuples (X, Y) that have the smallest length and the smallest maximum dimension of submodules among all the pairs that satisfy eq. (3.1) and $X \neq Y$. Then, we show that the considered pair is of a particular form. After this we can find precisely the smallest value of n. The details are given below.

Let n^* be the smallest positive integer such that there exists a solution of eq. (3.1) with $X \neq Y$. For a pair of n^*-tuples (X, Y) define

$$r(X, Y) = \max\{\dim X_i,\ \dim Y_i \mid i \in \{1, \ldots, n^*\}\}.$$

Let r^* be the minimum value of $r(X, Y)$ over all the pairs of n^*-tuples (X, Y) that satisfy eq. (3.1) and $X \neq Y$. Let (X', Y') be one such pair of n^*-tuples with $r(X', Y') = r^*$ and $\dim X'_1 = r^*$.

Consider the pair of n^*-tuples (X^*, Y^*), which equals to the pair (X', Y') restricted on the submodule X'_1, i.e., $X^*_i = X'_i \cap X'_1$ and $Y^*_i = Y'_i \cap X'_1$, for $i \in \{1, \ldots, n^*\}$. One can verify that (X^*, Y^*) is a solution of eq. (3.1). Moreover, $X^* \neq Y^*$. Indeed, if $X^* = Y^*$, then there exists $j \in \{1, \ldots, n^*\}$ such that $X'_1 = Y'_j$, which implies $X' = Y'$, because otherwise the reduced pair $(X' \setminus X'_1, Y' \setminus Y'_j)$ is a solution of eq. (3.1) of the length $n < n^*$ and $X' \setminus X'_1 \neq Y' \setminus Y'_j$. Since n^* is the minimum, from the contradiction, $X^* \neq Y^*$. Also, $r(X^*, Y^*) = r^*$ and for all $i \in \{1, \ldots, n^*\}$, $X^*_i, Y^*_i \subseteq X^*_1$.

Now we are going to find explicitly the pair (X^*, Y^*). Introduce some additional notations. Denote $I_j = \{i \mid \dim X^*_i < r^* - j\}$, $J_j = \{i \mid \dim Y^*_i < r^* - j\}$ and

$$\Sigma_j = \sum_{\dim V = r^* - j} \mathbb{1}_V,$$

for $j \in \{0, \ldots, r^*\}$, where the summation is over all the submodules V of X^*_1 of the given dimension.

Prove by induction that for all t, $0 \leq t \leq r^*$, eq. (3.1) with $X = X^*$ and $Y = Y^*$ can be transformed to

$$a\sum_{i=0}^{t}(-1)^i q^{\binom{i}{2}}\Sigma_i = \sum_{i\in J_t}\mathbb{1}_{Y_i^*} - \sum_{i\in I_t}\mathbb{1}_{X_i^*}, \tag{3.2}$$

for some positive integer a, by changing the order of terms and substituting the values, which is found on previous steps of the induction.

Prove the base step, $t = 0$. Calculate the restriction of eq. (3.1) on the module X_1^* and put all the terms $\mathbb{1}_{X_1^*} = \Sigma_0$ to the left hand side of the equality and all other terms to the right hand side. We get,

$$a\Sigma_0 = \sum_{i\in J_0}\mathbb{1}_{Y_i^*} - \sum_{i\in I_0}\mathbb{1}_{X_i^*},$$

where $a = |\{i \mid X_i^* = X_1^*\}|$, which is exactly eq. (3.2) for $t = 0$.

Assume that eq. (3.2) holds for some $t \in \{0, \ldots, r^* - 1\}$. Let $Z \subset X_1^*$ be a submodule of dimension $r^* - t - 1$. Restrict eq. (3.2) on Z,

$$a\sum_{i=0}^{t}(-1)^i q^{\binom{i}{2}} \sum_{\dim V = r^*-i}\mathbb{1}_{V\cap Z} = \sum_{i\in J_t}\mathbb{1}_{Y_i^*\cap Z} - \sum_{i\in I_t}\mathbb{1}_{X_i^*\cap Z}. \tag{3.3}$$

The dimension of Z is the largest among all the submodules that appear in eq. (3.3) and it is smaller than r^*. For the pair of n^*-tuples $X \cap Z = (X_1^* \cap Z, \ldots, X_{n^*}^* \cap Z)$ and $Y \cap Z = (Y_1^* \cap Z, \ldots, Y_{n^*}^* \cap Z)$, $r(X \cap Z, Y \cap Z) < r^*$. Also, $(X \cap Z, Y \cap Z)$ satisfies eq. (3.1), and therefore $X \cap Z = Y \cap Z$.

Denote $b = |\{i \in J_t \mid Z = Y_i^*\}|$ and $c = |\{i \in I_t \mid Z = X_i^*\}|$. Prove that either $b = 0$ or $c = 0$. Assume the opposite. Then there exist $i, j \in \{1, \ldots, n^*\}$ such that $Y_i^* = X_j^*$. The $n^* - 1$-tuples $X^* \setminus X_j^*$ and $Y^* \setminus Y_i^*$ form a solution of eq. (3.1) such that $X^* \setminus X_j^* \neq Y^* \setminus Y_i^*$. But then the length of the pairs is $n^* - 1 < n^*$. By contradiction, $b = 0$ or $c = 0$.

Calculate the number of $\mathbb{1}_Z$ terms from the left and from the right hand sides of eq. (3.3). Since $X \cap Z = Y \cap Z$, the numbers are equal. From Lemma 3.1.1 there are $\begin{bmatrix} t+1 \\ i \end{bmatrix}_q$ submodules of dimension $r^* - i$ of X_1^* that contain the module Z of dimension $r^* - t - 1$. Using Lemma 3.2.1,

$$a\sum_{i=0}^{t}(-1)^i q^{\binom{i}{2}} \begin{bmatrix} t+1 \\ i \end{bmatrix}_q = a(-1)^t q^{\binom{t+1}{2}} = b - c,$$

and therefore $c = 0$ if t is even and $b = 0$ if t is odd.

All the submodules of X_1^* of dimension $r^* - t - 1$ are present in the right hand side of eq. (3.2) with positive or negative sign, depending on the parity of t, with the same multiplicity. Move all the terms that correspond to submodules of dimension $r^* - t - 1$ from the right hand side to the left hand side of eq. (3.2). Now, it has the form of eq. (3.2) calculated for $t + 1$,

$$a\sum_{i=0}^{t+1}(-1)^i q^{\binom{i}{2}}\Sigma_i = \sum_{i\in J_{t+1}}\mathbb{1}_{Y_i^*} - \sum_{i\in I_{t+1}}\mathbb{1}_{X_i^*}.$$

By induction, for $t = r^*$, we get, that eq. (3.1) *is equivalent to the following equality,*

$$a\sum_{i=0}^{r^*}(-1)^i q^{\binom{i}{2}}\Sigma_i = \sum_{i\in J_{r^*}=\emptyset}\mathbb{1}_{Y_i^*} - \sum_{i\in I_{r^*}=\emptyset}\mathbb{1}_{X_i^*} \equiv 0.$$

After moving all the summands with negative coefficients to the right hand side, we get the equality in the form of eq. (3.1). Note that $|\Sigma_i| = \begin{bmatrix} r^* \\ r^*-i \end{bmatrix}_q = \begin{bmatrix} r^* \\ i \end{bmatrix}_q$. Calculate,

$$n^* = a\sum_{\substack{0\le i\le r^* \\ i \text{ even}}} q^{\binom{i}{2}}\begin{bmatrix} r^* \\ i \end{bmatrix}_q = a\sum_{\substack{0\le i\le r^* \\ i \text{ odd}}} q^{\binom{i}{2}}\begin{bmatrix} r^* \\ i \end{bmatrix}_q = \frac{1}{2}a\sum_{i=0}^{r^*} q^{\binom{i}{2}}\begin{bmatrix} r^* \\ i \end{bmatrix}_q.$$

If we assume $r^* \le k$, then all the submodules are cyclic and $X^* = Y^*$, see Lemma 2.4.1 applied to eq. (3.1) with $X = X^*$ and $Y = Y^*$. Hence, $r^* = k+1$. Also, $a = 1$, and from Lemma 3.2.1,

$$n^* = \frac{1}{2}\sum_{i=0}^{k+1} q^{\binom{i}{2}}\begin{bmatrix} k+1 \\ i \end{bmatrix}_q = \frac{1}{2}\prod_{i=0}^{k}(1+q^i) = \prod_{i=1}^{k}(1+q^i) = N_k.$$

Hence, $n \ge n^* = N_k$. □

Remark 3.2.1. A similar bound to those proved in Lemma 3.2.2 is observed in [12] by Cho for the minimum size of a support of a nonzero null t-design for vector spaces (see the definition in [12]). Though the problems are somewhat different, we believe that the proof of Lemma 3.2.2 can be simplified using the results of Cho.

The proof of the main result of this chapter follows.

Proof of Theorem 3.0.2. Let $C \subseteq A^n$ be an R-linear code with an unextendable Hamming isometry. According to the main result of [51], every module over a finite simple ring is injective. Since the matrix ring R is simple, the R-module A is injective and thus A is pseudo-injective (see Example 2.2.1). By Proposition 2.3.1, for the n-tuples $\mathcal{U}$ and $\mathcal{V}$, eq. (2.1) holds and $\mathcal{U} \ne \mathcal{V}$. From Lemma 3.2.2, $n \ge N_k$.

Prove the second part of the statement. Let C be the code over the alphabet $B = \mathrm{M}_{k\times(k+1)}(\mathbb{F}_q)$ and let $f \in \mathrm{Hom}_R(C, B^{N_k})$ be the unextendable Hamming isometry that are constructed in the original proof of Theorem 3.0.1 in [61]. The mentioned code C has an all-zero coordinate and $f(C)$ does not. Note that the length of C is exactly N_k. Since $\ell > k$, in A there exists a submodule isomorphic to B, so C can be considered as a code in A^{N_k} and $f \in \mathrm{Hom}_R(C, A^{N_k})$. Since C and $f(C)$ have different number of all-zero coordinates, the map f is an unextendable Hamming isometry. □

Let us observe the case of a vector space alphabet.

Example 3.2.1. Let $n = q + 1$. Let the alphabet $A = \mathbb{F}_{q^\ell}$ be a field extension of $\mathbb{F}_q$ of degree $\ell > 1$ (see Remark 1.5.1). Label all the elements in $\mathbb{F}_q$, $x_1, x_2, \ldots, x_q \in \mathbb{F}_q$. Let $\omega \in \mathbb{F}_{q^\ell} \setminus \mathbb{F}_q$. Consider the $\mathbb{F}_q$-linear codes $C_1 = \langle v_1, v_2 \rangle_{\mathbb{F}_q}$ and $C_2 = \langle u_1, u_2 \rangle_{\mathbb{F}_q}$ in $\mathbb{F}_{q^\ell}^n$ with

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & \ldots & 1 & 0 \\ x_1 & x_2 & \ldots & x_q & 1 \end{pmatrix} \xrightarrow{f} \begin{pmatrix} 1 & 1 & \ldots & 1 & 0 \\ \omega & \omega & \ldots & \omega & 0 \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}.$$

The $\mathbb{F}_q$-linear map $f : C_1 \to C_2$, defined by $f(v_1) = u_1$ and $f(v_2) = u_2$, is a Hamming isometry. Indeed, let $\alpha v_1 + \beta v_2$ be an arbitrary element in $C_1 \setminus \{0\}$, where $\alpha, \beta \in \mathbb{F}_q$. If $\beta = 0$, then $\mathrm{wt}(\alpha v_1 + \beta v_2) = n - 1$. If $\beta \neq 0$ then the equation $\alpha + \beta x_i = 0$, where $i \in \{1, \ldots, q\}$, has exactly one solution $x_i = -\alpha\beta^{-1} \in \mathbb{F}_q$ and thus $\mathrm{wt}(\alpha v_1 + \beta v_2) = n - 1$. Therefore, all nonzero elements in C_1 have the weight equal to $n-1$. It is easy to see that all nonzero codewords in C_2 also have the weight $n - 1$. The map f maps nonzero elements of C_1 to nonzero elements of C_2 and hence is an isometry. At the same time, there is no monomial map that acts on C_1 in the same way as f. The last coordinates of all vectors in C_2 are always zero, but there is no such all-zero coordinate in C_1.

This example provides a counterpoint to the examples of unextendable Hamming isometries for linear codes over non-Frobenius rings in [35] and [61]. It is a particular case of the code from Theorem 3.0.1.

For vector space alphabet we have the following corollary of Theorem 3.0.2.

Corollary 3.2.1 (see [24])**.** *Let $\mathbb{F}_q$ be a finite field and let A be an $\mathbb{F}_q$-linear vector space of dimension greater than one. Let $n \leq q$ and let $C \subseteq A^n$ be a $\mathbb{F}_q$-linear code. Any $\mathbb{F}_q$-linear Hamming isometry of C extends to a monomial map. Moreover, for any $n > q$ there exists a code in A^n that has an unextendable $\mathbb{F}_q$-linear Hamming isometry.*

Proof. See Theorem 3.0.2 with the ring $R = \mathrm{M}_{1\times 1}(\mathbb{F}_q) = \mathbb{F}_q$ and a left $\mathbb{F}_q$-module $A = \mathrm{M}_{1\times \ell}(\mathbb{F}_q) = \mathbb{F}_q^\ell$. The value $N_1 = \prod_{i=1}^{1}(1 + q^i) = 1 + q$. □

Our original proof of Corollary 3.2.1 given in [24] uses other combinatorial techniques related to covering of vector spaces, discussed in [10] and [46].

4. MDS CODES

Let A be a finite set alphabet and let C be a code in A^n. A well-known result of Singleton claims that,

$$|C| \leq |A|^{n-d+1},$$

where d is the minimum distance of the code. Note that the bound is valid for codes that are not necessarily linear in a classical sense. When a code attains the bound, it is called a maximum distance separable code, or shortly, an *MDS code*. Denote $k = n - d + 1$. We say that C is an $(n, k)_A$ MDS code. Note that $k = \log_{|A|} |C|$ represents an analogue of the dimension of a code in linear case.

In this chapter we discuss an analogue of the extension theorem for MDS codes over a module alphabet. The following theorem is our main result.

Theorem 4.0.1 (see [19])**.** *Let R be a ring with identity and let A be a finite left R-module. Let C be an R-linear $(n, k)_A$ MDS code, $k \neq 2$. Each R-linear Hamming isometry $f : C \to A^n$ extends to a monomial map.*

Also, in this chapter we make a more precise description of extension properties of additive MDS codes and classical linear codes. Among the developed geometric tools we provide a result on the minimum size of a multi-fold partition of a vector space, see Theorem 4.2.1.

4.1 Codes over a module alphabet

Consider the general module alphabet context and recall the notations of Section 2.3. Before using the properties of MDS codes, one general property of the n-tuple $\mathcal{V}$ of the code C is the following. Since the encoding map λ is injective, $\ker \lambda = \bigcap_{i=1}^{n} \ker \lambda_i = \{0\}$. Hence,

$$\bigcap_{i=1}^{n} V_i = \{0\}.$$

Lemma 4.1.1. *Let C be an R-linear $(n, k)_A$ MDS code. For each k-element subset $I \subseteq \{1, \ldots, n\}$, the equality of right R-modules hold,*

$$\bigoplus_{i \in I} V_i^{\perp} = \widehat{M}.$$

Moreover, $|V_i^{\perp}| = |A|$, for all $i \in \{1, \ldots, n\}$.

Proof. It is a well-known fact that deleting any $n-k$ coordinates of C we get a code of the same cardinality, see for example the proof for classical linear codes, [47, p. 319].

Let $I \subseteq \{1,\dots,n\}$ be a subset with k elements. Let C' be a code obtained from C by keeping only coordinates from I. Since C is MDS, the map $\lambda' = (\lambda_i)_{i\in I}$, $\lambda' : M \to A^k$ is an encoding map of C' and thus $\bigcap_{i\in I} V_i = \{0\}$. Calculating the annihilators of both sides, we get $\sum_{i\in I} V_i^\perp = \widehat{M}$.

All the modules M, C and C' are isomorphic to A^k. Thus the dual modules $\widehat{M}$ and $\widehat{A}^k$ are isomorphic as right R-modules. Since for all $i \in \{1,\dots,n\}$, $V_i^\perp = \operatorname{im}\widehat{\lambda}_i$ (see eq. (2.3)), we have $|V_i^\perp| = |\operatorname{im}\widehat{\lambda}_i| \le |\widehat{A}|$. Consider the following inequalities,

$$|\widehat{A}|^k = |\widehat{M}| = \left|\sum_{i\in I} V_i^\perp\right| \le \prod_{i\in I} |V_i^\perp| \le |\widehat{A}|^k.$$

Therefore there are equalities everywhere in the expression above. We get $|V_i^\perp| = |\widehat{A}| = |A|$ and the equality of the statement. □

Next lemma shows that for an MDS code the condition of pseudo-injectivity of the alphabet in Proposition 2.3.1 can be omitted.

Lemma 4.1.2. *Let C be an R-linear $(n,k)_A$ MDS code and let $f : C \to A^n$ be an R-linear map. If $\mathcal{V} = \mathcal{U}$, then f extends to a monomial map.*

Proof. The proof is almost identical to the second part of the proof of Proposition 2.3.1. Let $\sigma, \tau \in \operatorname{Hom}_R(M, A)$ be two maps that encode a column in C and a column in $f(C)$ correspondingly. Since C is an MDS code, from Lemma 4.1.1, $\operatorname{im}\sigma = A$, because $|\operatorname{im}\sigma| = |M/\ker\sigma| = |(\ker\sigma)^\perp| = |A|$.

Let $\ker\sigma = \ker\tau = N \subseteq M$. Then $|\operatorname{im}\tau| = |\operatorname{im}\sigma| = |A|$, which means $\operatorname{im}\tau = A$. Consider the canonical isomorphisms $\bar{\sigma}, \bar{\tau} : M/N \to A$. The map $h \in \operatorname{Aut}_R(A)$, defined as $h = \bar{\tau}\bar{\sigma}^{-1}$, satisfies the equality $h\sigma = \tau$. □

Note that the statement of the lemma remains correct if we only require each map λ_i to be onto, for $i \in \{1,\dots,n\}$.

Recall the two equivalent equations,

$$\sum_{i=1}^{n} \mathbb{1}_{V_i} = \sum_{i=1}^{n} \mathbb{1}_{U_i}. \qquad \text{(2.1 revisited)}$$

$$\sum_{i=1}^{n} |V_i| \mathbb{1}_{V_i^\perp} = \sum_{i=1}^{n} |U_i| \mathbb{1}_{U_i^\perp}. \qquad \text{(2.2 revisited)}$$

Proof of Theorem 4.0.1. By contradiction, assume that there exists an unextendable Hamming isometry $f \in \operatorname{Hom}_R(C, A^n)$. From Proposition 2.3.1 and Lemma 4.1.2, $\mathcal{U} \neq \mathcal{V}$ and $(\mathcal{U}, \mathcal{V})$ satisfies eq. (2.1), or equivalently, $(\mathcal{U}, \mathcal{V})$ satisfies (2.2). It is clear that $f(C)$ is also an MDS code.

The proof is obvious for the case $k = 1$, so let $k \ge 3$. This means, from Lemma 4.1.1, for any different $i, j, l \in \{1,\dots,n\}$, $V_i^\perp \cap (V_j^\perp + V_l^\perp) = \{0\}$.

Without loss of generality, assume that $U_1^\perp$ is nontrivially covered by the modules $V_1^\perp, \ldots, V_t^\perp$, $t > 1$, i.e. $U_1^\perp = \bigcup_{i=1}^{t} V_i^\perp$, $\{0\} \subset V_i^\perp \subset U_1^\perp$, for $i \in \{1, \ldots, t\}$ and no module is contained in another.

Take a nonzero element $a \in U_1^\perp \cap V_1^\perp$ and a nonzero element $b \in U_1^\perp \cap V_2^\perp$. Obviously, since $V_1^\perp \cap V_2^\perp = \{0\}$, $a + b \notin V_1^\perp \cup V_2^\perp$. But $a + b \in U_1^\perp$ and hence $t > 2$. There exists an index i, let it be 3, such that $a + b \in U_1^\perp \cap V_3^\perp$. Then $a + b \in (V_1^\perp + V_2^\perp) \cap V_3^\perp \neq \{0\}$, which gives a contradiction. □

We observe the case of MDS codes of dimension 2 in Section 4.2.3, where R is a finite field and the alphabet A is a vector space. In Section 4.3 we generalize an extension property for MDS codes over a group alphabet. Recall that a *nontrivial partition* of a finite abelian group G is a set of proper subgroups $H_1, \ldots, H_t$ with the property that for any $g \in G \setminus \{0\}$ there exists unique $i \in \{1, \ldots, t\}$, such that $g \in H_i$.

Theorem 4.1.1 (see [50]). *If there exists a nontrivial partition of a finite abelian group G, then G is a non-simple elementary abelian group, i.e., $G \cong \mathbb{Z}_p^m$ for some prime p and integer $m \geq 2$.*

Proposition 4.1.1 (see [19]). *Let R be a ring with identity and let A be a finite left R-module such that A, considered as an abelian group, is not non-simple elementary. Let C be an $(n, 2)_A$ MDS code. Each Hamming isometry $f \in \mathrm{Hom}_R(C, A^n)$ extends to a monomial map.*

Proof. By contradiction, assume that there exists an unextendable Hamming isometry $f \in \mathrm{Hom}_R(C, A^n)$. From Proposition 2.3.1 and Lemma 4.1.2, the corresponding solution $\mathcal{U} \neq \mathcal{V}$ and $(\mathcal{U}, \mathcal{V})$ satisfies eq. (2.2). From Lemma 4.1.1, $V_i^\perp \cap V_j^\perp = U_i^\perp \cap U_j^\perp = \{0\}$ for all $i \neq j \in \{1, \ldots, n\}$. Also, since $\mathcal{U} \neq \mathcal{V}$, there exists $t \in \{1, \ldots, n\}$ such that $V_t^\perp = \bigcup_{j=1}^{n} V_t^\perp \cap U_j^\perp$ and the covering is nontrivial. Obviously, $(V_t^\perp \cap U_j^\perp) \cap (V_t^\perp \cap U_i^\perp) = \{0\}$. Hence, the module $V_t^\perp$ has a nontrivial partition. Considering $V_t^\perp$ as a finite abelian group, from Theorem 4.1.1, it is isomorphic to $\mathbb{Z}_p^m$, where p is a prime and $m \geq 2$.

Since C is MDS, $\mathrm{im}\, \lambda_t = A$ and $M \cong A^2$. Hence, $A^2/V_t \cong A$ as abelian groups. Therefore, $V_t \cong A$. From eq. (1.3), $\widehat{V}_t \cong \widehat{M}/V_t^\perp$. Since an abelian group and its character dual are isomorphic, $A \cong \widehat{V}_t \cong \widehat{M}/V_t^\perp \cong A^2/V_t^\perp$ and $V_t^\perp \cong A$ thereby. From the contradiction, the map f extends to a monomial map. □

Remark 4.1.1. In Theorem 4.0.1 and Proposition 4.1.1 the ring R may not be finite.

4.2 Additive codes

The general result of the previous section particularly implies the extension theorem for MDS additive codes of dimension different than two. Consider the context of codes over a vector space alphabet. The alphabet A is a vector space over a finite field $\mathbb{F}_q$.

Corollary 4.2.1 (see [23]). *Let C be a $\mathbb{F}_q$-linear $(n,k)_A$ MDS code, $k \neq 2$. Each $\mathbb{F}_q$-linear Hamming isometry of C extends to a monomial map.*

Proof. See Theorem 4.0.1. □

In Section 4.2.3 we solve the extension problem for additive MDS codes with $k = 2$. Also, we develop and use tools to investigate more deeply the extension property of classical linear codes and particularly, near-MDS codes (see Section 4.2.2).

4.2.1 Multi-fold partitions of vector spaces

Definition 4.2.1. Let Λ be a positive integer. A Λ-*fold partition* of an $\mathbb{F}_q$-linear vector space V is a multiset of vector spaces $\{U_1, \ldots, U_n\}$, where $U_i \subseteq V$, such that for each $v \in V \setminus \{0\}$, $|\{i \mid v \in U_i\}| = \Lambda$.

The condition from the definition can be rewritten as, for all $v \in V \setminus \{0\}$, $\sum_{i=1}^{n} \mathbb{1}_{U_i}(v) = \Lambda$. We call a Λ-fold partition of the space V *nontrivial* if it contains at least one proper subspace of V.

There is a well known bound on the minimum size of the partition. In [7, Lemma 5] it was proved that for a nontrivial 1-fold partition of an m-dimensional vector space V the inequality holds,

$$n \geq q^{\lceil \frac{m}{2} \rceil} + 1.$$

In [27, Theorem 4], it was proven that if $\dim U_i \geq m-r$, for all $i \in \{1, \ldots, n\}$, then $n \geq q^r + \Lambda$, where $r = \max_{i \in \{1,\ldots,n\}} \dim U_i < m$. However, it appears that the restriction on the dimensions of subspaces is not necessary. Following the ideas of [7] and [27], we prove the following.

Theorem 4.2.1. *For a nontrivial Λ-fold partition of an m-dimensional vector space the equality holds,*

$$n \geq q^{\lceil \frac{m}{2} \rceil} + \Lambda.$$

Proof. See the proof in [23]. □

Theorem 4.2.1 is used to get two technical lemmas that will be used in the proofs of propositions in the next sections. Recall that for the context of additive codes, the modules in the n-tuples $\mathcal{U}$ and $\mathcal{V}$ are vector spaces and recall again the dual equation,

$$\sum_{i=1}^{n} |V_i| \mathbb{1}_{V_i^\perp} = \sum_{i=1}^{n} |U_i| \mathbb{1}_{U_i^\perp}. \qquad \text{(2.2 revisited)}$$

Lemma 4.2.1. *Let eq. (2.2) holds and $\mathcal{U} \neq \mathcal{V}$ and let for all $i, j \in \{1, \ldots, n\}$, $V_i^\perp = V_j^\perp$ or $V_i^\perp \cap V_j^\perp = \{0\}$. Denoting $m = \min\{\dim_{\mathbb{F}_q} V_i^\perp \mid V_i^\perp \neq \{0\}\}$, we have $n > q^{\lceil \frac{m}{2} \rceil} + 1$.*

Proof. See the proof in [23]. □

Lemma 4.2.2. *Let $n \geq 3$ and let $(\mathcal{U}, \mathcal{V})$ satisfies eq. (2.2). If for any different $i, j, k \in \{1, \ldots, n\}$, $\dim_{\mathbb{F}_q}(V_i^\perp + V_j^\perp + V_k^\perp) = \dim_{\mathbb{F}_q} V_i^\perp + \dim_{\mathbb{F}_q} V_j^\perp + \dim_{\mathbb{F}_q} V_k^\perp$, then $\mathcal{U} = \mathcal{V}$.*

Proof. See the proof in [23]. □

4.2.2 Additive isometries of classical linear codes

Let $\mathbb{F}_q$ be a finite field and let $\mathbb{F}_{q^\ell}$ be a finite field extension of $\mathbb{F}_q$. Whereas the classical MacWilliams Extension Theorem describes linear isometries of linear codes in $\mathbb{F}_{q^\ell}^n$ it does not apply to $\mathbb{F}_q$-linear isometries of $\mathbb{F}_{q^\ell}$-linear codes. On the vector space alphabet A consider a structure of the finite field $\mathbb{F}_{q^\ell}$ (see Remark 1.5.1).

Theorem 4.2.2 (see [23])**.** *Let C be an $\mathbb{F}_{q^\ell}$-linear code in $\mathbb{F}_{q^\ell}^n$ with $n \leq q^{\lceil \frac{\ell}{2} \rceil}$. Each $\mathbb{F}_q$-linear Hamming isometry of C extends to an $\mathbb{F}_q$-linear monomial map on $\mathbb{F}_{q^\ell}^n$.*

Proof. Assume that $f : C \to A^n$ is an unextendable $\mathbb{F}_q$-linear isometry and thus the pair $(\mathcal{U}, \mathcal{V})$ is a solution of eq. (2.2) and $\mathcal{U} \neq \mathcal{V}$. Let $i \neq j \in \{1, \ldots, n\}$. If one or both of ith or jth columns of C are all-zero, then $V_i^\perp \cap V_j^\perp = \{0\}$. If $V_i^\perp \neq \{0\}$ and $V_j^\perp \neq \{0\}$, then there are two possible cases. In the first case, the ith column and jth column are linearly dependent, which means that they differs by a nonzero scalar from $\mathbb{F}_{q^\ell}$. Since multiplication by a nonzero scalar in $\mathbb{F}_{q^\ell}$ is an $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^\ell}$, considered as an $\mathbb{F}_q$-linear vector space, $V_i^\perp = V_j^\perp$. Since the maps λ_i, λ_j are onto, $|V_i^\perp| = |V_j^\perp| = |A|$.

In the second case the ith and jth columns are linearly independent over $\mathbb{F}_{q^\ell}$, the set $\{(x_i, x_j) \mid (x_1, \ldots, x_n) \in C\} \subseteq A^2$ has $q^{2\ell} = |A^2|$ elements. Then the map $\lambda_{i,j} = (\lambda_i, \lambda_j) : M \to A^2$ is onto. It is easy to calculate that $|V_i \cap V_j| = |M|/|A^2|$ and hence $|V_i^\perp + V_j^\perp| = |A^2|$. Since $|V_i^\perp| = |V_j^\perp| = |A|$ we get $V_i^\perp \cap V_j^\perp = \{0\}$. The conditions of Lemma 4.2.1 are satisfied and hence $n \geq q^{\lceil \frac{\ell}{2} \rceil} + 1$. □

It is clear that much more large class of codes, not only MDS codes, satisfy the extension theorem. For example, in the case of $\mathbb{F}_{q^\ell}$-linear codes, the following holds.

Theorem 4.2.3 (see [23])**.** *Let $C \subseteq \mathbb{F}_{q^\ell}^n$ be an $\mathbb{F}_{q^\ell}$-linear code such that any 3 columns of a generator matrix of C are linearly independent over $\mathbb{F}_{q^\ell}$. Each $\mathbb{F}_q$-linear Hamming isometry of C extends to an $\mathbb{F}_q$-linear monomial map on $\mathbb{F}_{q^\ell}^n$.*

Proof. As in the proof of Theorem 4.2.2, by contradiction, let $(\mathcal{U}, \mathcal{V})$ be a solution of eq. (2.2) with $\mathcal{U} \neq \mathcal{V}$. For every different $i, j, t \in \{1, \ldots, n\}$ the set $\{(x_i, x_j, x_t) \mid (x_1, \ldots, x_n) \in C\} \subseteq A^3$ has $|A^3|$ elements, because every three columns of C are linearly independent. In the same way as in the proof of Theorem 4.2.2, we get the isomorphism of vector spaces $V_i^\perp \oplus V_j^\perp \oplus V_t^\perp \cong \mathbb{F}_{q^\ell}^3$

and the equalities of cardinalities $|V_i^\perp| = |V_j^\perp| = |V_t^\perp| = q^\ell$. The conditions of Lemma 4.2.2 holds, thus $\mathcal{U} = \mathcal{V}$ and we get a contradiction. □

We can now easily prove an analogue of the extension theorem for near-MDS codes. According to [18, Corollary 3.3], we can give the following definition. An $\mathbb{F}_{q^\ell}$-linear code $C \subseteq \mathbb{F}_{q^\ell}^n$ is called *near-MDS* if $d(C) + d(C^\perp) = n$, where $d(C)$ is the minimum distance and $C^\perp$ is the orthogonal code, with respect to a dot product.

Corollary 4.2.2 (see [23]). *Let $C \subseteq \mathbb{F}_{q^\ell}^n$ be an $\mathbb{F}_{q^\ell}$-linear $[n,k]_{\mathbb{F}_{q^\ell}}$ near-MDS code with $k \geq 4$. Each $\mathbb{F}_q$-linear Hamming isometry of C extends to an $\mathbb{F}_q$-linear monomial map on $\mathbb{F}_{q^\ell}^n$.*

Proof. In [18, p. 33] it was proved that for a near-MDS $[n,k]_{\mathbb{F}_{q^\ell}}$ code any $k-1$ columns of its generator matrix are linearly independent. Since $k - 1 \geq 3$, Theorem 4.2.3 proves the statement. □

4.2.3 MDS codes of dimension two

For MDS codes of dimension $k = 2$, the approach presented in the proof of Theorem 4.0.1 fails. But we still can improve the result of Corollary 3.2.1, which states that an $\mathbb{F}_q$-linear code in A^n with unextendable Hamming isometry should have its length greater than $q + 1$. Recall that $\dim_{\mathbb{F}_q} A = \ell$.

Theorem 4.2.4 (see [23]). *Let C be a $\mathbb{F}_q$-linear $(n,2)_A$ MDS code, where $n \leq q^{\lceil \frac{\ell}{2} \rceil}$. Each $\mathbb{F}_q$-linear Hamming isometry of C extends to a monomial map.*

Proof. Assume that $f : C \to A^n$ is an unextendable $\mathbb{F}_q$-linear Hamming isometry. By Proposition 2.3.1, the pair $(\mathcal{U}, \mathcal{V})$ is a solution of eq. (2.2) and $\mathcal{U} \neq \mathcal{V}$. From Lemma 4.1.1, the spaces $V_i^\perp$, $i \in \{1, \ldots, n\}$ intersect each other in zero and $\max\{\dim V_i^\perp \mid V_i^\perp \neq \{0\}\} = \ell$. Thus, from Lemma 4.2.1, $n > q^{\lceil \frac{\ell}{2} \rceil}$. □

The value $q^{\lceil \frac{\ell}{2} \rceil}$ can be presented in a more clear way. If ℓ is even, then it is equal to $\sqrt{|A|}$ and if ℓ is odd, then it is equal to $\sqrt{q|A|}$. The bounds presented in Theorem 4.2.4 and Theorem 4.2.2 are accurate for the case of an alphabet of even dimension over $\mathbb{F}_q$.

Example 4.2.1. Let $\ell = 2t$ be a positive even integer. Let $\mathbb{F}_{q^t}$ be a finite field extension of $\mathbb{F}_q$ of degree t and let $\mathbb{F}_{q^\ell}$ be a quadratic extension of $\mathbb{F}_{q^t}$. In such a way, $[\mathbb{F}_{q^\ell} : \mathbb{F}_q] = 2t = \ell$. Consider an $\mathbb{F}_{q^t}$-linear code $C = \langle \vec{v}_1, \vec{v}_2, \vec{v}_3, \vec{v}_4 \rangle_{\mathbb{F}_{q^t}} \subset \mathbb{F}_{q^\ell}^n$, where $n = q^t + 1 = \sqrt{q^\ell} + 1$,

$$\begin{pmatrix} \vec{v}_1 \\ \vec{v}_2 \\ \vec{v}_3 \\ \vec{v}_4 \end{pmatrix} = \begin{pmatrix} 0 & 1 & \ldots & 1 \\ 1 & x_1 & \ldots & x_{q^t} \\ 0 & \omega & \ldots & \omega \\ \omega & x_1\omega & \ldots & x_{q^t}\omega \end{pmatrix} \xrightarrow{f} \begin{pmatrix} 0 & 1 & \ldots & 1 \\ 0 & \omega & \ldots & \omega \\ 1 & x_1 & \ldots & x_{q^t} \\ \omega & x_1\omega & \ldots & x_{q^t}\omega \end{pmatrix} = \begin{pmatrix} \vec{v}_1 \\ \vec{v}_3 \\ \vec{v}_2 \\ \vec{v}_4 \end{pmatrix},$$

the elements x_i, $i \in \{1, \ldots, q^t\}$, are all different and $\omega \in \mathbb{F}_{q^\ell} \setminus \mathbb{F}_{q^t}$. Let $f : C \to \mathbb{F}_{q^\ell}^n$ be an $\mathbb{F}_{q^t}$-linear map that acts by fixing $\vec{v}_1$ and $\vec{v}_4$ and permuting $\vec{v}_2$ and $\vec{v}_3$.

Calculate the weights of elements of C. It is clear that $\vec{v}_1, \ldots, \vec{v}_4$ have the Hamming weight $n-1$ and for all $\alpha_1, \ldots, \alpha_4 \in \mathbb{F}_{q^t}$, with at most one equals zero, $\mathrm{wt}_H(\alpha_1\vec{v}_1 + \cdots + \alpha_4\vec{v}_4) = n$. Note that for all $\alpha, \beta \in \mathbb{F}_{q^t} \setminus \{0\}$, $\mathrm{wt}_H(\alpha\vec{v}_1 + \beta\vec{v}_4) = \mathrm{wt}_H(\alpha\vec{v}_2 + \beta\vec{v}_3) = n$ and $\mathrm{wt}_H(\alpha\vec{v}_1 + \beta\vec{v}_2) = \mathrm{wt}_H(\alpha\vec{v}_3 + \beta\vec{v}_4) = \mathrm{wt}_H(\alpha\vec{v}_1 + \beta\vec{v}_3) = \mathrm{wt}_H(\alpha\vec{v}_2 + \beta\vec{v}_4) = n - 1$.

One can verify that f is a Hamming isometry, the minimum weight in C is $n - 1$, and hence C is a $(q^t + 1, 2)_{\mathbb{F}_{q^\ell}}$ MDS code. Moreover, f is an $\mathbb{F}_{q^t}$-linear Hamming isometry of C to itself. Note that in the left matrix there is no column with zeros in the first two positions, but the first column in the right matrix have zeros in the first two positions. Therefore, being also an $\mathbb{F}_q$-linear Hamming isometry, f does not extend even to an $\mathbb{F}_q$-linear monomial map. Finally, one additional property of the constructed code is that C is an $\mathbb{F}_{q^\ell}$-linear code since $\vec{v}_3 = \omega\vec{v}_1$ and $\vec{v}_4 = \omega\vec{v}_2$.

The example was first obtained by finding a solution of eq. (2.2) with $\mathcal{U} \neq \mathcal{V}$, using the geometric techniques. However, once found, it is easier to prove the specified properties of the code in the example explicitly, rather than giving a geometric proof.

The case of an odd alphabet dimension is more difficult. Here we only give an example of an MDS code of dimension 2 and length 5 with an unextendable isometry for the case $q = 2$ and $\ell = 3$.

Example 4.2.2. Let $A = \mathbb{F}_2^3$ and let $x, y, z \in A$ be three linearly independent vectors. Consider an $\mathbb{F}_2$-linear code C generated by the rows of the left matrix,

$$\begin{pmatrix} x & 0 & x & x & x \\ y & 0 & y & y & y \\ z & 0 & z & z & z \\ 0 & x & x & x+y & y \\ 0 & y & y & z & x+y+z \\ 0 & z & z & x+z & x+y \end{pmatrix} \xrightarrow{f} \begin{pmatrix} x & 0 & x & x & x \\ y & 0 & y & y & y \\ 0 & x & x & x+y & y \\ z & 0 & z & z & z \\ 0 & y & y & z & x+y+z \\ 0 & z & z & x+z & x+y \end{pmatrix}.$$

Let $f : C \to A^5$ be an $\mathbb{F}_2$-linear map that fixes 1st, 2nd, 5th and 6th rows and permute 3rd and 4th rows of the matrix. It can be directly verified that C is an $\mathbb{F}_2$-linear $(5, 2)_A$ MDS code, f is a Hamming isometry and f is not extendable.

We think that the bound presented in Theorem 4.2.4 is accurate for any odd $\ell > 1$ and any finite field $\mathbb{F}_q$, however, for the moment we only have a proof in characteristics 2. The construction of the example is much less elegant and requires more geometrical background than the construction presented in Example 4.2.1.

4.3 Group codes

In this section we prove the extension theorem for MDS codes over a group alphabet. A finite abelian group is a $\mathbb{Z}$-module. Using the results of the previous sections it is possible to get the complete extension theorem for MDS codes over a group alphabet, both abelian and nonabelian.

For the case of a nonabelian group G we use a nice result by Forney concerning MDS group codes.

Theorem 4.3.1 (see [29])**.** *If C is an (n,k) MDS code over a nonabelian group alphabet, then $k=1$ or $k=n$.*

Lemma 4.3.1. *Let C be an $(n,n)_G$ or $(n,1)_G$ MDS code. Every code homomorphism $f: C \to G^n$ that preserves the Hamming distance extends to a monomial map.*

Proof. Let G be a finite group. Let C be an $(n,n)_G$ MDS code. Then $C = G^n$ and a Hamming isometry $f: C \to G^n$ is a Hamming isometry of the group G^n to itself. Using Theorem 2.1.2, f is monomial (in the context of group codes), i.e., acts by a permutation of coordinates and by an alphabet automorphism on each coordinate. Now, let C be an $(n,1)_G$ MDS code and let $f: C \to G^n$ be a code isometry. Since C is MDS, $C \cong G$ and the projection on the ith coordinate $f_i : G \cong C \to G$ is an injective map. Hence f_i is in $\mathrm{Aut}(G)$. Therefore, by defining $\pi \in \mathfrak{S}_n$ to be a trivial permutation and $\phi_i = f_i$, the map f extends to a monomial map. □

Theorem 4.3.2 (see [19])**.** *Let G be a finite group. Let C be an $(n,k)_G$ MDS group code over an alphabet G. Every homomorphism $f: C \to G^n$ that preserves the Hamming distance extends to a monomial map, except for the case $k=2$ and $G \cong \mathbb{Z}_p^m$ for a prime p and $m \geq 2$. In this case, the map f extends if $n \leq p^{\lceil \frac{m}{2} \rceil}$.*

Proof. Consider consequently the cases. If G is nonabelian, from Theorem 4.3.1, $k=1$ or $k=n$. From Lemma 4.3.1, the statement of the theorem holds. Let G be an abelian group. If $k \neq 2$, from Theorem 4.0.1, considering $R = \mathbb{Z}$, the statement holds again. Let $k=2$. If G not isomorphic to $\mathbb{Z}_p^m$ for some prime p and integer $m \geq 2$, then the statement holds according to Proposition 4.1.1. Finally, let $G \cong \mathbb{Z}_p^m$, $m \geq 2$. The group $\mathbb{Z}_p$ can be seen as a finite field of order p and the group G then has a structure of an m-dimensional vector space. In Theorem 4.2.4 we proved that $n \leq p^{\lceil \frac{m}{2} \rceil}$. □

Remark 4.3.1. Note that Theorem 4.3.2 is a generalization of Theorem 4.0.1 for the case of a group alphabet. In both cases, the value k of an MDS code that differs from 2 always leads to an extension property. However, an attempt to generalize these results for MDS codes over an arbitrary alphabet, i.e. without any algebraic structure, fails. In [55] an example of a combinatorial $(4,3)$ MDS binary code with an unextendable Hamming isometry is given . Though, except this case, all Hamming isometries of combinatorial $(n, n-1)$ MDS codes over arbitrary alphabet, $n \neq 4$, are extendable.

5. SYMMETRIZED WEIGHT COMPOSITION AND GENERAL WEIGHTS

In previous chapters we put our attention on extension properties of different classes of codes over module alphabets equipped with the Hamming weight. However, there exist other weight functions that are used in coding theory. In this chapter we observe general weight functions and particularly one special weight, namely the symmetrized weight composition.

Consider the context of a module alphabet. Let R be a ring with identity and let A be a finite left R-module. Let n be a positive integer and let $C \subseteq A^n$ be an R-module code. Consider the group $\mathrm{Aut}_R(A)$ of all R-linear automorphisms of A and a subgroup $G \leq \mathrm{Aut}_R(A)$. The group $\mathrm{Aut}_R(A)$ acts on A and G inherits the action. Denote by A/G the set of the orbits of the action of the group G on the alphabet A.

Definition 5.0.1 (see [28])**.** A *symmetrized weight composition built on* G is a map $\mathrm{swc}_G : A^n \times A/G \to \{0, \ldots, n\}$ such that for each $a \in A^n$, $O \in A/G$,

$$\mathrm{swc}_G(a, O) = |\{i \mid a_i \in O\}|.$$

We say that $f \in \mathrm{Hom}_R(C, A^n)$ is an swc_G*-preserving map* if for all orbits $O \in A/G$, for all $a \in C$, $\mathrm{swc}_G(a, O) = \mathrm{swc}_G(f(a), O)$.

Definition 5.0.2. An R-linear map $h : A^n \to A^n$ is called G*-monomial* if there exist a permutation $\pi \in \mathfrak{S}_n$ and automorphisms $g_1, \ldots, g_n \in G$ such that for every $a \in A^n$,

$$h(a) = \left(g_1(a_{\pi(1)}), \ldots, g_n(a_{\pi(n)})\right).$$

The alphabet A is said to have an *extension property with respect to* swc_G if for every positive integer n and every R-linear code $C \subseteq A^n$, each swc_G-preserving map $f \in \mathrm{Hom}_R(C, A^n)$ extends to a G-monomial map.

An extension theorem for classical linear codes equipped with the symmetrized weight composition was proved by Goldberg in [31]. He proved that for any subgroup $G \leq \mathbb{F}_q^*$, the alphabet $\mathbb{F}_q$ has an extension property with respect to swc_G.

Recall that the socle of A, denoted $\mathrm{soc}(A)$, is the sum of all simple submodules of A.

Theorem 5.0.1 (see [28, Theorem 3])**.** *Let R be a finite ring with identity and let A be a finite left R-module. If A has a cyclic socle, then, for each subgroup $G \leq \mathrm{Aut}_R(A)$, the alphabet A has an extension property with respect to* swc_G.

The question of the converse, i.e., whether an alphabet A has an extension property with respect to swc_G only if A has a cyclic socle, is asked in in [28].

In this direction, a partial answer is given in [2] where the author showed, with some additional assumptions and for the subgroup $G = \mathrm{Aut}_R(A)$, that if A does not have a cyclic socle, then A does not have an extension property with respect to swc_G.

In this chapter we improve Theorem 5.0.1, for the case of infinite rings and give a complete answer on the question. The main result follows.

Theorem 5.0.2 (see [25]). *Let R be a ring with identity and let A be a finite left R-module. For each subgroup $G \leq \mathrm{Aut}_R(A)$, the alphabet A has an extension property with respect to swc_G if and only if the socle of A is cyclic.*

There is also one additional improvement that can be made by weakening the definition of an extension property, see Remark 5.6.2.

Using Theorem 5.0.2, we can say when an extension property fails to hold for general weight functions. We define a *general weight function* as a map $\omega : A \to \mathbb{Q}^t$, where t is a positive integer. For every $a \in A^n$ the weight $\omega(a)$ is defined as the sum $\sum_{i=1}^{n} \omega(a_i)$.

We say that a map $f \in \mathrm{Hom}_R(C, A^n)$ is an *ω-preserving map* if for any $a \in C$, $\omega(a) = \omega(f(a))$.

Note that swc_G can be seen as a general weight function, by indexing the orbits of A/G with numbers $\{1, \ldots, t\}$, where $t = |A/G|$, we redefine $\mathrm{swc}_G : A \to \mathbb{Q}^t$ as $(\mathrm{swc}_G(a))_k = \mathrm{swc}_G(a, O_k)$, for $k \in \{1, \ldots, t\}$.

Let $U(\omega) = \{g \in \mathrm{Aut}_R(A) \mid \forall a \in A,\ \omega(g(a)) = \omega(a)\}$ be the symmetry group of the weight ω. An alphabet A is said to have an *extension property with respect to ω* if for any positive integer n and for any R-linear code $C \subseteq A^n$, each ω-preserving map $f \in \mathrm{Hom}_R(C, A^n)$ extends to an $U(\omega)$-monomial map. For general weight functions we prove the following.

Theorem 5.0.3 (see [25]). *Let R be a ring with identity, let A be a finite left R-module and let ω be a general weight function. If A has a non-cyclic socle, then A does not have an extension property with respect to ω.*

Unlike the particular case of symmetrized weight compositions, for general weight functions an extension property does not always hold even when the socle is cyclic. Counterexamples are given in [5, 65]. For instance, it is still an open question if an extension property holds for a cyclic group alphabet equipped with the Lee weight. In this direction, in recent works [26, 44], the authors solved the problem for cyclic groups of prime power order.

5.1 Closure of a group

Let G be a group acting on a set X. The *closure* of a subgroup $H \leq G$ with respect to the action on X, denoted $\overline{H}$, is defined as,

$$\overline{H} = \{g \in G \mid \forall O \in X/H,\ g(O) = O\}.$$

Evidently, H is a subgroup of $\overline{H}$. The group is called *closed with respect to the action on* X when $H = \overline{H}$. In other words, $H \leq G$ is closed with respect to the action on X if H consists of all those elements in G that preserve the orbits of H. Note that the closure of a group is closed, i.e., $\overline{\overline{H}} = \overline{H}$.

This definition of closure is introduced by Wood in [62], however a similar definition of a closed group and a definition of a closure of a group were introduced by Wielandt in his 2-closure theory (see [59]). More results on the closure can be found in [17, Section 2.4] and [69].

Example 5.1.1. Let n be a positive integer, let $X = \{1, \ldots, n\}$. The symmetric group $\mathfrak{S}_n$ acts on X in a natural way. Consider the cyclic group $H = \langle (1 \ldots m) \rangle$ generated by the cycle of length m, where $m \leq n$. The subgroup H has $n-m+1$ orbits acting on X, $X/H = \{\{1, \ldots, m\}, \{m+1\}, \ldots, \{n\}\}$. Every permutation $g \in \mathfrak{S}_n$ that fixes all $i \in \{n-m+1, \ldots, n\}$ preserves the orbits in X/H. Hence $\overline{H} \cong \mathfrak{S}_m$ and H is not closed with respect to the action on X, unless $m \leq 2$.

In this chapter we consider the subgroups of $\mathrm{Aut}_R(A)$ that acts on the alphabet A in a natural way, and the notion of a closed group and a closure is defined in the group $\mathrm{Aut}_R(A)$ with respect to this action.

Example 5.1.2. Let $R = \mathbb{Z}$ and let $A = \mathbb{Z}_2 \oplus \mathbb{Z}_2$. The group $\mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$ consists of 6 elements and is isomorphic to the symmetric group $\mathfrak{S}_3$. Let H be a cyclic subgroup generated by the automorphism ϕ, $\phi((1,0)) = (0,1)$ and $\phi((0,1)) = (1,1)$. Obviously, $|H| = 3$ and A/H has two orbits, $\{(0,0)\}$ and $A \setminus \{(0,0)\}$. Thus, $\overline{H} = \mathrm{Aut}_R(A)$ and the group H is not closed.

Example 5.1.3. The subgroups $\{e\}$ and $\mathrm{Aut}_R(A)$ of $\mathrm{Aut}_R(A)$ are closed.

For every weight function ω its symmetry group $U(\omega)$ is closed. Indeed, if $g \in \mathrm{Aut}_R(A)$ preserves the orbits of $U(\omega)$, then $\omega(g(a)) = \omega(a)$, for all $a \in O$ and $O \in A/U(\omega)$, and thus $g \in U(\omega)$.

5.2 Extension criterion

In this section we prove propositions for the symmetrized weight composition that are similar to Proposition 2.1.1 and Proposition 2.3.1 for the Hamming weight.

Proposition 5.2.1. *A map $f \in \mathrm{End}_R(A^n)$ is an swc_G-preserving map if and only if it is a $\overline{G}$-monomial map.*

Proof. Note that the set A/G always contains the zero orbit $\{0\}$. For every $a \in A^n$, $\mathrm{swc}_G(a, \{0\}) = |\{i \mid a_i = 0\}| = n - \mathrm{wt}_H(a)$, where wt_H is the Hamming weight. Thus, if f is an swc_G-preserving map, then f is a Hamming isometry. From Proposition 2.1.1, f is an $\mathrm{Aut}_R(A)$-monomial map (or the same, monomial), with permutation $\pi \in \mathfrak{S}_n$ and automorphisms $g_1, \ldots, g_n \in \mathrm{Aut}_R(A)$.

For each $i \in \{1, \ldots, n\}$ and $b \in A$, let $a = (0, \ldots, 0, b, 0, \ldots, 0) \in A^n$ be the element with b in the ith position and 0 elsewhere. Then, for a nonzero orbit $O \in A/G$, $\mathrm{swc}_G(a, O)$ equals 1 if $b \in O$ and 0 otherwise. From the

other side, $\mathrm{swc}_G(f(a), O) = 1$ if $g_{\pi^{-1}(i)}(b) \in O$ and 0 otherwise. Since f is an swc_G-preserving map, $g_{\pi^{-1}(i)}$ preserves the orbits of A/G. Therefore, for each $j \in \{1, \ldots, n\}$, $g_j \in \overline{G}$ and thus f is a $\overline{G}$-monomial map.

Conversely, if f is a $\overline{G}$-monomial map, then f preserves the orbits of A/G on each coordinate and hence, it preserves swc_G. □

Proposition 5.2.2 (see [25])**.** *The map $f \in \mathrm{Hom}_R(C, A^n)$ preserves swc_G if and only if for each orbit $O \in A/G$, the following equality holds,*

$$\sum_{i=1}^{n} \mathbb{1}_{\lambda_i^{-1}(O)} = \sum_{i=1}^{n} \mathbb{1}_{\mu_i^{-1}(O)}. \tag{5.1}$$

If f extends to a $\overline{G}$-monomial map, then there exists a permutation $\pi \in \mathfrak{S}_n$ such that for each orbit $O \in A/G$, the equality holds,

$$\lambda_{\pi(i)}^{-1}(O) = \mu_i^{-1}(O). \tag{5.2}$$

Proof. For every $w \in M$ and $O \in A/G$,

$$\mathrm{swc}_G(\lambda(w), O) = \sum_{i=1}^{n} \mathbb{1}_O(\lambda_i(w)) = \sum_{i=1}^{n} \mathbb{1}_{\lambda_i^{-1}(O)}(w).$$

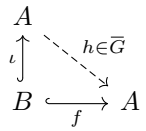
Therefore, f is an swc_G-preserving map if and only if eq. (5.1) holds.

If f extends to a $\overline{G}$-monomial map with a permutation $\pi \in \mathfrak{S}_n$ and automorphisms $g_1, \ldots, g_n \in \overline{G}$, then for all $i \in \{1, \ldots, n\}$, $\mu_i = g_i \lambda_{\pi(i)}$. Hence, for all $O \in A/G$, $\mu_i^{-1}(O) = \lambda_{\pi(i)}^{-1}(g_i^{-1}(O)) = \lambda_{\pi(i)}^{-1}(O)$. □

5.3 G-pseudo-injective modules

For the completeness of the extension criterion, we introduce the following new notion.

Definition 5.3.1. Let A be a finite R-module and let G be a subgroup of $\mathrm{Aut}_R(A)$. An R-module A is called *G-pseudo-injective*, if for every submodule $B \subseteq A$, each injective map $f \in \mathrm{Hom}_R(B, A)$, such that for every $O \in A/G$, $f(O \cap B) \subseteq O$, extends to an element of $\overline{G}$.



Example 5.3.1. The $\mathbb{F}_q$-module $\mathbb{F}_q$ is G-pseudo-injective for all $G \leq \mathbb{F}_q^*$, since it has only two $\mathbb{F}_q$-submodules, $\{0\}$ and $\mathbb{F}_q$ itself.

Consider the vector space $A = \mathbb{F}_3^3$. The group $\mathrm{Aut}_{\mathbb{F}_3}(\mathbb{F}_3^3)$ is isomorphic to the group $\mathrm{GL}_3(\mathbb{F}_q)$ of 3×3 invertible matrices over $\mathbb{F}_q$. The vector space A

is not G-pseudo-injective for a cyclic subgroup $G < \mathrm{GL}_3(\mathbb{F}_3)$ generated by the matrix

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

Indeed, the property fails for the subspace $B = \langle (1,0,0),(0,1,0)\rangle_{\mathbb{F}_3}$ and the map $f \in \mathrm{Hom}_{\mathbb{F}_3}(B, \mathbb{F}_3^3)$, $f(1,0,0) = (0,1,0)$, $f(0,1,0) = (1,0,0)$. The proof of this fact is detailed in Proposition 6.3.3.

An analogue of the last statement of Proposition 2.3.1 for the swc_G follows.

Proposition 5.3.1 (see [25])**.** *If A is G-pseudo-injective and eq.* (5.2) *holds for all orbits $O \in A/G$, then f extends to a $\overline{G}$-monomial map.*

Proof. Fix $i \in \{1,\dots,n\}$. From eq. (5.2) calculated in the orbit $\{0\}$, $\ker \lambda_{\pi(i)} = \ker \mu_i = N \subseteq M$. Consider the canonical injective maps $\bar{\lambda}_{\pi(i)}, \bar{\mu}_i : M/N \to A$ such that $\bar{\lambda}_{\pi(i)}(\overline{w}) = \lambda_{\pi(i)}(w)$ and $\bar{\mu}_i(\overline{w}) = \mu_i(w)$ for all $w \in M$, where $\overline{w} = w + N$.

Let $O \in A/G$. Since $\lambda_{\pi(i)}^{-1}(O) = \mu_i^{-1}(O)$, $\lambda_{\pi(i)}(w) \in O$ if and only if $\mu_i(w) \in O$, for $w \in M$. Therefore, $\bar{\lambda}_{\pi(i)}(\overline{w}) \in O$ if and only if $\bar{\mu}_i(\overline{w}) \in O$, for $\overline{w} \in M/N$. Equivalently, $\bar{\lambda}_{\pi(i)}^{-1}(O) = \bar{\mu}_i^{-1}(O)$.

Note that $\mathrm{im}\,\lambda_{\pi(i)} = \mathrm{im}\,\bar{\lambda}_{\pi(i)}$. For the injective map

$$h_i = \bar{\mu}_i \bar{\lambda}_{\pi(i)}^{-1} \in \mathrm{Hom}_R(\mathrm{im}\,\lambda_{\pi(i)}, A),$$

the inclusion $h_i(O \cap \mathrm{im}\,\lambda_{\pi(i)}) \subseteq O$ holds for all $O \in A/G$. Since A is G-pseudo-injective, there exists an element $g_i \in \overline{G}$ such that $g_i = h_i$ on $\mathrm{im}\,\lambda_{\pi(i)} \subseteq A$. The map $\phi : A^n \to A^n$ given by $\phi(a_1,\dots,a_n) = (g_1(a_{\pi(1)}),\dots,g_n(a_{\pi(n)}))$ is a $\overline{G}$-monomial map extending f. The map ϕ extends f because we see from $g_i = h_i$ on $\mathrm{im}\,\lambda_{\pi(i)}$ that $\mu_i = g_i \lambda_{\pi(i)}$. □

Proposition 5.3.2 (see [25])**.** *An R-module A is G-pseudo-injective if and only if for every code $C \subseteq A^1$ of length one, each swc_G-preserving map $f \in \mathrm{Hom}_R(C, A)$ extends to a $\overline{G}$-monomial map.*

Proof. Prove the contrapositive. By definition, A is not G-pseudo-injective if there exists a module $C \subseteq A$ and an injective map $f \in \mathrm{Hom}_R(C, A)$, such that for each $O \in A/G$, $f(O \cap C) \subseteq O$, but f does not extend to an element of $\overline{G}$. Equivalently, $\mathrm{swc}_G(x, O) = \mathrm{swc}_G(f(x), O)$ for all $x \in C$ and $O \in A/G$, yet f does not extend to an element of $\overline{G}$. □

Remark 5.3.1. Based on Proposition 5.3.2, for a weight function ω we can easily get the following statement. If A is not $U(\omega)$-pseudo-injective, then there exists a code $C \subset A^1$ and there exists an ω-preserving map $f \in \mathrm{Hom}_R(C, A)$ that does not extend to a $\overline{G}$-monomial map.

In [15, 67] the authors used the property of pseudo-injectivity to describe an extension property for the Hamming weight. They showed that an alphabet is

not pseudo-injective if and only if there exists an R-linear code $C \subset A^1$ with an unextendable Hamming isometry. Proposition 5.3.2 is an analogue of this fact.

From Theorem 5.0.1 and Proposition 5.3.2, it follows that if A has a cyclic socle, then A is G-pseudo-injective, for all $G \leq \mathrm{Aut}_R(A)$. Not all the modules are G-pseudo-injective. It is even true that not all pseudo-injective modules are G-pseudo-injective, for some $G \leq \mathrm{Aut}_R(A)$. In Chapter 6 we give a description of G-pseudo-injectivity of finite vector spaces.

5.4 Posets and Möbius function

Definition 5.4.1. A *partial order* $\preceq$ is a binary relation over a set X, such that for all $x, y, z \in X$ the following holds,

- reflexivity: $x \preceq x$,
- antisymmetry: if $x \preceq y$ and $y \preceq x$, then $x = y$,
- transitivity: if $x \preceq y$ and $y \preceq z$, then $x \preceq z$.

The pair $(X, \preceq)$ is called a partially ordered set (*poset*).

Let $(X, \preceq)$ be a poset, where X is finite. For $x, y \in X$, denote $x \prec y$ if $x \preceq y$ and $x \neq y$. Its *Möbius function* $\mu : X \times X \to \mathbb{Z}$ is defined in a recursive way,

$$\mu(x,y) = \begin{cases} 1 & , \text{ if } x = y; \\ -\sum_{x \preceq z \prec y} \mu(x,z) & , \text{ if } x \prec y; \\ 0 & , \text{ if } x \not\preceq y. \end{cases}$$

Do not confuse the Möbius function μ with the encoding map $\mu : M \to A^n$ of the image $f(C)$. From the definition, for any $x \prec y \in X$,

$$\sum_{x \preceq z \preceq y} \mu(x,z) = 0.$$

Consider the poset $(X, \succeq)$, where $\succeq$ is the inverted partial order, i.e., such that $x \succeq y$ if and only if $y \preceq x$, for all $x, y \in X$. Let μ^* be the Möbius function of this poset. The functions μ and μ^* are related.

Proposition 5.4.1 ([52, Proposition 3])**.** *Let $(X, \succeq)$ be the poset obtained by inverting the order of a finite poset $(X, \preceq)$, and let μ^* and μ be the Möbius functions of $(X, \succeq)$ and $(X, \preceq)$ correspondingly. Then, for all $x, y \in X$,*

$$\mu^*(x,y) = \mu(y,x).$$

Recall the basic definitions and results of matrix modules from Section 3.1. Let $R = \mathrm{M}_{k \times k}(\mathbb{F}_q)$ be the matrix ring, where k is a positive integer and q is a prime power. Let M be a left m-dimensional R-module. Considering the ring R as a left R-module over itself,

$$\dim R = k.$$

Let $\mathcal{L}(M)$ be the set of submodules of M and let μ be the Möbius function of the poset $(\mathcal{L}(M), \subseteq)$.

Lemma 5.4.1. *For every $V \in \mathcal{L}(M)$, if $\dim V > k$, then*

$$\sum_{U \in \mathcal{L}(M)} \mu(U,V)\mathbb{1}_U = 0.$$

Proof. For a submodule $U \subseteq M$ and an element $w \in M$ the inclusion $w \in U$ holds if and only if for the cyclic module Rw the inclusion $Rw \subseteq U$ holds. For every $V \in \mathcal{L}(M)$ and $w \in M$,

$$\sum_{U \in \mathcal{L}(M)} \mu(U,V)\mathbb{1}_U(w) = \sum_{U \subseteq V} \mu(U,V)\mathbb{1}_U(w) = \sum_{Rw \subseteq U \subseteq V} \mu(U,V).$$

If $Rw \not\subseteq V$, then the sum is empty and the equality from the statement holds. Suppose $Rw \subseteq V$. Since $\dim Rw \leq \dim R = k < \dim V$, $Rw \subset V$. Using the duality of the Möbius function, see Proposition 5.4.1,

$$\sum_{Rw \subseteq U \subseteq V} \mu(U,V) = \sum_{V \supseteq U \supseteq Rw} \mu^*(V,U) = 0.$$

□

Remark 5.4.1. Since the poset $(\mathcal{L}(M), \subseteq)$ is isomorphic to the poset of subspaces of an m-dimensional vector space, see Remark 3.1.1, based on the result for vector spaces, see [56, Example 3.10.2], for every $U, V \in \mathcal{L}(M)$,

$$\mu(U,V) = \begin{cases} (-1)^{\dim V - \dim U} q^{\binom{\dim V - \dim U}{2}} & \text{, if } U \subseteq V; \\ 0 & \text{, otherwise.} \end{cases}$$

5.5 Code construction

In this section we construct a code over a matrix module alphabet with an $\mathrm{swc}_{\{e\}}$-preserving map that does not extend to an $\mathrm{Aut}_R(A)$-monomial map. We will use this construction in the next section to prove extension theorems for the symmetrized weight compositions and general weight functions.

An $\mathrm{swc}_{\{e\}}$-preserving map is of particular interests because it acts on each codeword in A^n by permuting the coordinates. Such a map preserves the complete weight enumerator of a code.

Lemma 5.5.1. *For every positive integer ℓ there exists an integer $m > \ell$ such that*

$$\sum_{i=0}^{\ell-1} \begin{bmatrix} m \\ i \end{bmatrix}_q < q^{\ell(m-\ell)}.$$

Proof. If $\ell = 1$ the inequality holds for each $m > 1$. Let $\ell \geq 2$. If $m \geq 2\ell$, then

$$\sum_{i=0}^{\ell-1} \begin{bmatrix} m \\ i \end{bmatrix}_q < \ell \begin{bmatrix} m \\ \ell - 1 \end{bmatrix}_q = \ell \prod_{i=0}^{\ell-2} \frac{q^{m-i}-1}{q^{\ell-1-i}-1} < \ell \prod_{i=0}^{\ell-2} q^m = q^{(\ell-1)m + \log_q \ell},$$

where the first inequality holds because $\begin{bmatrix} m \\ i \end{bmatrix}_q < \begin{bmatrix} m \\ \ell-1 \end{bmatrix}_q$ for $i \in \{0, \ldots, \ell-1\}$ and $m \geq 2\ell$. The inequality $q^{(\ell-1)m+\log_q \ell} \leq q^{\ell(m-\ell)}$ holds for all $m \geq \ell^2 + \log_q \ell$. The value $m = \ell^2 + \lceil \log_q \ell \rceil \geq 2\ell$ satisfies the inequality in the statement. □

Let $R = \mathrm{M}_{k\times k}(\mathbb{F}_q)$ be the matrix ring, where k is a positive integer and q is a prime power. Let ℓ be a positive integer greater than k. Let M be an m-dimensional left R-module, where $m > \ell$ is an integer that satisfies the inequality in Lemma 5.5.1. The dual module $\widehat{M}$ is a right R-module of dimension m.

Fix a submodule X in $\mathcal{L}(\widehat{M})$ of dimension $m - \ell$ and define two subsets of $\mathcal{L}(\widehat{M})$,

$$S_1 = \left\{ P \in \mathcal{L}(\widehat{M}) \mid \dim P = \ell,\ P \cap X = \{0\} \right\},$$

$$S_2 = \left\{ P \in \mathcal{L}(\widehat{M}) \mid \dim P < \ell,\ P \cap X = \{0\} \right\}.$$

Calculate the cardinalities of these sets. From Lemma 3.1.1,

$$|S_1| = q^{l(m-l)} \begin{bmatrix} l \\ l \end{bmatrix}_q = q^{l(m-l)}.$$

Since $S_2 \subset \{P \in \mathcal{L}(\widehat{M}) \mid \dim P < \ell\}$ and $\begin{bmatrix} m \\ i \end{bmatrix}_q$ is the number of i-dimensional submodules of $\widehat{M}$,

$$|S_2| < \sum_{i=0}^{\ell-1} \begin{bmatrix} m \\ i \end{bmatrix}_q.$$

Since we chose m to satisfy the inequality in Lemma 5.5.1, $|S_1| > |S_2|$.

Let $\mathrm{F}(X, Y)$ denote the set of all maps from the set X to the set Y. Consider the poset $(\mathcal{L}(\widehat{M}), \subseteq)$ with the Möbius function μ and define the map,

$$\Delta : \mathrm{F}(S_1, \mathbb{Q}) \to \mathrm{F}(S_2, \mathbb{Q}), \quad \Delta(\phi)(Q) = \sum_{P \in S_1} \phi(P)\mu(Q, P),$$

for $Q \in S_2$, $\phi \in \mathrm{F}(S_1, \mathbb{Q})$. The map Δ is a $\mathbb{Q}$-linear homomorphism of $\mathbb{Q}$-linear vector spaces and the inequality holds,

$$\dim_{\mathbb{Q}} \ker \Delta \geq \dim_{\mathbb{Q}} \mathrm{F}(S_1, \mathbb{Q}) - \dim_{\mathbb{Q}} \mathrm{F}(S_2, \mathbb{Q}) = |S_1| - |S_2| > 0.$$

Let

$$\xi \in \ker \Delta$$

be a nonzero map with integer values.

For any module $V \in \mathcal{L}(M)$ the annihilator module $V^\perp$ is in $\mathcal{L}(\widehat{M})$, and for any module $P \in \mathcal{L}(\widehat{M})$, $P^\perp \in \mathcal{L}(M)$. Define the map $\eta \in \mathrm{F}(\mathcal{L}(M), \mathbb{Q})$ as follows, for $V \in \mathcal{L}(M)$,

$$\eta(V) = \begin{cases} \xi(V^\perp) & \text{, if } V^\perp \in S_1; \\ 0 & \text{, otherwise.} \end{cases}$$

Note that η is a nonzero map that has only integer values, since so is ξ. Define the map

$$W : \mathrm{F}(\mathcal{L}(M), \mathbb{Q}) \to \mathrm{F}(M, \mathbb{Q}), \quad \zeta \mapsto \sum_{U \in \mathcal{L}(M)} \zeta(U) \mathbb{1}_U.$$

A similar map was observed in [66, 67].

Proposition 5.5.1. *The equality $W(\eta) = 0$ holds.*

Proof. For every $P \in S_1$, $\dim V = \ell > k$, and thus, from Lemma 5.4.1,

$$0 = \sum_{Q \in \mathcal{L}(\widehat{M})} \mu(Q, P) \mathbb{1}_Q = \sum_{Q \subseteq P} \mu(Q, P) \mathbb{1}_Q = \mathbb{1}_P + \sum_{Q \subset P} \mu(Q, P) \mathbb{1}_Q.$$

If $P \in S_1$ and $Q \subset P$, then $\dim Q < \dim P = \ell$ and $Q \cap X \subseteq P \cap X = \{0\}$. Hence $Q \in S_2$ and the equality holds,

$$\mathbb{1}_P = -\sum_{Q \subset P} \mu(Q, P) \mathbb{1}_Q = -\sum_{Q \in S_2} \mu(Q, P) \mathbb{1}_Q.$$

Recall that the map ξ is in the kernel of Δ. Then,

$$\begin{aligned} \sum_{P \in S_1} \xi(P) \mathbb{1}_P &= -\sum_{P \in S_1} \xi(P) \sum_{Q \in S_2} \mu(Q, P) \mathbb{1}_Q \\ &= -\sum_{Q \in S_2} \left(\sum_{P \in S_1} \xi(P) \mu(Q, P) \right) \mathbb{1}_Q \\ &= -\sum_{Q \in S_2} \Delta(\xi)(Q) \mathbb{1}_Q = 0. \end{aligned}$$

The Fourier transform is a $\mathbb{Q}$-linear map. For all $P \in S_1$, $\dim P = \ell$, $|P| = q^{k\ell}$ and $|P^\perp| = q^{(m-\ell)k}$. Calculate,

$$\begin{aligned} \mathcal{F}(W(\eta)) &= \sum_{U \in \mathcal{L}(M)} \eta(U) \mathcal{F}(\mathbb{1}_U) \overset{(1.1)}{=} \sum_{U^\perp \in S_1} \xi(U^\perp) |U| \mathbb{1}_{U^\perp} \\ &= \sum_{P \in S_1} |P^\perp| \xi(P) \mathbb{1}_P = q^{(m-\ell)k} \sum_{P \in S_1} \xi(P) \mathbb{1}_P = 0. \end{aligned}$$

The Fourier transform is invertible, thus $W(\eta) = \mathcal{F}^{-1}(0) = 0$. □

Define two maps $\eta_+, \eta_- \in \mathrm{F}(\mathcal{L}(M), \mathbb{Q})$, as

$$\eta_+(V) = \max\{\eta(V), 0\}, \quad \eta_-(V) = \max\{-\eta(V), 0\},$$

for $V \in \mathcal{L}(M)$. Obviously, $\eta = \eta_+ - \eta_-$ and the maps η_+ and η_- have non-intersecting supports. From Proposition 5.5.1, $W(\eta_+) = W(\eta + \eta_-) = W(\eta) + W(\eta_-) = W(\eta_-)$.

Define a positive integer $n = W(\eta_+)(0) = W(\eta_-)(0)$. Let $(V_i)_{i=1}^n$ and $(U_i)_{i=1}^n$, be two n-tuples of submodules of M, such that,

$$|\{i \mid V_i = V\}| = \eta_+(V), \quad |\{i \mid U_i = V\}| = \eta_-(V),$$

for all $V \in \mathcal{L}(M)$. Such n-tuples of modules exist since η_+ and η_- have non-negative integer values.

Proposition 5.5.2. *For all $i \in \{1, \dots, n\}$, $V_i \oplus X^\perp = M$ and $U_i \oplus X^\perp = M$.*

Proof. Let $V \in \mathcal{L}(M)$ be such that $\eta_+(V) > 0$ or $\eta_-(V) > 0$. Then $\eta(V) \neq 0$, which means $V^\perp \in S_1$, and hence $\dim V^\perp = \ell$ and $V^\perp \cap X = \{0\}$. From the first equality, $\dim V = \dim M - \dim V^\perp = m - \ell$. From the second equality, calculating the annihilators of both sides, $V + X^\perp = M$. Recall that $\dim X^\perp = m - (m - \ell) = \ell$, and therefore $V \cap X^\perp = \{0\}$. Hence $M = V \oplus X^\perp$. The statement of the proposition follows from the inequalities, $\eta_+(V_i) > 0$ and $\eta_-(U_i) > 0$, for $i \in \{1, \dots, n\}$. □

Let A be an ℓ-dimensional left R-module. Since $\ell = \dim X^\perp = \dim A$ there exists an isomorphism of matrix modules $\psi : X^\perp \to A$. For every $i \in \{1, \dots, n\}$, using Proposition 5.5.2, define $\lambda_i, \mu_i \in \mathrm{Hom}_R(M, A)$,

$$\lambda_i : M = V_i \oplus X^\perp \to A, \quad (v, x) \mapsto \psi(x),$$
$$\mu_i : M = U_i \oplus X^\perp \to A, \quad (u, x) \mapsto \psi(x).$$

Then, $\ker \lambda_i = V_i$, $\ker \mu_i = U_i$ and for all $a \in A$,

$$\lambda_i^{-1}(a) = \psi^{-1}(a) + V_i, \quad \mu_i^{-1}(a) = \psi^{-1}(a) + U_i.$$

Calculate, for $a \in A$, for $w \in M$,

$$\begin{aligned}\sum_{i=1}^n \mathbb{1}_{\lambda_i^{-1}(a)}(w) &= \sum_{i=1}^n \mathbb{1}_{\psi^{-1}(a)+V_i}(w) = \sum_{V \in \mathcal{L}(M)} \eta_+(V) \mathbb{1}_{\psi^{-1}(a)+V}(w) \\ &= \sum_{V \in \mathcal{L}(M)} \eta_+(V) \mathbb{1}_V(w - \psi^{-1}(a)) = W(\eta_+)(w - \psi^{-1}(a)),\end{aligned}$$

and in the same way,

$$\sum_{i=1}^n \mathbb{1}_{\mu_i^{-1}(a)}(w) = W(\eta_-)(w - \psi^{-1}(a)).$$

Evidently, since $W(\eta_+) = W(\eta_-)$, for every orbit $O = \{a\} \in A/\{e\}$, eq. (5.1) holds. In particular, for the orbit $O = \{0\}$,

$$\sum_{i=1}^n \mathbb{1}_{\ker \lambda_i} = \sum_{i=1}^n \mathbb{1}_{\ker \mu_i}.$$

Also, for all $i, j \in \{1, \dots, n\}$, $V_i = \ker \lambda_i \neq \ker \mu_j = U_j$, since the supports of η_+ and η_- are disjoint.

Define the maps $\lambda, \mu \in \mathrm{Hom}_R(M, A^n)$ as $\lambda = (\lambda_1, \dots, \lambda_n)$, $\mu = (\mu_1, \dots, \mu_n)$. Since eq. (5.1) holds for $O = \{0\}$, we have

$$\ker \lambda = \bigcap_{i=1}^{n} \ker \lambda_i = \bigcap_{i=1}^{n} \ker \mu_i = \ker \mu.$$

Denote $N = \ker \lambda \subseteq M$. Let $\bar{\lambda}, \bar{\mu}$ be two canonical injective maps $\bar{\lambda}, \bar{\mu} \in \mathrm{Hom}_R(M/N, A^n)$ such that $\bar{\lambda}(\overline{w}) = \lambda(w)$ and $\bar{\mu}(\overline{w}) = \mu(w)$ for all $w \in M$, where $\overline{w} = w + N$.

Define the code $C \subset A^n$ as the image $C = \mathrm{im}\, \bar{\lambda} = \mathrm{im}\, \lambda$. Define a map $f \in \mathrm{Hom}_R(C, A^n)$ as $f = \bar{\mu}\bar{\lambda}^{-1}$, so that $f\lambda = \mu$.

Proposition 5.5.3. *Let $R = \mathrm{M}_{k\times k}(\mathbb{F}_q)$ and let $A = \mathrm{M}_{k\times \ell}(\mathbb{F}_q)$, where $\ell > k$. The defined map $f \in \mathrm{Hom}_R(C, A^n)$ preserves $\mathrm{swc}_{\{e\}}$ and does not extend to an $\mathrm{Aut}_R(A)$-monomial map.*

Proof. From Proposition 5.2.2, f is an $\mathrm{swc}_{\{e\}}$-preserving map, because eq. (5.1) holds for every $O = \{a\} \in A/\{e\}$. The map f does not extend to an $\mathrm{Aut}_R(A)$-monomial map, since eq. (5.2) does not hold for the zero orbit $O = \{0\}$. □

5.6 Proof of the main results

In order to prove Theorem 5.0.2, we use the approach of [16] and reduce the problem to the case of matrix module alphabets. Recall some necessary results.

The *Jacobson radical* of R, denoted $\mathrm{rad}(R)$, is an ideal, which equals to the intersection of all maximal left ideals, see [60, p. 178]. It is proved there that $\mathrm{rad}(R)$ is a two-sided ideal and the notion is left-right symmetric. The quotient ring $R/\mathrm{rad}(R)$ is semisimple, see [60, p. 181]. Recall that a non-zero ring is called semisimple if it is semisimple as a left R-module over itself.

Denote by $\mathrm{M}_{r\times r}(\mathbb{F}_q)$ the ring of $r \times r$ matrices over the finite field $\mathbb{F}_q$, where r is a positive integer and q is a prime power. If the ring R is finite, then there exists an isomorphism of rings,

$$R/\mathrm{rad}(R) \cong R_1 \times \cdots \times R_n,$$

where $R_i = \mathrm{M}_{r_i\times r_i}(\mathbb{F}_{q_i})$, for positive integers $n, r_1, \dots, r_n$ and prime powers $q_1, \dots, q_n$, see [42, Theorem 13.1]. Indeed, from the Wedderburn–Artin theorem, see [42, Theorem 3.5], any semisimple ring is isomorphic to the product of matrix rings over division rings. Since the ring R is finite, the division rings are finite, and it is known that finite division rings are fields, see the Wedderburn theorem [42, Theorem 13.1].

Since the canonical projection $R \to R/\mathrm{rad}(R)$ is a ring homomorphism, any $R/\mathrm{rad}(R)$-module can be considered as an R-module. For simple R-modules the converse holds: in [60, p. 179] it is shown that for any simple R-module T, $\mathrm{rad}(R)T = 0$, and hence any simple R-module is a simple $R/\mathrm{rad}(R)$-module.

Let R be finite and let M be an R-module. Since $\operatorname{soc}(M)$ is defined as a sum of simple submodules in M, there exist nonnegative integers $s_1, \ldots, s_n$ such that,

$$\operatorname{soc}(M) \cong s_1 T_1 \oplus \cdots \oplus s_n T_n.$$

Recall that an R-module M is called *cyclic* if there exists $x \in M$ such that $Rx = M$.

Proposition 5.6.1 ([67, Proposition 5.2])**.** *Let R be a finite ring. The socle $\operatorname{soc}(M)$ is cyclic if and only if $s_i \leq r_i$, for all $i \in \{1, \ldots, n\}$.*

Example 5.6.1. Consider the ring $R = \mathbb{Z}_4$ and let $M = \mathbb{Z}_4 \oplus \mathbb{Z}_2$ be a left R-module. The ring R has three ideals: $\{0\}$, $I = \{0, 2\}$ and R itself. Consequently, $\operatorname{rad}(R) = I$, since I is the only maximal ideal, and $R/\operatorname{rad}(I) \cong \mathrm{M}_{1\times 1}(\mathbb{F}_2) = R_1 \cong \mathbb{Z}_2$. The R_1-module $T_1 = \mathbb{Z}_2$ is a simple R_1-module and $r_1 = 1$.

In the same way as we calculated in Example 2.1.2, the socle $\operatorname{soc}(M)$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Since $T_1 \cong \mathbb{Z}_2$, $\operatorname{soc}(M) \cong 2T_1$ so that $s_1 = 2$. From the other side, $r_1 = 1$. From Proposition 5.6.1, since $s_1 > r_1$, the socle $\operatorname{soc}(\mathbb{Z}_4 \oplus \mathbb{Z}_2) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ is not a cyclic $\mathbb{Z}_4$-module.

Now we are ready to give a proof of the complete extension theorem for symmetrized weight composition.

Proof of Theorem 5.0.2. For the case of a finite ring our proof repeats the idea of [61, Theorem 4.1]. Let R be a finite ring. Theorem 5.0.1 states that if A has a cyclic socle, then A has an extension property with respect to swc_G, for any $G \leq \operatorname{Aut}_R(A)$. We prove that if the socle of the alphabet is not cyclic, then A does not have an extension property.

From Proposition 5.6.1, if $\operatorname{soc}(A)$ is not cyclic, then there exists an index i with $s_i > r_i$. Of course, $s_i T_i \subseteq \operatorname{soc}(A) \subseteq A$. Recall that $s_i T_i$ is the pullback to R of the R_i-module $B = \mathrm{M}_{r_i \times s_i}(\mathbb{F}_q)$.

Because $r_i < s_i$, Proposition 5.5.3 implies the existence of an R_i-linear code $C \subset B^n$ and an $\mathrm{swc}_{\{e\}}$-preserving map $f \in \operatorname{Hom}_{R_i}(C, B^n)$ that does not extend to an $\operatorname{Aut}_{R_i}(B)$-monomial map.

Denote $V = \ker \lambda_1$. Define a subcode $C' = \lambda(V) \subseteq \operatorname{im} \lambda = C$. The first column of C' is a zero-column, because $\lambda_1(V) = \{0\}$. Assume that the code $f(C')$ has a zero-column. Then there exists $j \in \{1, \ldots, n\}$ such that $V \subseteq \ker \mu_j$. From the construction of Section 5.5, $\dim V = \dim M - s_i = \dim \ker \mu_j$ for all $j \in \{1, \ldots, n\}$. Also, $\ker \lambda_j \neq \ker \mu_k$ for all $j, k \in \{1, \ldots, n\}$. Therefore it is impossible to have $V \subseteq \ker \mu_j$ for some $j \in \{1, \ldots, n\}$ and thus $f(C')$ does not have a zero-column.

The projection mappings $R \to R/\operatorname{rad}(R) \to R_i$ allow us to consider C' and f as an R-module and an R-linear homomorphism correspondingly.

We have $C' \subset (s_i T_i)^n \subseteq \operatorname{soc}(A)^n \subseteq A^n$ as R-modules. The map f thus preserves $\mathrm{swc}_{\{e\}}$ on the R-linear code $C' \subset A^n$. Since $\{e\} \leq G$, f is an swc_G-preserving map. The codes C' and $f(C')$ have different number of zero columns and hence f does not extend to an $\operatorname{Aut}_R(A)$-monomial map. Finally, A does not have an extension property with respect to swc_G for any $G \leq \operatorname{Aut}_R(A)$.

Now we prove the statement of the theorem for the case of arbitrary ring. Recall the notation $R_A = R/\operatorname{ann}(A)$ observed in Section 2.4 on p. 13. We follow the idea of the proof of Theorem 2.4.1. By definition, an R-module A has an extension property with respect to swc_G if for any positive integer n, for any R-linear code $C \subseteq A^n$, each R-linear swc_G-preserving map $f \in \mathrm{Hom}_R(C, A^n)$ extends to a G-monomial map. Hence, R-module A has an extension property with respect to swc_G if and only if R_A-module A has an extension property with respect to swc_G, where $G \leq \mathrm{Aut}_{R_A}(A) = \mathrm{Aut}_R(A)$.

The socle $\mathrm{soc}(A)$ is the same for the module A considered both as R-module and R_A-module. It is cyclic as an R-module if and only if it is cyclic as an R_A-module.

From Lemma 2.4.2, the ring R_A is finite and hence the theorem holds for R_A. From the arguments above, the statement of the theorem also holds for the case of an infinite ring. □

The extension theorem for general weight functions now is straightforward.

Proof of Theorem 5.0.3. Let ω be a general weight function defined on A. Let $C \subseteq A^n$ be a code and let $f \in \mathrm{Hom}_R(C, A^n)$ be an unextendable $\mathrm{swc}_{U(\omega)}$-preserving map that exists due to Theorem 5.0.2. The map f is then an ω-preserving map and it does not extend to an $U(\omega)$-monomial map. □

Remark 5.6.1. The length of the code, constructed in Section 5.5 and used in the proofs of Theorem 5.0.2 and Theorem 5.0.3, can be large. For the ring $R = \mathrm{M}_{k\times k}(\mathbb{F}_q)$ and a matrix module alphabet A, we can give a lower bound on the code length, $n \geq \prod_{i=1}^{k}(1 + q^i)$, which is obtained in Theorem 3.0.2. In Section 5.7 we show that for the special case $k = 1$ there exists an explicit construction that attains the bound. Moreover the resulting unextendable swc_G-preserving map can be a module automorphism of C.

Remark 5.6.2. We can modify the definition of an extension property to improve Theorem 5.0.2. Let G be a subgroup of $\mathrm{Aut}_R(A)$. We say that A has the *extension property with respect to* swc_G, if for any positive integer n and for any linear code $C \subseteq A^n$, each swc_G-preserving map $f \in \mathrm{Hom}_R(C, A^n)$ extends to a $\overline{G}$-monomial map. The new definition is weaker than the original one, since the class of $\overline{G}$-monomial maps contains all G-monomial maps.

One can verify that the symmetrized weight compositions built on groups G and $\overline{G}$ are the same, so it is logical to expect that the definition of an extension property must be the same for both groups. Also, from Proposition 5.2.1, A has an extension property with respect to swc_G if and only if any swc_G-preserving map $f \in \mathrm{Hom}_R(C, A^n)$ extends to an R-linear swc_G-preserving map of A^n.

Independently from the definition we choose, Theorem 5.0.1 and Theorem 5.0.2 remain correct. Note that for the case of general weight functions the two definition are the same, since the symmetry group of a weight function is closed.

Example 5.6.2. To illustrate Theorem 5.0.2 and Theorem 5.0.3, consider a finite R-module alphabet A, where R is a PID (see the definition in Section 2.5).

From Lemma 2.5.1, A has a cyclic socle if and only if A is cyclic itself. Thus, A has an extension property with respect to swc_G, for all $G \leq \mathrm{Aut}_R(A)$, if and only if A is cyclic. Also, if A is a noncyclic R-module, then A does not have an extension property with respect to any general weight function.

5.7 Additive codes

In the previous section we showed that an extension property holds for linear codes over a finite module alphabet with respect to the symmetrized weight composition if and only if the socle of the alphabet is cyclic. For alphabets with a noncyclic socle we prove the existence of an unextendable swc_G-preserving map. However, our construction is implicit.

Below we give an explicit construction of a code with an unextendable $\mathrm{swc}_{\{e\}}$-preserving map. Moreover, the constructed code and the map have nice additional properties, see Proposition 5.7.1. Unlike the general case, where we do not know the length of the constructed code, for vector space alphabet we show that the length can be relatively small.

Let $\mathbb{F}_q$ be a finite field and let A be an $\mathbb{F}_q$-linear vector space of dimension $\ell = 2$, where q is a prime power. The group $\mathrm{Aut}_{\mathbb{F}_q}(A)$ is isomorphic to the group $\mathrm{GL}_2(\mathbb{F}_q)$ of 2×2 invertible matrices with entries in $\mathbb{F}_q$. By introducing a basis of A we identify $\mathrm{Aut}_{\mathbb{F}_q}(A)$ and $\mathrm{GL}_2(\mathbb{F}_q)$.

Let M be an $\mathbb{F}_q$-linear 4-dimensional vector space. Fix bases of A and M. Consider the trivial subgroup $\{I_2\} < \mathrm{GL}_2(\mathbb{F}_q)$, where I_2 is the 2×2 identity matrix. Each orbit of $\{I_2\}$ contains only one point and the group $\{I_2\}$ is closed in $\mathrm{GL}_2(\mathbb{F}_q)$.

Let $\chi(x) = x^2 + \alpha x + \beta$ be an irreducible polynomial over $\mathbb{F}_q$, where $\beta, \alpha \in \mathbb{F}_q$. Then $Q : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q$, $(a, b) \mapsto a^2 + \alpha ab + \beta b^2$ is a quadratic form and $Q(a, b) = 0 \iff a = b = 0$.

Let $\mathbb{P}_1(\mathbb{F}_q)$ be a projective line, $|\mathbb{P}_1(\mathbb{F}_q)| = q + 1$. For any $[a : b] \in \mathbb{P}_1(\mathbb{F}_q)$, define a matrix $\Lambda_{[a:b]} \in \mathrm{M}_{4\times 2}(\mathbb{F}_q)$,

$$\Lambda_{[a:b]} = \frac{1}{Q(a,b)} \begin{pmatrix} -ba & -b^2 \\ a^2 & ab \\ \beta b^2 & -\alpha b^2 - ab \\ -\beta ab & a^2 + \alpha ab \end{pmatrix},$$

and let $\Omega_{[a:b]} \in \mathrm{M}_{4\times 2}(\mathbb{F}_q)$ be a matrix obtained from $\Lambda_{[a:b]}$ by swapping the second and the third row,

$$\Omega_{[a:b]} = \frac{1}{Q(a,b)} \begin{pmatrix} -ba & -b^2 \\ \beta b^2 & -\alpha b^2 - ab \\ a^2 & ab \\ -\beta ab & a^2 + \alpha ab \end{pmatrix}.$$

The matrices are well-defined, i.e. they do not depend on the choice of class representatives in $\mathbb{P}_1(\mathbb{F}_q)$.

For any $p \in \mathbb{P}_1(\mathbb{F}_q)$, define $\mathbb{F}_q$-linear maps $\lambda_p, \mu_p : M \to A$ as $\lambda_p(w) = w\Lambda_p$ and $\mu_p(w) = w\Omega_p$, for all vectors $w \in M$. Let $\lambda, \mu \in \mathrm{Hom}_F(M, A^n)$ be defined as $\lambda = (\lambda_p)_{p\in\mathbb{P}_1(\mathbb{F}_q)}$ and $\mu = (\mu_p)_{p\in\mathbb{P}_1(\mathbb{F}_q)}$. Note that the map λ is injective. Define an $\mathbb{F}_q$-linear code $C \subset A^n$ as the image $C = \mathrm{im}\,\lambda$. Define an $\mathbb{F}_q$-linear map $f : C \to A^n$ as $f = \mu\lambda^{-1}$. The generator matrix of C can be presented as a concatenation of the Λ-matrices and the generator matrix of the image $f(C)$ is a concatenation of the Ω-matrices.

Consider the irreducible polynomial $\bar{\chi}(x) = \chi(-x) = x^2 - \alpha x + \beta$ and consider a finite field extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$, $\mathbb{F}_{q^2} = \mathbb{F}_q[x]/(\bar{\chi}(x))$. Choose the basis $1, \omega$ in $\mathbb{F}_{q^2}$, where $\bar{\chi}(\omega) = 0$, and identify A and $\mathbb{F}_{q^2}$, as vector spaces (see Remark 1.5.1).

Proposition 5.7.1. *The code C is an $\mathbb{F}_{q^2}$-linear $[q+1, 2]_{\mathbb{F}_{q^2}}$ MDS code. The map f is an $\mathbb{F}_q$-linear $\mathrm{swc}_{\{I_2\}}$-preserving automorphism of C that does not extend to a $\mathrm{GL}_2(\mathbb{F}_q)$-monomial map.*

Proof. Prove that the map f is an $\mathrm{swc}_{\{I_2\}}$-preserving map. For each $(x, y) \in A$, $[a : b] \in \mathbb{P}_1(\mathbb{F}_q)$ denote

$$V_{[a:b]} = \langle (a, b, 0, 0), (0, 0, a, b)\rangle_{\mathbb{F}_q},$$
$$U_{[a:b]} = \langle (a, 0, b, 0), (0, a, 0, b)\rangle_{\mathbb{F}_q},$$

and check that,

$$\lambda^{-1}_{[a:b]}(\{(x, y)\}) = (-\alpha x - \beta y, x, x, y) + V_{[a:b]},$$
$$\mu^{-1}_{[a:b]}(\{(x, y)\}) = (-\alpha x - \beta y, x, x, y) + U_{[a:b]}.$$

Indeed, for $\lambda_{[a:b]}$ calculate,

$$(a, b, 0, 0)\Lambda_{[a:b]} = \frac{1}{Q(a, b)}(-ba^2 + ba^2, -ab^2 + ab^2) = (0, 0),$$
$$(0, 0, a, b)\Lambda_{[a:b]} = \frac{1}{Q(a, b)}(\beta ab^2 - \beta a^2 b, -\alpha ab^2 - ba^2 + ba^2 + \alpha ab^2) = (0, 0),$$
$$(-\alpha, 1, 1, 0)\Lambda_{[a:b]} = \frac{1}{Q(a, b)}(\alpha ba + a^2 + \beta b^2, \alpha b^2 + ab - \alpha b^2 - ab) = (1, 0),$$
$$(-\beta, 0, 0, 1)\Lambda_{[a:b]} = \frac{1}{Q(a, b)}(\beta ba - \beta ab, \beta b^2 + a^2 + \alpha ab) = (0, 1).$$

In the same way make calculations for the maps $\mu_{[a:b]}$. The constructed $q + 1$-tuples of spaces correspond to the solution of Type 3 observed in [21], where we prove that $\sum_{p\in\mathbb{P}_1(\mathbb{F}_q)} \mathbb{1}_{V_p} = \sum_{p\in\mathbb{P}_1(\mathbb{F}_q)} \mathbb{1}_{U_p}$. One can verify this equality by hand. Also, for every $(x, y) \in A$ eq. (5.1) holds,

$$\sum_{[a:b]\in\mathbb{P}_1(\mathbb{F}_q)} \mathbb{1}_{(-\alpha x-\beta y,x,x,y)+V_{[a:b]}} = \sum_{[a:b]\in\mathbb{P}_1(\mathbb{F}_q)} \mathbb{1}_{(-\alpha x-\beta y,x,x,y)+U_{[a:b]}}.$$

Hence, by Proposition 5.2.2, f is an $\mathrm{swc}_{\{I_2\}}$-preserving map. However, f does not extend even to a $\mathrm{GL}_2(\mathbb{F}_q)$-monomial map since condition (5.2) does not hold for the zero orbit $\{0\} \in A/\{I_2\}$.

Prove that $f(C) = C$. Denote $\vec{v}_i = \lambda(\vec{e}_i)$, $i \in \{1, 2, 3, 4\}$, where $\vec{e}_i \in M$ is the vector with 1 on the ith position and zeros elsewhere. The map f fixes $\vec{v}_1$ and $\vec{v}_4$ and swaps $\vec{v}_2$ and $\vec{v}_3$, hence $f(C) = C$.

The code C is a $\mathbb{F}_q$-linear code in $\mathbb{F}_{q^2}^n$. Note that $\vec{v}_3 = \omega\vec{v}_1$ and $\vec{v}_4 = \omega\vec{v}_2$. Indeed, for any $[a : b] \in \mathbb{P}_1(\mathbb{F}_q)$,

$$(-ba - b^2\omega)\omega = -ba\omega - b^2(\alpha\omega - \beta) = \beta b^2 - (\alpha b^2 + ab)\omega,$$
$$(a^2 + ab\omega)\omega = a^2\omega + ab(\alpha\omega - \beta) = -\beta ab - (a^2 + \alpha ab)\omega.$$

So, C is an $\mathbb{F}_{q^2}$-linear code. However, $f : C \to C$ is not an $\mathbb{F}_{q^2}$-linear map.

Considering C as a code in a Hamming space $\mathbb{F}_{q^2}^n$, it is equivalent, with a $\mathrm{GL}_2(\mathbb{F}_q)$-monomial equivalence, to a code observed in Example 4.2.1, where we proved that C is a $[q + 1, 2]_{\mathbb{F}_{q^2}}$ MDS code. □

From Proposition 5.7.1, since f is an $\mathbb{F}_q$-linear $\mathrm{swc}_{\{I_2\}}$-preserving map, it acts locally as a permutation of each codeword. Nevertheless, since f is not extendable to a $\{I_2\}$-monomial map, which acts by permutation of columns, there is no general permutation that acts globally as f.

To illustrate the constructions we give an example for the finite field $\mathbb{F}_2$.

Example 5.7.1. Let $q = 2$. Consider the quadratic form $Q : \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2$, $Q(a, b) = a^2 + ab + b^2$, where $a, b \in \mathbb{F}_2$. Consider the projective line $\mathbb{P}_1(\mathbb{F}_2) = \{[0 : 1], [1 : 0], [1 : 1]\}$. Write down the matrix $\Lambda_{[a:b]}$, for each $[a : b] \in \mathbb{P}_1(\mathbb{F}_2)$,

$$\Lambda_{[0:1]} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}, \Lambda_{[1:1]} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}, \Lambda_{[1:0]} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Define an $\mathbb{F}_2$-linear code $C \subseteq (\mathbb{F}_2^2)^3$ as an $\mathbb{F}_2$-span of rows in the left matrix,

$$\begin{pmatrix} 01 & 11 & 00 \\ 00 & 11 & 10 \\ 11 & 10 & 00 \\ 00 & 10 & 01 \end{pmatrix} \xrightarrow{f} \begin{pmatrix} 01 & 11 & 00 \\ 11 & 10 & 00 \\ 00 & 11 & 10 \\ 00 & 10 & 01 \end{pmatrix},$$

and define an $\mathbb{F}_2$-linear map $f : C \to (\mathbb{F}_2^2)^3$ as it is shown in the main construction above. It is easy to check that f is an unextendable $\mathrm{swc}_{\{I_2\}}$-preserving map.

6. G-PSEUDO-INJECTIVITY OF VECTOR SPACES

Recall our Definition 5.3.1 of G-pseudo-injectivity,. Let A be a finite R-module and let G be a subgroup in $\mathrm{Aut}_R(A)$. The R module A is called G-pseudo-injective, if for any submodule $B \subseteq A$, each injective map $f \in \mathrm{Hom}_R(B, A)$, such that for any $O \in A/G$, $f(O \cap B) \subseteq O$, extends to an element of the closure $\overline{G}$.

In this chapter we investigate the G-pseudo-injectivity of vector spaces. Apparently, despite the fact that vector spaces are pseudo-injective (as injective modules, see Example 2.2.1), almost all vector spaces, except a few families, are not G-pseudo-injective for some G. The main result of this chapter is formulated in the following theorem.

Theorem 6.0.1 (see [22])**.** *Let $\mathbb{F}_q$ be a finite field and let V be an n-dimensional $\mathbb{F}_q$-linear vector space. The space V is G-pseudo-injective for every subgroup $G \leq \mathrm{GL}_n(\mathbb{F}_q)$ if and only if $n < 3$ or $V = \mathbb{F}_2^3$.*

6.1 General properties

Proposition 6.1.1. *Every n-dimensional $\mathbb{F}_q$-linear vector space V is $\mathrm{GL}_n(\mathbb{F}_q)$-pseudo-injective and $\{I_n\}$-pseudo-injective, where I_n is the identity $n \times n$ matrix.*

Proof. Note that these two subgroups are closed in $\mathrm{GL}_n(\mathbb{F}_q)$ with respect to the action on V. The set $V/\mathrm{GL}_n(\mathbb{F}_q)$ has only two orbits, $\{0\}$ and $V \setminus \{0\}$. Since V is pseudo-injective, for every subspace $U \subseteq V$ an $\mathbb{F}_q$-linear injective map $f : U \to V$ extends to an element in $\mathrm{GL}_3(\mathbb{F}_q)$. It is easy to see that $f(0) = 0$ and $0 \notin f(U \setminus \{0\})$.

Since $V/\{I_n\} = \{\{x\} \mid x \in V\}$, for any subspace $U \subseteq V$, any injective map $f : U \to V$, such that $f(x) = x$, for all $x \in U$, extends to the map that corresponds to I_n. □

Lemma 6.1.1. *Let $U \subseteq V$ be a subspace of dimension smaller than 2 and let G be a subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$. Any injective map $f : U \to V$ that preserves the orbits of G extends to an element of G.*

Proof. If $U = \{0\}$, then $f : \{0\} \to V$ is a zero map and hence extends to the trivial map that corresponds to $I_n \in G$. If U is one-dimensional, let $u \in V \setminus \{0\}$ be such that $U = \langle u \rangle_{\mathbb{F}_q}$. Let O be an orbit in V/G that contains u. Since f preserves the orbits of G, there exists $v \in O$ such that $v = f(u)$ and there exists $g \in G$ such that $v = g(u)$. Then, for any $x \in \mathbb{F}_q$, $f(xu) = xf(u) = xv =$

$xg(u) = g(xu)$. But $\{xu \mid x \in \mathbb{F}_q\} = U$ and therefore f extends to an element of G □

Remark 6.1.1. In the same way as in the proof of Lemma 6.1.1 we can prove the following generalized fact. Consider a ring R with identity and a finite R-module A. It is true that for any cyclic submodule $U \subseteq A$ any injective map $f \in \mathrm{Hom}_R(U, A)$ which preserves the orbits of $G \leq \mathrm{Aut}_R(A)$, extends to an element of G.

6.2 Poset of orbit partitions

Definition 6.2.1. A *partition* α of a finite set X is a set of subsets of X,

$$\alpha = \{c_1, \ldots, c_t\},$$

such that $c_1 \sqcup \cdots \sqcup c_t = X$, where $c_i \subseteq X$, for all $i \in \{1, \ldots, t\}$, t is a positive integer and the operation $\sqcup$ denotes the disjoint union of sets.

A partition α_1 of the set X is said to be *finer* than a partition α_2 of the same set X, denoted $\alpha_1 \preceq \alpha_2$, if each set in α_2 is a disjoint union of sets from α_1. The binary relation "finer" is a partial order on the set of all partitions of X.

Example 6.2.1. Let $X = \{1, 2, 3\}$. Then for the three partitions $\alpha_1 = \{\{1, 2, 3\}\}$, $\alpha_2 = \{\{1, 2\}, \{3\}\}$ and $\alpha_3 = \{\{1\}, \{2\}, \{3\}\}$ the relations hold, $\alpha_3 \preceq \alpha_2 \preceq \alpha_1$.

Let X be a finite set and let G be a finite group acting on X (from the right side). The set of orbits of the action, denoted as X/G, induces a partition of the set X into a union of disjoint subsets, denoted α_G.

Let H be a subgroup of G. The subgroup H inherits an action on X from G. Obviously, $\alpha_H \preceq \alpha_G$.

Recall Definition 5.4.1 of a partially ordered set (poset). Denote by $\mathcal{P}_G$ the poset $(\{\alpha_H \mid H \leq G\}, \preceq)$. Define the union of the partitions α_{H_1} and α_{H_2}, denoted $\alpha_{H_1} \cup \alpha_{H_2}$, as the finest element in $\mathcal{P}_G$ such that $\alpha_{H_1}, \alpha_{H_2} \preceq \alpha_{H_1} \cup \alpha_{H_2}$. Note that such an element exists and is unique.

Proposition 6.2.1. *Let $H = \langle h_1, \ldots, h_k \rangle \leq G$. Then $\alpha_H = \bigcup_{i=1}^{k} \alpha_{\langle h_i \rangle}$.*

Proof. Since $\langle h_i \rangle \leq H$, it is true that $\alpha_{\langle h_i \rangle} \preceq \alpha_H$, for all $i \in \{1, \ldots, k\}$, and thus $\alpha = \bigcup_{i=1}^{k} \alpha_{\langle h_i \rangle} \preceq \alpha_H$.

Let J be a subgroup of G that contains all elements in G that preserves all classes in α. The subgroup J is closed with respect to the action on X and $\alpha = \alpha_J$. It is easy to see that $h_i \in J$, for all $i \in \{1, \ldots, k\}$, which means $H \leq J$. Thereby, $\alpha_H \preceq \alpha_J = \alpha$. □

Proposition 6.2.2. *Let $H \leq G$ be a subgroup that is closed with respect to the action on X and let $J = \{g \in H \mid g(x) = x\}$ for some $x \in X$. The subgroup J is closed with respect to the action on X and $\alpha_J \preceq \alpha_H$.*

Proof. The group J is a subgroup of H, which means $\alpha_J \preceq \alpha_H$. Let $g \in G$ be an element that preserves all orbits in α_J. Then $g \in H$ and $g(x) = x$, so $g \in J$. Therefore $J = \overline{J}$. □

6.3 Proof of the main result

Let V be an $\mathbb{F}_q$-linear vector space of dimension n. Consider the right action of $\mathrm{GL}_n(\mathbb{F}_q)$ on V by the right matrix multiplication.

6.3.1 Spaces of dimension that differs from 3

Proposition 6.3.1. *If $\dim_{\mathbb{F}_q} V \leq 2$, then for every subgroup $G \leq \mathrm{GL}_n(\mathbb{F}_q)$ the space V is G-pseudo-injective.*

Proof. Let U be a subspace of V and let $f : U \to V$ be a map that preserves the orbits of G. If $U = V$, then f is an element of G. If U is a proper subspace, $\dim_{\mathbb{F}_q} U < 2$ and from Lemma 6.1.1, f extends to an element of $G \leq \overline{G}$. Hence V is G-pseudo-injective. □

Since in this section we consider the case $n \neq 3$ and the case $n \leq 2$ is already observed, let $n \geq 4$.

Let $m \geq 2$ be an integer such that $m \leq \sqrt{n}$, for instance, $m = 2$. Consider the following block-diagonal $m^2 \times m^2$ matrix,

$$T = \begin{pmatrix} M & 0 & \dots & 0 \\ 0 & M & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & M \end{pmatrix},$$

consisting of m blocks on the diagonal, where $M \in \mathrm{GL}_m(\mathbb{F}_q)$. The matrix T generates the cyclic subgroup $\langle T \rangle < \mathrm{GL}_{m^2}(\mathbb{F}_q)$. Consider the block diagonal $n \times n$ matrix,

$$T' = \begin{pmatrix} T & 0 \\ 0 & I_{n-m^2} \end{pmatrix},$$

where $I_{n-m^2} \in \mathrm{GL}_{n-m^2}(\mathbb{F}_q)$ is the identity matrix.

Lemma 6.3.1. *The cyclic group $\langle T' \rangle \leq \mathrm{GL}_n(\mathbb{F}_q)$ is closed with respect to the action on V.*

Proof. Let $B \in \mathrm{GL}_{m^2}(\mathbb{F}_q)$ be an element that preserves the orbits of $\langle T \rangle$, i.e., $B \in \overline{\langle T \rangle}$. For all vectors $v = (x_1, \dots, x_m) \in \mathbb{F}_q^{m^2}$, where each x_i is an m-dimensional vector, there exists an integer p_v such that

$$vB = vT^{p_v}.$$

Let B has the block form, $B = (B_{ij})_{i,j\in\{1,\dots,m\}}$, where each $B_{ij} \in \mathrm{M}_{m\times m}(\mathbb{F}_q)$. Put $v = v_i = (0,\dots,0,x,0,\dots,0)$ with the vector $x \in \mathbb{F}_q^m$ on ith position, $i \in \{1,\dots,m\}$. Then the equality becomes,

$$(xB_{i1}, xB_{i2}, \dots, xB_{im}) = (0,\dots,0,xM^{p_{v_i}},0,\dots,0).$$

Since the vector $x \in \mathbb{F}_q^m$ is arbitrary, $B_{ij} = 0$ for all $i \neq j \in \{1,\dots,m\}$.

Put $v = v_{i,j} \in \mathbb{F}_q^{m^2}$, the vector with $x \in \mathbb{F}_q^m$ on ith and jth positions, $i \neq j \in \{1,\dots,m\}$, and 0 everywhere else. We get then two equalities,

$$xB_{ii} = xM^{p_{v_{i,j}}} \text{ and } xB_{jj} = xM^{p_{v_{i,j}}},$$

for each $x \in \mathbb{F}_q^m$. Therefore, $B_{ii} = B_{jj}$ for all $i,j \in \{1,\dots,m\}$.

Put $v = v_0 = (e_1, e_2, \dots, e_m)$, where $e_i \in \mathbb{F}_q^m$ is a vector with 1 on the ith position and 0 everywhere else. Then, for any $i \in \{1,\dots,m\}$,

$$e_iB_{11} = e_iM^{p_{v_0}},$$

which implies $B_{11} = M^{p_{v_0}}$, for some integer p_{v_0}. Hence $B = T^{p_{v_0}}$, $B \in \langle T\rangle$ and thus $\overline{\langle T\rangle} \subseteq \langle T\rangle$. Therefore, $\langle T\rangle$ is closed with respect to the action on $\mathbb{F}_q^{m^2}$.

It is easy to see that the group $\langle T'\rangle$ is closed subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ with respect to the action on $V \cong \mathbb{F}_q^n$. □

Let $m = 2$. Note that the matrix $T' \in \mathrm{GL}_n(\mathbb{F}_q)$ depends on the choice of the matrix $M \in \mathrm{GL}_2(\mathbb{F}_q)$. In next proposition we suppose that M is a matrix of multiplicative order q^2-1. Such a matrix exists: choose M to be a multiplication matrix of an element $\omega \in \mathbb{F}_{q^2}$, where $\mathbb{F}_{q^2}$ is a finite field extension of $\mathbb{F}_q$ and ω is a primitive element of $\mathbb{F}_{q^2}$.

Proposition 6.3.2. *If $\dim_{\mathbb{F}_q} V \geq 4$, then V is not $\langle T'\rangle$-pseudo-injective.*

Proof. Denote $G = \langle T'\rangle$ and denote by U the subspace of V of dimension 2 generated by the vectors $a = (1,0,0,\dots,0)$ and $b = (0,1,0,\dots,0)$. The subspace U intersects only 2 orbits of V/G: $\{0\}$ and $U \setminus \{0\}$. Indeed, since we chose M to be a multiplication matrix of a generator $\omega \in \mathbb{F}_{q^2}^*$, any nonzero vector in U can by mapped by some element of G to any nonzero vector in U.

A linear map $f : U \to V$ defined by, $f(a) = b$ and $f(b) = a$, is an automorphism of the vector space $U \subset V$. It preserves the orbits in V/G.

By contradiction, assume that f extends to an element of $\overline{G}$. As we proved in Lemma 6.3.1, $G = \overline{G}$. From the construction, the elements of G acts by a multiplication on the first pair of coordinates. Since we are interested in only two first coordinates, let $c \in \mathbb{F}_{q^2}$ be an element that corresponds to the vector $(1,0)$ and let $d \in \mathbb{F}_{q^2}$ corresponds to $(0,1)$. Hence, there exists an element $x \in \mathbb{F}_{q^2}$ such that $f(c) = xc$ and $f(d) = xd$. But from the other side, $f(c) = d$ and $f(d) = c$. Combining these equalities we get,

$$xc = d \text{ and } xd = c.$$

From this, $x^2 = 1$ and $c^2 = d^2$. Rewriting the last equality, $c^2 - d^2 = (c-d)(c+d) = 0$ that implies $c = d$ or $c = -d$ which is impossible, since c and d are linearly independent over $\mathbb{F}_q$. From the contradiction, f does not extend to an element of $\overline{G}$ and hence V is not G-pseudo-injective. □

6.3.2 Three-dimensional spaces

Observe the case $q \neq 2$ and consider the following matrix $X \in \mathrm{GL}_3(\mathbb{F}_q)$,

$$X = \begin{pmatrix} M & 0 \\ 0 & \det M \end{pmatrix},$$

where M is a multiplication matrix of a primitive element $\omega \in \mathbb{F}_{q^2}$. Additionally assume that M is represented in the $\mathbb{F}_q$-linear basis $1, \omega$.

Proposition 6.3.3. *Let V be a 3-dimensional $\mathbb{F}_q$-linear vector space, $q \neq 2$. The space V is not $\langle X \rangle$-pseudo-injective.*

Proof. Denote $G = \langle X \rangle < \mathrm{GL}_3(\mathbb{F}_q)$. Since $\det : \mathrm{GL}_2(\mathbb{F}_q) \to \mathbb{F}_q^*$ is a multiplicative function, $(\det M)^n = \det M^n$, and thus every element of G is of the form

$$X^k = \begin{pmatrix} M^k & 0 \\ 0 & \det M^k \end{pmatrix},$$

for some positive integer k.

Consider a subspace $U = \langle (1,0,0), (0,1,0) \rangle_{\mathbb{F}_q} \subset V$. Define an $\mathbb{F}_q$-linear map $f : U \to V$ by $f((1,0,0)) = (0,1,0)$ and $f((0,1,0)) = (1,0,0)$. As in the proof of Proposition 6.3.2, $f(U) = U$ and U intersects only two orbits of V/G: $\{0\}$ and $U \setminus \{0\}$.

By contradiction, assume that there exists $g \in \overline{G}$ such that $g = f$ on U. Then g has the following form,

$$g = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ \alpha & \beta & \gamma \end{pmatrix},$$

for some $\alpha, \beta \in \mathbb{F}_q$, $\gamma \in \mathbb{F}_q^*$. Use the fact that g preserves the orbits of G. There exists an integer p_1 such that $(0,0,1)g = (0,0,1)X^{p_1}$, or the same, $(\alpha, \beta, \gamma) = (0, 0, (\det M)^{p_1})$. Hence $\alpha = \beta = 0$.

For $v = (x,y,z) \in V$ there exists an integer p_v such that $(x,y,z)g = (y,x,\gamma z) = (x,y,z)X^{p_v} = ((x,y)M^{p_v}, z(\det M)^{p_v})$. Put $v = v_1 = (1,1,1)$. Then

$$((1,1),\gamma) = ((1,1)M^{p_{v_1}}, \det M^{p_{v_1}}).$$

Since $M^{p_{v_1}}$ is a multiplication matrix, it fixes a nonzero element in $\mathbb{F}_q^2$ if and only if $M^{p_{v_1}} = I_2$. From the equality on the third coordinate, $\gamma = \det I_2 = 1$.

Put $v = v_2 = (1,0,1)$. Then we have

$$((0,1),1) = ((1,0)M^{p_{v_2}}, \det M^{p_{v_2}}).$$

We chose M to be such that $(1,0)M = (0,1)$ and therefore $M^{p_{v_2}} = M$. Hence $\det M^{p_{v_2}} = \det M = 1$. Recall ω is a generator of $\mathbb{F}_{q^2}^*$. It is a well-known fact that the norm $N : \mathbb{F}_{q^2}^* \to \mathbb{F}_q^*$, defined as $N(\omega^k) = (\det M)^k$ is an onto map (see [43, pp. 284 – 291]). Since $\mathbb{F}_q \neq \mathbb{F}_2$, $\mathbb{F}_q^* \neq \{1\}$, we get a contradiction. Therefore, V is not G-pseudo-injective. □

Now, observe the case $q = 2$ and $V = \mathbb{F}_2^3$.

Proposition 6.3.4. *For each subgroup $G \leq \mathrm{GL}_3(\mathbb{F}_2)$ the space $\mathbb{F}_2^3$ is G-pseudo-injective.*

Proof. Prove by contradiction. Suppose that there exist a subgroup G, a subspace $U \subseteq V$ and an injective $\mathbb{F}_2$-linear map $f : U \to V$ such that f preserves the orbits of G but does not extend to an element of $\overline{G}$.

Note that such a subspace and a map exist for some group G means that they also exist for the closure $\overline{G}$. Hence, without loss of generality, we assume that G is closed with respect to the action on V.

From Lemma 6.1.1 we know that if $\dim_{\mathbb{F}_2} U \leq 1$, then f extends to an element of G. The same for $U = V$. Therefore $\dim_{\mathbb{F}_2} U = 2$, $U = \langle a, b\rangle_{\mathbb{F}_2} = \{0, a, b, a + b\}$ for some $a, b \in V$.

Let $h \in \mathrm{GL}_3(\mathbb{F}_2)$ be a matrix of change of basis such that $ah = (1, 0, 0)$ and $bh = (0, 1, 0)$. Then the map $hf : hU \to V$ preserves the orbits of the group $G^h = \{h^{-1}gh \mid g \in G\}$ and does not extend to an element of $\overline{G^h}$. Thus, without loss of generality, we may assume that $a = (1, 0, 0)$ and $b = (0, 1, 0)$.

Since a and $f(a)$ are in the same orbit of G, there exists an element $g \in G$ such that $g(f(a)) = a$. Then, the map gf preserves the orbits of G but does not extend to an element of G. Again, without loss of generality, we may assume that $f(a) = a$.

Let $G_a \leq G$ be a subgroup that contains all the elements of G that fix a. From Proposition 6.2.2, G_a is closed. The map f does not extend to an element of G_a. Therefore we can assume that G is a closed subgroup that fixes a.

Denote $f(b) = c$. Then $f(a + b) = a + c$. The map f preserves the orbits of G if and only if the elements b, c and $a + b, a + c$ belong to the same orbits.

The final computational problem that we have to solve is the following.

1. Find all closed subgroups G of $\mathrm{GL}_3(\mathbb{F}_2)$ that have a one-element orbit $O_a = \{(1, 0, 0)\}$.

2. For all such G, let $O_b \subseteq \mathbb{F}_2^3$ be an orbit of G that contains $(0, 1, 0)$. Check that for any $c \in O_b$, such that $(1, 0, 0) + c$ and $(1, 1, 0)$ are in the same orbit of G, there exists $g \in G$ such that $(0, 1, 0)g = c$.

To compute all the closed subgroups of $\mathrm{GL}_3(\mathbb{F}_2)$ use the fact that the closed subgroups are in relation with the partition of $\mathbb{F}_2^3$ into orbits of subgroups in $\mathrm{GL}_3(\mathbb{F}_2)$, see Proposition 6.2.1. The idea is the following, we first compute the orbits of all cyclic subgroup, then we calculate all the elements in the poset $\mathcal{P}_{\mathrm{GL}_3(\mathbb{F}_2)}$. Now, having all possible partitions into orbits we can easily calculate all closed subgroups.

The result is computed. See p. 83 for a SAGE source code. □

7. EXTENSION PROPERTIES OF OTHER CODES

7.1 Stabilizer quantum codes

Error-correcting codes are used for the secure information transmission. In the same way quantum error-correcting codes are used for the secure transmission of quantum-information in quantum channels. There exist several models and approaches to construct quantum error-correcting codes. In this section we are discussing the stabilizer quantum error-correcting codes (see [37, Section 7.4.5]).

In [40] the authors show that there exists a relation between the stabilizer quantum codes and special additive codes and one can define a stabilizer quantum code as an additive code with an additional condition of self-orthogonality. In this section we use this model.

Consider the context of codes over a vector space alphabet with an $\mathbb{F}_q$-linear vector space alphabet $A = \mathbb{F}_q^2$ equipped with the Hamming weight wt_H. Let p be a characteristic of $\mathbb{F}_q$. Fix an $\mathbb{F}_q$-linear basis in A. Every element $a \in A$ can be represented as a pair $a = (a_1, a_2)$, for some $a_1, a_2 \in \mathbb{F}_q$. On A^n define the *trace-symplectic* antisymmetric $\mathbb{F}_p$-bilinear form, $\langle -, - \rangle_s : A^n \times A^n \to \mathbb{F}_p$,

$$\langle x, y \rangle_s = \sum_{i=1}^{n} \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x_{i1}y_{i2} - x_{i2}y_{i1}),$$

where $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace function (see [43, p. 284]).

Let C be an $\mathbb{F}_p$-linear code $C \subseteq A^n$. Define the orthogonal code $C^{\perp_s} = \{x \in A^n \mid \forall y \in C,\ \langle x, y \rangle_s = 0\}$.

Definition 7.1.1. An $\mathbb{F}_p$-linear code $C \subseteq A^n$ is called a *stabilizer quantum code* if $C \subseteq C^{\perp_s}$.

The error-correcting capability of a quantum code is defined by the minimum Hamming weight of the set $C^{\perp_s} \setminus C$ if $C \subset C^{\perp_s}$, and the set $C \setminus \{0\}$ if $C^{\perp_s} = C$.

In this section we observe linear quantum stabilizer codes. For this class of codes we define an extension property and show that it does not hold for almost all codes except for one family.

A quantum code C is called linear if it is an $\mathbb{F}_{q^2}$-linear subspace of A^n, where on the vector space $A = \mathbb{F}_q^2$ we consider a structure of a finite field $\mathbb{F}_{q^2}$ (see Remark 1.5.1).

Considering $A = \mathbb{F}_{q^2}$, recall that the *hermitian form* $\langle -, - \rangle_h : A^n \times A^n \to \mathbb{F}_{q^2}$ is an $\mathbb{F}_q$-bilinear form that is defined in the following way,

$$\langle x, y \rangle_h = \sum_{i=1}^{n} x_i^q y_i.$$

For every $\alpha \in \mathbb{F}_{q^2}$, $\langle \alpha x, y \rangle_h = \alpha^q \langle x, y \rangle_h = \langle x, \alpha^q y \rangle_h$.

Note that the norm $N : \mathbb{F}_{q^2}^* \to \mathbb{F}_q^*, \omega \to \omega^{q+1}$ is an onto map, see [43, pp. 284 – 291]. Norm of 0 is equal to 0. Also note that since $\omega \mapsto \omega^q$ is a Frobenius automorphism, the equality $\omega^q = \omega$ implies $\omega \in \mathbb{F}_q$.

In [40, Lemma 14 and 18] the authors prove that if the quantum code C is linear, then $C^{\perp_s} = C^{\perp_h}$, where the hermitian orthogonal is defined in a similar way. The set $C^{\perp_h}$ is an $\mathbb{F}_{q^2}$-linear subspace of A^n.

Definition 7.1.2. Let C be a linear quantum code. We say that an $\mathbb{F}_{q^2}$-linear map $f : C^{\perp_h} \to A^n$ is a *quantum isometry*, if

- f is a Hamming isometry on $C^{\perp_h}$.
- f preserves the hermitian orthogonality on C, i.e., for all $x, y \in C$,

$$\langle x, y \rangle_h = 0 \iff \langle f(x), f(y) \rangle_h = 0,$$

Such definition of a quantum isometry represents the fact that a map that preserves a quantum code should preserve its metric parameters, algebraic structure and hermitian self-orthogonality. If f is a linear quantum isometry of a quantum code C, then $f(C)$ is a linear quantum code with the same error-correcting capability.

To study an extension property of quantum codes we need to define a universal group of morphisms that acts on the ambient space and preserves the elements of the category of quantum codes. Unlike the case of classical additive or linear codes we cannot define directly the quantum isometry of an ambient space, since the code $C = A^n$ is not self-orthogonal. That's why we define the universal group of such maps as the set of linear maps $h : A^n \to A^n$ such that for every quantum code $C \subset A^n$, h restricted on C is a quantum isometry. One can easily verify that this set coincides with the set of linear maps $A^n \to A^n$ that preserves the Hamming weight and hermitian orthogonality.

Definition 7.1.3. We say that an $\mathbb{F}_{q^2}$-linear map $h : A^n \to A^n$ is *quantum monomial*, if there exist a permutation $\pi \in \mathfrak{S}_n$ and nonzero scalars $a_1, \ldots, a_n \in \mathbb{F}_{q^2}^*$, with $N(a_i) = N(a_j)$ for all $i, j \in \{1, \ldots, n\}$, such that

$$h(x_1, \ldots, x_n) = \left(a_1 x_{\pi(1)}, \ldots, a_n x_{\pi(n)}\right).$$

The following proposition holds.

Proposition 7.1.1. *An $\mathbb{F}_{q^2}$-linear map $h : A^n \to A^n$ is a Hamming isometry that preserves the hermitian orthogonality on A^n if and only if h is quantum monomial.*

Proof. From the MacWilliams Extension Theorem (see Theorem 2.1.1), h is a linear Hamming isometry if and only if there exist a permutation $\pi \in \mathfrak{S}_n$ and nonzero scalars $a_1, \ldots, a_n \in \mathbb{F}_{q^2}^*$ such that

$$h(x_1, \ldots, x_n) = \left(a_1 x_{\pi(1)}, \ldots, a_n x_{\pi(n)}\right).$$

Calculate,

$$\langle h(x), h(y)\rangle_h = \sum_{i=1}^{n} a_i x_{\pi(i)} a_i^q y_{\pi(i)}^q = \sum_{i=1}^{n} N(a_i)\langle x_{\pi(i)}, y_{\pi(i)}\rangle_h.$$

Put $x = (1, 1, 0, \ldots, 0)$ and $y = (1, -1, 0, \ldots, 0)$. Then $\langle x, y\rangle_h = 0$. Since h preserves hermitian orthogonality, $0 = \langle h(x), h(y)\rangle_h = N(a_{\pi^{-1}(1)}) - N(a_{\pi^{-1}(2)})$. In the same way, for all $i, j \in \{1, \ldots, n\}$, $N(a_i) = N(a_j)$.

Conversely, if h is a quantum monomial map, then,

$$\langle h(x), h(y)\rangle_h = N(a_1)\langle x, y\rangle_h,$$

and hence h preserves hermitian orthogonality. □

Now we can naturally define an extension property for quantum codes.

Definition 7.1.4. We say that an *extension property holds for $\mathbb{F}_{q^2}$-linear quantum codes* if for every $\mathbb{F}_{q^2}$-linear quantum code $C \subset \mathbb{F}_{q^2}^n$ each $\mathbb{F}_{q^2}$-linear quantum isometry f of C extends to a quantum monomial map.

Proposition 7.1.2. *An extension property holds for $\mathbb{F}_4$-linear quantum codes.*

Proof. From the MacWilliams Extension Theorem, a Hamming isometry f extends to a monomial map with a permutation $\pi \in \mathfrak{S}_n$ and nonzero scalars $a_1, \ldots, a_n \in \mathbb{F}_4$. Since $\mathbb{F}_2^* = \{1\}$, $N(a_i) = 1$, for every $i \in \{1, \ldots, n\}$. Thus f extends to a quantum monomial map. □

For $q > 2$ we show that an extension property does not hold.

At first, consider the case $q > 3$. Let $n = 3$ and let $C = \langle (1, x, y)\rangle_{\mathbb{F}_{q^2}}$ be a linear quantum code, where $x, y \in \mathbb{F}_{q^2}^*$, $N(x) \neq -1$ and $N(y) = -1 - N(x)$. Such x and y exist because N is onto. Since,

$$N(1) + N(x) + N(y) = 0,$$

we have $C \subset C^{\perp_h}$. Also, $C^{\perp_h} = \langle (1, x, y), (-x^q, 1, 0)\rangle_{\mathbb{F}_{q^2}}$, because

$$\langle (1, x, y), (-x^q, 1, 0)\rangle_h = -x^{q^2} + x + 0 = -x + x = 0.$$

Define an $\mathbb{F}_{q^2}$-linear map $f : C^{\perp_h} \to \mathbb{F}_{q^2}^3$, as

$$f(1, x, y) = (1, a, b), \quad f(-x^q, 1, 0) = (-x^q, \frac{a}{x}, 0),$$

where $a, b \in \mathbb{F}_{q^2}$ are such that $N(a) \neq 0, -1, N(x)$ and $N(b) = -1 - N(a)$. Such a and b exist because N is onto and $q > 3$. By the construction, f is a linear quantum isometry of C.

Prove that f does not extend to a quantum monomial map by contradiction. Assume that there exist a permutation $\pi \in \mathfrak{S}_3$ and nonzero scalars a_1, a_2, a_3, with $N(a_1) = N(a_2) = N(a_3)$ such that

$$f(x_1, x_2, x_3) = (a_1 x_{\pi(1)}, a_2 x_{\pi(2)}, a_3 x_{\pi(3)}).$$

From the form of f, π is either trivial or $\pi = (12)(3)$. If π is trivial, then $a_1 = 1$, $a_2 = \frac{a}{x}$ and $a_3 = \frac{b}{y}$. Thus, $1 = N(1) = N(a_2) = N(a)/N(x)$, which means $N(a) = N(x)$ that contradicts to the assumption $N(a) \neq N(x)$.

If $\pi = (12)(3)$, then $a_1 = -x^q = \frac{1}{x}$ that leads to $-x^{q+1} = 1$ or the same $N(x) = -1$. But $N(x) \neq -1$, so, from the contradiction, f does not extend to a quantum monomial map.

For the case $q = 3$, define $C = \langle (x, x, x, x, x, x) \rangle_{\mathbb{F}_9}$, where $N(x) = 1$ and define

$$f(x_1, x_2, x_3, x_4, x_5, x_6) = (x_1, x_2, x_3, -x_4, -x_5, -x_6).$$

Hence $f(x, x, x, x, x, x) = (x, x, x, -x, -x, -x)$. One can easily verify that f is a linear quantum isometry of C. However, f does not extend to a quantum monomial map. Indeed, for every permutation we consider, there exist at least two nonzero scalars a_i and a_j that have different values 1 or -1.

7.2 Gabidulin codes

We finish this chapter observing the rank weight, for which the results of Chapter 5 do not apply.

Let $\mathbb{F}_q$ be a finite field and let $\mathbb{F}_{q^m}$ be a finite field extension of $\mathbb{F}_q$ of order m. On $\mathbb{F}_{q^m}$ we consider a structure of an m-dimensional $\mathbb{F}_q$-linear vector space by fixing a basis $u_1, \ldots, u_m \in \mathbb{F}_{q^m}$. Let n be a positive integer and let $(x_1, \ldots, x_n)$ be a vector in $\mathbb{F}_{q^m}^n$. For every $i \in \{1, \ldots, m\}$ the element x_i has the expansion in the basis $x_i = a_{1i}u_1 + \cdots + a_{mi}u_m$. The *rank weight* is a function $\mathrm{wt}_R : \mathbb{F}_{q^m}^n \to \{0, \ldots, \min(n, m)\}$ defined as the maximum number of $\mathbb{F}_q$-linearly independent coordinates, or equivalently, as the rank of the following matrix,

$$\mathrm{wt}_R(x_1, \ldots, x_n) = \mathrm{rank} \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}.$$

We observe $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$ with the rank metric. Such codes are called the Gabidulin codes. The theory of rank metric codes was introduced in [30].

In the group $\mathrm{GL}_n(\mathbb{F}_{q^m}) \cong \mathrm{Aut}_{\mathbb{F}_{q^m}}(\mathbb{F}_{q^m}^n)$ we distinguish the subgroup G generated by two subgroups: $\{xI_n \mid x \in \mathbb{F}_{q^m}^*\}$ and $\mathrm{GL}_n(\mathbb{F}_q)$. The weight preserving maps of the ambient space are described in the following theorem.

Theorem 7.2.1 (see [6]). *A map $f : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^n$ is an $\mathbb{F}_{q^m}$-linear wt_R-preserving map if and only if $f \in G$.*

To describe extension properties of Gabidulin codes we cannot directly use the results of Chapter 5 for general weight function. The main reason is that the rank weight does not splits in the sum of weights of coordinates, i.e.,

$$\mathrm{wt}_R(x_1, \ldots, x_n) \neq \mathrm{wt}_R(x_1) + \cdots + \mathrm{wt}_R(x_n),$$

in general, where $x_i \in \mathbb{F}_{q^m}$. The same holds, for example, for the poset weight and the Rosenbloom-Tsfasman weight.

However, we can put the alphabet A to be equal $\mathbb{F}_{q^m}^n$ and in such a way consider all Gabidulin codes as $R = \mathbb{F}_{q^m}$-linear codes over the alphabet $A = \mathbb{F}_{q^m}^n$ of length one. This is the case of the vector space alphabet. Then, from Theorem 7.2.1 the symmetry group of the rank weigh $\mathrm{wt}_R : A \to \mathbb{Q}$, $U(\mathrm{wt}_R) = G$, which particularly means that the defined group G is closed with respect to the action on $\mathbb{F}_{q^m}^n$.

Proposition 7.2.1. *An extension theorem holds for Gabidulin codes, i.e., for every $\mathbb{F}_{q^m}$-linear code $C \subseteq \mathbb{F}_{q^m}^n$ each $\mathbb{F}_{q^m}$-linear wt_R-preserving map $f : C \to \mathbb{F}_{q^m}^n$ extends to an element of G, if and only if the $\mathbb{F}_{q^m}$-linear vector space $\mathbb{F}_{q^m}^n$ is G-pseudo-injective.*

Proof. It is clear that the map $f : C \to A$ is a wt_R-preserving map if and only if f is a swc_G-preserving map. The statement follows from Proposition 5.3.2. □

For the moment we cannot give positive or negative answer on the question if an extension property holds for the Gabidulin codes. One can notice that similar characterization of an extension properties in terms of G-pseudo-injectivity can be obtained for arbitrary module alphabets equipped with general weights as long as the symmetry group of the weight on the full R-module A^n is known.

In particular, if the alphabet A is a vector space the problem is related to G-pseudo-injectivity of vector spaces.

8. ISOMETRY GROUPS OF COMBINATORIAL CODES

A group of isometries of a classical linear code is the group of those linear bijections from the code to itself that preserve the Hamming distance. In particular, from the classical MacWilliams Extension Theorem (see Theorem 2.1.1) it follows that each isometry of a linear code to itself extends to a monomial map.

As it is discussed in previous chapters, for linear codes over module alphabets an analogue of the MacWilliams Extension Theorem does not hold in general. This means that there exist codes with isometries to itself that do not extend to monomial maps (see Example 4.2.1). In the context of combinatorial codes, that is, codes without any algebraic structure, the situation is similar, see [4, 41, 55].

Along with the group of isometries of a code we observe the subgroup of those isometries that extend to monomial maps. Except the case of classical linear codes, the two groups may not be the same.

In [62] and [68] Wood investigated the question of how different the two groups of a linear code over a matrix module alphabet can be. He showed, under certain assumptions, that there exists a linear code over a matrix module alphabet with predefined group of isometries and group of monomial isometries. In this chapter we prove a similar statement for combinatorial codes.

8.1 Preliminaries

Recall the context of combinatorial codes. Let A be a finite set alphabet and let n be a positive integer. The map $\rho_H : A^n \times A^n \to \{0, \dots, n\}$ denotes the Hamming distance. A map $h : A^n \to A^n$ is called monomial if there exists a permutation $\pi \in \mathfrak{S}_n$ and permutations $\sigma_1, \dots, \sigma_n \in \mathfrak{S}(A)$ such that for each $a \in A^n$,

$$h(a) = \big(\sigma_1(a_{\pi(1)}), \dots, \sigma_n(a_{\pi(n)})\big) .$$

Let $C \subseteq A^n$ be a code with $m \geq 3$ codewords. Consider the message set $M = \{1, \dots, m\}$, and consider an encoding map $\lambda : M \to A^n$ of the code C, that is, an injective map such that $\lambda(M) = C$. For every $g \in \mathfrak{S}(M)$ the map $\lambda g \lambda^{-1} : C \to C$ is a well-defined bijection.

Definition 8.1.1. The *group of isometries* of C is the set

$$\mathrm{Iso}(C) := \{g \in \mathfrak{S}(M) \mid \lambda g \lambda^{-1} \text{ is a Hamming isometry}\},$$

and the *group of monomial isometries* of C is the set

$$\mathrm{Mon}(C) := \{g \in \mathfrak{S}(M) \mid \lambda g \lambda^{-1} \text{ extends to a monomial map}\}.$$

The group $\mathrm{Mon}(C)$ is a subgroup of $\mathrm{Iso}(C)$ since every monomial map is a Hamming isometry.

Remark 8.1.1. In coding theory the notion of the automorphism group $\mathrm{Aut}(C)$ of those monomial maps that preserve C is often used. The set of all monomial maps of A^n form a group, which is isomorphic to the wreath product $\mathfrak{S}_n \wr \mathfrak{S}(A)$, see [17, Section 2.6]. Note that $\mathrm{Mon}(C)$ and $\mathrm{Aut}(C)$ are different objects: $\mathrm{Mon}(C)$ is a subgroup of $\mathfrak{S}(M)$ and $\mathrm{Aut}(C)$ is a subgroup of the full group of monomial maps. However, there exists a connection. For a monomial map $h \in \mathrm{Aut}(C)$ the map $\lambda^{-1}h\lambda$ is in $\mathrm{Iso}(C)$. By defining the map $\mathrm{restr} : \mathrm{Aut}(C) \to \mathrm{Iso}(C), h \mapsto \lambda^{-1}h\lambda$, we have the equality of groups $\mathrm{Mon}(C) = \mathrm{restr}(\mathrm{Aut}(C))$. The groups $\mathrm{Mon}(C)$ and $\mathrm{Aut}(C)$ are isomorphic unless the homomorphism restr has a nontrivial kernel. The last holds if and only if the code has two columns that differ by a permutation of the alphabet.

From Theorem 2.1.2, $\mathrm{Iso}(A^n) = \mathrm{Mon}(A^n)$. However, in general, for codes in A^n the equality of the groups does not hold.

Example 8.1.1. Suppose $A = \{0, 1\}$, $M = \{1, \ldots, 5\}$. Consider the code C of cardinality 5 in A^4,

$$C = \{(0,0,0,0), (1,1,0,0), (1,0,1,0), (1,0,0,1), (0,1,1,0)\},$$

where the encoding map $\lambda : M \to C$ is defined in the presented order. The group $\mathrm{Iso}(C) < \mathfrak{S}_5$ is generated by the cycles (12), (123) and (4, 5) and has 12 elements. From the other side, $\mathrm{Mon}(C)$ is a subgroup of $\mathrm{Iso}(C)$ generated by permutations (12) and (123). For example, denoting $g_0 = (45) \in \mathrm{Iso}(C)$, the map $\lambda g_0 \lambda^{-1}$ is an isometry of C that does not extend to a monomial map,

$$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array} \xrightarrow{\lambda g_0 \lambda^{-1}} \begin{array}{cccc} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{array}.$$

Indeed, one can easily check that $\lambda g_0 \lambda^{-1} : C \to C$ is a Hamming isometry. Also, the fourth column from the right hand side has equal first four elements, but there is no such column from the left hand side. Hence, the code isomorphism $\lambda g_0 \lambda^{-1}$ does not extend to a monomial map.

Therefore, $\mathrm{Mon}(C) \neq \mathrm{Iso}(C)$. Note that the group $\mathrm{Aut}(C)$ is generated by two elements. One acts by swapping the second and the third column of C and another acts by inverting the symbols in the first two columns and then swapping the first two columns. Both groups $\mathrm{Aut}(C)$ and $\mathrm{Mon}(C)$ have 6 elements and are isomorphic to the symmetric group $\mathfrak{S}_3$.

There exist more complex examples. Recall that a code $C \subseteq A^n$ is an (n, K, d) q-ary code if it has cardinality K, minimum distance d and the alphabet has q elements. According to [55], if C is $(q, q^2, q-1)$ or $(q+1, q^2, q)$ q-ary MDS code with $q \neq 2$, then $|\mathrm{Iso}(C)| > |\mathrm{Mon}(C)|$, and thus $\mathrm{Iso}(C) \neq \mathrm{Mon}(C)$. The same holds, for example, for $(q, (q-1)^2, q-1)$ q-ary equidistant codes, where $q \geq 5$ and both q and $q-1$ are prime powers (see [41]).

8.2 Main result

Let q denote the cardinality of the alphabet A, $q \geq 2$. Recall that $M = \{1, \ldots, m\}$. Consider the set $\mathcal{P}$ of all the partitions of the set M that have at most q classes,

$$\mathcal{P} := \big\{\{c_1, \ldots, c_t\} \mid c_1 \sqcup \cdots \sqcup c_t = M, \;\; t \leq q\big\},$$

where $c_i \subseteq M$, for $i \in \{1, \ldots, t\}$, and $\sqcup$ denotes the disjoint union of sets.

The canonical action of the group $\mathfrak{S}(M)$ on the set $\mathcal{P}$ is defined in the following way, for $g \in \mathfrak{S}(M)$, for $\alpha = \{c_1, \ldots, c_t\} \in \mathcal{P}$,

$$g(\alpha) := \{g(c_1), \ldots, g(c_t)\}.$$

In $\mathcal{P}$ we distinguish a subset

$$\mathcal{P}_2 := \Big\{\big\{\{i, j\}, \{M \setminus \{i, j\}\}\big\} \;\Big|\; i \neq j \in M\Big\}.$$

Since each partition in $\mathcal{P}_2$ has two classes, which is not greater than q, $\mathcal{P}_2 \subset \mathcal{P}$. The group $\mathfrak{S}(M)$ naturally acts on $\mathcal{P}_2$ and $\mathcal{P} \setminus \mathcal{P}_2$. The main result of this chapter follows.

Theorem 8.2.1 (see [20])**.** *Let m be a positive integer, $m \geq 5$ or $m = 3$. Let A be a finite set alphabet and let C be a code over the alphabet A of cardinality m. The following statements hold.*

(i) The group $\mathrm{Iso}(C) \leq \mathfrak{S}(M)$ *is closed with respect to the action on* $\mathcal{P}_2$*.*

(ii) The group $\mathrm{Mon}(C)$ *is equal to an intersection of* $\mathrm{Iso}(C)$ *with a subgroup of* $\mathfrak{S}(M)$ *that is closed with respect to the action on* $\mathcal{P} \setminus \mathcal{P}_2$*.*

(iii) For each subgroup $H_1 \leq \mathfrak{S}(M)$ that is closed with respect to the action on $\mathcal{P} \setminus \mathcal{P}_2$, for each subgroup $H_2 \leq \mathfrak{S}(M)$ that is closed with respect to the action on $\mathcal{P}_2$, there exists a code C of cardinality m such that

$$\mathrm{Mon}(C) = H_1 \cap \mathrm{Iso}(C) \quad \textit{and} \quad \mathrm{Iso}(C) = H_2.$$

From the fact that, for $m \geq 5$, the trivial subgroup $\{e\}$ and the full group $\mathfrak{S}(M)$ are closed with respect to the action on $\mathcal{P} \setminus \mathcal{P}_2$ and $\mathcal{P}_2$ respectively, we get the first corollary.

Corollary 8.2.1. *For every integer $m \geq 5$, there exists a code C of cardinality m with the maximal group* $\mathrm{Iso}(C) = \mathfrak{S}(M)$ *and the minimal group* $\mathrm{Mon}(C) = \{e\}$*.*

Remark 8.2.1. For the case $m = 3$, $\mathcal{P} \setminus \mathcal{P}_2$ has two partitions: $\{\{1, 2, 3\}\}$ and $\{\{1\}, \{2\}, \{3\}\}$. The trivial group $\{e\}$ fixes both of them, but also so does every permutation in $\mathfrak{S}_3$ and hence $\{e\}$ is not closed with respect to the action on $\mathcal{P} \setminus \mathcal{P}_2$.

By using Theorem 8.2.1 (iii) with $H_1 = \mathfrak{S}(M)$, which is closed with respect to the action on $\mathcal{P} \setminus \mathcal{P}_2$, we get the second corollary.

Corollary 8.2.2. *For every integer $m \geq 5$ or $m = 3$, for each subgroup $H \leq \mathfrak{S}(M)$ that is closed with respect to the action on $\mathcal{P}_2$, there exists a code C of cardinality m such that the groups* $\mathrm{Mon}(C)$ *and* $\mathrm{Iso}(C)$ *coincide and are both equal to H.*

Example 8.2.1. For $m = 5$ and $q = 2$, consider the code C of the following form.

0	0	1	2	3	4	6	5	4	3	4	3	2	2	1	0
0	1	0	0	0	0	1	1	1	1	0	0	0	0	0	0
0	0	1	0	0	0	1	0	0	0	1	1	1	0	0	0
0	0	0	1	0	0	0	1	0	0	1	0	0	1	1	0
0	0	0	0	1	0	0	0	1	0	0	1	0	1	0	1
0	0	0	0	0	1	0	0	0	1	0	0	1	0	1	1

The numbers over the header line represent the number of occurrences of the column under the line in the code. For instance, in this example, the third column appears once in the code, the fourth column appears twice in the code and the second column does not appear anywhere in the code.

We indicated several columns that does not appear in the code for the completeness. In fact, all possible columns (up to a permutation of the alphabet) are presented in the table. The vertical lines separate the columns with different numbers of 1s.

One can check that the code C is a $(40, 5, 22)$ equidistant binary code with the maximal group of isometries $\mathrm{Iso}(C) = \mathfrak{S}(M)$ and the minimal group of monomial isometries $\mathrm{Mon}(C) = \{e\}$.

Remark 8.2.2. In general, for $m \geq 5$, there is no direct relation between the subgroups of $\mathfrak{S}(M)$ closed with respect to the action on $\mathcal{P}_2$ and $\mathcal{P} \setminus \mathcal{P}_2$. There exists a subgroup that is closed with respect to the action on $\mathcal{P} \setminus \mathcal{P}_2$ but not closed with respect to the action on $\mathcal{P}_2$. For example, if $m = 5$, $q = 3$ and the group is $G = \langle (12)(34), (12)(35) \rangle < \mathfrak{S}_5$. There also exists a subgroup that is closed with respect to the action on $\mathcal{P}_2$ but not closed with respect to the action on $\mathcal{P} \setminus \mathcal{P}_2$. Consider $m = 5$, $q = 2$ and $G = \langle (12)(34) \rangle < \mathfrak{S}_5$.

For codes with $m = 4$ codewords the statement of the theorem does not hold in general and needs to be refined. This case is observed in Section 8.5. The proof of the main result is given in the next sections.

8.3 Auxiliary results

8.3.1 Multiplicity function

Recall that for sets X, Y, let $\mathrm{F}(X, Y)$ denote the set of all maps from X to Y. Consider the map $\Psi : \mathrm{F}(M, A) \to \mathcal{P}$,

$$x \mapsto \Psi(x) := \{x^{-1}(a) \mid a \in A\} \setminus \{\emptyset\}.$$

The number of classes in $\Psi(x)$ is at most $|A| = q$, so $\Psi(x) \in \mathcal{P}$ and hence the map is defined.

Recall that $\lambda : M \to A^n$ is an encoding map of C. Let $\lambda_k : M \to A$ denote the projection of λ on kth coordinate for $k \in \{1, \ldots, n\}$. Define the *multiplicity function* $\eta_\lambda \in \mathrm{F}(\mathcal{P}, \mathbb{Q})$, as follows, for $\alpha \in \mathcal{P}$,

$$\eta_\lambda(\alpha) := |\{k \mid \Psi(\lambda_k) = \alpha\}|.$$

Proposition 8.3.1. *For every non-zero function $\eta \in \mathrm{F}(\mathcal{P}, \mathbb{Q})$ with nonnegative integer values there exist a positive integer n and a map $\lambda : M \to A^n$, such that $\eta_\lambda = \eta$. If $\mathcal{P}_2$ is a subset of the support of η, then such map λ is injective.*

Proof. Define $n = \sum_{\alpha \in \mathcal{P}} \eta(\alpha)$ and let $\alpha_1, \ldots, \alpha_n \in \mathcal{P}$ be the n-tuple of partitions such that for all $\alpha \in \mathcal{P}$,

$$\eta(\alpha) = |\{k \mid \alpha = \alpha_k\}|.$$

Enumerate the elements of the alphabet $A = \{a_1, \ldots, a_q\}$ and fix $k \in \{1, \ldots, n\}$. Let $\alpha_k = \{c_1, \ldots, c_t\}$, for some $t \leq q$. Define the map $\lambda_k \in \mathrm{F}(M, A)$ as

$$\forall i \in \{1, \ldots, t\}, \forall j \in c_i, \;\; \lambda_k(j) = a_i.$$

It is easily seen that $\Psi(\lambda_k) = \alpha_k$. Define $\lambda = (\lambda_1, \ldots, \lambda_n) : M \to A^n$. Then, for all $\alpha \in \mathcal{P}$, $\eta_\lambda(\alpha) = |\{k \mid \Psi(\lambda_k) = \alpha\}| = |\{k \mid \alpha_k = \alpha\}| = \eta(\alpha)$.

Assume that λ is not injective. Then there exist $i \neq j \in M$ such that $\lambda(i) = \lambda(j)$, or equivalently, for all $k \in \{1, \ldots, n\}$, $\lambda_k(i) = \lambda_k(j)$. This means that for all $k \in \{1, \ldots, n\}$, i and j belong to the same class of α_k. The partition $\alpha' = \{\{i, i'\}, M \setminus \{i, i'\}\} \in \mathcal{P}_2$ has i and j in different classes, where $i' \in M \setminus \{i, j\} \neq \emptyset$. Since $\mathcal{P}_2$ is a subset of the support of η, there exists $k' \in \{1, \ldots, n\}$ such that $\alpha_{k'} = \alpha'$. From the contradiction, λ is injective. □

Note that the set $\mathcal{P}_2$ in the statement of the proposition can be replaced, for example, by a smaller set of partitions of the form $\{\{i\}, M \setminus \{i\}\}$, $i \in M$, or any other set that satisfies the property observed in the proof. We use the already defined set $\mathcal{P}_2$ in order to avoid new notations.

8.3.2 Extension criterion and stabilizers

Let $\mathcal{O}$ denote the set of pairs of elements of M,

$$\mathcal{O} := \big\{\{i, j\} \;\big|\; \{i, j\} \subset M\big\}.$$

The group $\mathfrak{S}(M)$ acts on $\mathcal{O}$ in the following way, for $g \in \mathfrak{S}(M)$,

$$g(\{i, j\}) := \{g(i), g(j)\}.$$

Consider the action of $\mathfrak{S}(M)$ on the vector spaces $\mathrm{F}(\mathcal{P}, \mathbb{Q})$ and $\mathrm{F}(\mathcal{O}, \mathbb{Q})$, so that, for $g \in \mathfrak{S}(M)$, $\eta \in \mathrm{F}(\mathcal{P}, \mathbb{Q})$ and $\alpha \in \mathcal{P}$,

$$g(\eta)(\alpha) := \eta(g^{-1}(\alpha)),$$

and for $x \in \mathrm{F}(\mathcal{O}, \mathbb{Q})$ and $p \in \mathcal{O}$,

$$g(x)(p) := x(g^{-1}(p)).$$

The group $\mathfrak{S}(M)$ acts on the vector spaces by automorphisms, i.e., a map $\phi : V \to V$, associated to the action of g on V, is a $\mathbb{Q}$-linear bijection, where V is either $\mathrm{F}(\mathcal{P}, \mathbb{Q})$ or $\mathrm{F}(\mathcal{O}, \mathbb{Q})$.

For $\alpha \in \mathcal{P}$ and $p = \{i, j\} \in \mathcal{O}$, define the function $\Delta_\alpha \in \mathrm{F}(\mathcal{O}, \mathbb{Q})$ as

$$\Delta_\alpha(p) := \begin{cases} 0, & \text{if } i \text{ and } j \text{ belong to the same class in } \alpha; \\ 1, & \text{otherwise.} \end{cases}$$

Consider the $\mathbb{Q}$-linear map,

$$W : \mathrm{F}(\mathcal{P}, \mathbb{Q}) \to \mathrm{F}(\mathcal{O}, \mathbb{Q}), \quad W(\eta)(p) := \sum_{\alpha \in \mathcal{P}} \eta(\alpha)\Delta_\alpha(p),$$

where $\eta \in \mathrm{F}(\mathcal{P}, \mathbb{Q})$, $p \in \mathcal{O}$. A similar map was observed in [66, 67].

Proposition 8.3.2. *A map $f : C \to A^n$ is a Hamming isometry if and only if $W(\eta_\lambda) = W(\eta_{f\lambda})$. The map f extends to a monomial map if and only if $\eta_\lambda = \eta_{f\lambda}$.*

Proof. Calculate the Hamming distance, for all $p = \{i, j\} \in \mathcal{O}$,

$$\begin{aligned} \rho_H(\lambda(i), \lambda(j)) &= |\{k \mid \lambda_k(i) \neq \lambda_k(j)\}| \\ &= |\{k \mid \Delta_{\Psi(\lambda_k)}(p) = 1\}| \\ &= \sum_{\alpha \in \mathcal{P}} |\{k \mid \Psi(\lambda_k) = \alpha\}| \Delta_\alpha(p) \\ &= \sum_{\alpha \in \mathcal{P}} \eta_\lambda(\alpha)\Delta_\alpha(p) = W(\eta_\lambda)(p). \end{aligned}$$

The map f is a Hamming isometry if and only if for all $\{i, j\} \subset M$,

$$\rho_H(\lambda(i), \lambda(j)) = \rho_H(f\lambda(i), f\lambda(j)),$$

which is equivalent to the equality $W(\eta_\lambda) = W(\eta_{f\lambda})$.

The map f extends to a monomial map if and only if there exist a permutation $\pi \in \mathfrak{S}_n$ and permutations $\sigma_1, \ldots, \sigma_n \in \mathfrak{S}(A)$ such that $f\lambda_k = \sigma_k \lambda_{\pi(k)}$, for all $k \in \{1, \ldots, n\}$.

It is an easy exercise to verify that $\Psi(x) = \Psi(y)$ for two maps $x, y \in \mathrm{F}(M, A)$, if and only if there exists a permutation $\sigma \in \mathfrak{S}(A)$ such that $\sigma x = y$.

If f extends to a monomial map, then for all $\alpha \in \mathcal{P}$,

$$\begin{aligned} \eta_{f\lambda}(\alpha) &= |\{k \mid \Psi(f\lambda_k) = \alpha\}| \\ &= |\{k \mid \Psi(\sigma_k \lambda_{\pi(k)}) = \alpha\}| \\ &= |\{k \mid \Psi(\lambda_{\pi(k)}) = \alpha\}| = \eta_\lambda(\alpha). \end{aligned}$$

Conversely, let $\eta_{f\lambda} = \eta_\lambda$. Then for all $\alpha \in \mathcal{P}$ the cardinality of sets $X_\alpha = \{k \mid \Psi(\lambda_k) = \alpha\}$ and $Y_\alpha = \{k \mid \Psi(f\lambda_k) = \alpha\}$ are equal. The set $\{1, \ldots, n\}$ is then a disjoint union of the subsets X_α for $\alpha \in \mathcal{P}$. It is also equal to a disjoint union of the subsets Y_α for $\alpha \in \mathcal{P}$. Thus, there exists $\pi \in \mathfrak{S}_n$ such that for all $\alpha \in \mathcal{P}$, $\pi(X_\alpha) = Y_\alpha$. Therefore, for all $k \in \{1, \ldots, n\}$, $\Psi(\lambda_{\pi(k)}) = \Psi(f\lambda_k)$. From this, for every $k \in \{1, \ldots, n\}$ there exists $\sigma_k \in \mathfrak{S}(A)$ such that $\sigma_k \lambda_{\pi(k)} = f\lambda_k$, which means that f extends to a monomial map. □

For a map $\eta \in \mathrm{F}(\mathcal{P}, \mathbb{Q})$ define two stabilizers,

$$\mathrm{Stab}(\eta) := \{g \in \mathfrak{S}(M) \mid g(\eta) = \eta\},$$
$$\mathrm{Stab}_W(\eta) := \{g \in \mathfrak{S}(M) \mid W(g(\eta)) = W(\eta)\}.$$

Proposition 8.3.3. *If C is a code with an encoding map $\lambda : M \to A^n$, then*

$$\mathrm{Mon}(C) = \mathrm{Stab}(\eta_\lambda), \quad \mathrm{Iso}(C) = \mathrm{Stab}_W(\eta_\lambda).$$

Proof. For all $g \in \mathfrak{S}(M)$, for all $\alpha \in \mathcal{P}$,

$$\begin{aligned}\eta_{\lambda g}(\alpha) &= |\{k \mid \Psi(\lambda_k g) = \alpha\}| \\ &= |\{k \mid \Psi(\lambda_k) = g^{-1}(\alpha)\}| \\ &= \eta_\lambda(g^{-1}(\alpha)) = g(\eta_\lambda)(\alpha).\end{aligned}$$

The statement of the proposition follows directly from Proposition 8.3.2 applied for the map $\lambda g \lambda^{-1} : C \to A^n$. □

8.3.3 Two matrices

For two pairs $p, t \in \mathcal{O}$, the intersection $p \cap t \subset M$ can have at most 2 elements. On $\mathcal{O}$ fix an order. Let B be the $|\mathcal{O}| \times |\mathcal{O}|$ matrix defined over $\mathbb{Q}$ and indexed by the elements of $\mathcal{O}$. For $p, t \in \mathcal{O}$,

$$B_{p,t} := \begin{cases} 1, & \text{if } |p \cap t| = 1; \\ 0, & \text{if } |p \cap t| \neq 1. \end{cases}$$

Let $m \geq 5$ or $m = 3$. Define the $|\mathcal{O}| \times |\mathcal{O}|$ matrix D as follows, for $p, t \in \mathcal{O}$,

$$2(m-2)(m-4) \times D_{p,t} := \begin{cases} -m^2 + 8m - 14, & \text{if } |p \cap t| = 2 \ (\iff p = t); \\ m - 4, & \text{if } |p \cap t| = 1; \\ -2, & \text{if } |p \cap t| = 0 \ (\iff p \cap t = \emptyset). \end{cases}$$

Lemma 8.3.1. *If $m \geq 5$ or $m = 3$, then $BD = DB = I$, where I is the identity $|\mathcal{O}| \times |\mathcal{O}|$ matrix.*

Proof. For $p, t \in \mathcal{O}$,

$$(BD)_{p,t} = \sum_{r \in \mathcal{O}} B_{p,r} D_{r,t} = B_{p,t} D_{t,t} + \sum_{\substack{|r \cap p| = 1 \\ |r \cap t| = 1}} D_{r,t} + \sum_{\substack{|r \cap p| = 1 \\ |r \cap t| = 0}} D_{r,t}.$$

If $p = t$, then

$$(BD)_{p,p} = 0 + \sum_{|r\cap p|=1} D_{r,p} + 0 = \frac{1}{2(m-2)}|\{r \in \mathcal{O} \mid |r \cap p| = 1\}| = 1.$$

If $|p \cap t| = 1$, then

$$\begin{aligned}(BD)_{p,t} = \frac{-m^2+8m-14}{2(m-2)(m-4)} &+ \frac{1}{2(m-2)}|\{r \in \mathcal{O} \mid |r \cap p| = 1;\ |r \cap t| = 1\}| \\ &+ \frac{-1}{(m-2)(m-4)}|\{r \in \mathcal{O} \mid |r \cap p| = 1;\ |r \cap t| = 0\}| \\ &= \frac{-m^2+8m-14}{2(m-2)(m-4)} + \frac{1}{2(m-2)}(m-2) \\ &+ \frac{-1}{(m-2)(m-4)}(m-3) = 0.\end{aligned}$$

If $|p \cap t| = 0$, then

$$\begin{aligned}(BD)_{p,t} &= 0 + \frac{1}{2(m-2)}|\{r \in \mathcal{O} \mid |r \cap p| = 1;\ |r \cap t| = 1\}| \\ &+ \frac{-1}{(m-2)(m-4)}|\{r \in \mathcal{O} \mid |r \cap p| = 1;\ |r \cap t| = 0\}| \\ &= \frac{4}{2(m-2)} + \frac{-1}{(m-2)(m-4)}2(m-4) = 0.\end{aligned}$$

Hence, $BD = I$, the matrices B and D are invertible and $B^{-1} = D$. □

8.3.4 Properties of the map W

For a partition $\alpha \in \mathcal{P}$ let $\mathbb{1}_\alpha \in \mathrm{F}(\mathcal{P}, \mathbb{Q})$ be the map defined as follows, for $\beta \in \mathcal{P}$,

$$\mathbb{1}_\alpha(\beta) := \begin{cases} 1, & \text{if } \beta = \alpha; \\ 0, & \text{if } \beta \neq \alpha. \end{cases}$$

Note that, for a partition $\alpha \in \mathcal{P}$,

$$W(\mathbb{1}_\alpha) = \sum_{\beta\in\mathcal{P}} \mathbb{1}_\beta(\alpha)\Delta_\beta = \Delta_\alpha. \tag{8.1}$$

From now we assume that $m \geq 5$ or $m = 3$. For every map $x \in \mathrm{F}(\mathcal{O}, \mathbb{Q})$ define the map in $\mathrm{F}(\mathcal{P}, \mathbb{Q})$,

$$\xi_x := \sum_{r\in\mathcal{O}} x(r) \sum_{p\in\mathcal{O}} D_{r,p}\mathbb{1}_{\{p,M\setminus p\}},$$

where D is the matrix defined previously. Using Lemma 8.3.1, for $x \in \mathrm{F}(\mathcal{O}, \mathbb{Q})$ and $t \in \mathcal{O}$,

$$\begin{aligned} W(\xi_x)(t) &\overset{(8.1)}{=} \sum_{r\in\mathcal{O}} x(r) \sum_{p\in\mathcal{O}} D_{r,p}\Delta_{\{p,M\setminus p\}}(t) \\ &= \sum_{r\in\mathcal{O}} x(r) \sum_{p\in\mathcal{O}} D_{r,p}B_{p,t} = \sum_{r\in\mathcal{O}} x(r)(DB)_{r,t} = x(t). \end{aligned} \tag{8.2}$$

For every $\alpha \in \mathcal{P} \setminus \mathcal{P}_2$ define the function in $\mathrm{F}(\mathcal{P}, \mathbb{Q})$,

$$\zeta_\alpha := \mathbb{1}_\alpha - \xi_{\Delta_\alpha}.$$

Recall that for a partition $\alpha \in \mathcal{P}$, the function Δ_α is in $\mathrm{F}(\mathcal{O}, \mathbb{Q})$. For $\alpha \in \mathcal{P}$,

$$W(\zeta_\alpha) \overset{(8.1)}{=} \Delta_\alpha - W(\xi_{\Delta_\alpha}) \overset{(8.2)}{=} \Delta_\alpha - \Delta_\alpha = 0. \tag{8.3}$$

Consider the subspace V_0 of $\mathrm{F}(\mathcal{P}, \mathbb{Q})$ of those functions that take zero values on the partitions in $\mathcal{P} \setminus \mathcal{P}_2$ (i.e., functions that have the support in $\mathcal{P}_2$),

$$V_0 := \{\eta \in \mathrm{F}(\mathcal{P}, \mathbb{Q}) \mid \forall \alpha \in \mathcal{P} \setminus \mathcal{P}_2,\ \eta(\alpha) = 0\}.$$

The subspace V_0 is the image of the canonical embedding of $\mathrm{F}(\mathcal{P}_2, \mathbb{Q})$ into $\mathrm{F}(\mathcal{P}, \mathbb{Q})$.

Proposition 8.3.4. *If $m \geq 5$ or $m = 3$, then $\mathrm{F}(\mathcal{P}, \mathbb{Q}) = V_0 \oplus \ker W$.*

Proof. From eq. (8.2), the map $\xi_x \in \mathrm{F}(\mathcal{P}, \mathbb{Q})$ is a pre-image of a map $x \in \mathrm{F}(\mathcal{O}, \mathbb{Q})$ under the map W, and hence $W : \mathrm{F}(\mathcal{P}, \mathbb{Q}) \to \mathrm{F}(\mathcal{O}, \mathbb{Q})$ is onto. The dimension of the kernel of W is equal to $|\mathcal{P}| - |\mathcal{O}| = |\mathcal{P}| - |\mathcal{P}_2| = |\mathcal{P} \setminus \mathcal{P}_2|$, which is true for $m \neq 4$. Obviously, the maps ζ_α for $\alpha \in \mathcal{P} \setminus \mathcal{P}_2$, are linearly independent over $\mathbb{Q}$ and thus form a basis of $\ker W$: see eq. (8.3). The dimension of V_0 is equal to $|\mathcal{P}_2|$. Also, $\ker W \cap V_0 = \{0\}$. Therefore, $\mathrm{F}(\mathcal{P}, \mathbb{Q}) = V_0 \oplus \ker W$. □

8.4 Proof of the main result

Before starting to prove the main theorem, let us prove several necessary equalities.

For $g \in \mathfrak{S}(M)$ and $p = \{i, j\} \in \mathcal{O}$, the value $g(\Delta_\alpha)(p) = \Delta_\alpha(g^{-1}(p))$ is 0 if $g^{-1}(i)$ and $g^{-1}(j)$ belong to the same class in α, and the value is 1 otherwise. Obviously, $g^{-1}(i)$ and $g^{-1}(j)$ are in the same class of α if and only if i and j are in the same class of $g(\alpha)$. Thus we have the equality

$$\Delta_{g(\alpha)} = g(\Delta_\alpha). \tag{8.4}$$

For $g \in \mathfrak{S}(M)$, for $\eta \in \mathrm{F}(\mathcal{P}, \mathbb{Q})$ and $p \in O$,

$$\begin{aligned} W(g(\eta))(p) &= \sum_{\alpha\in\mathcal{P}} g(\eta)(\alpha)\Delta_\alpha(p) = \sum_{\alpha\in\mathcal{P}} \eta(g^{-1}(\alpha))\Delta_\alpha(p) \\ &= \sum_{\beta\in\mathcal{P}} \eta(\beta)\Delta_{g(\beta)}(p) \overset{(8.4)}{=} \sum_{\beta\in\mathcal{P}} \eta(\beta)\Delta_\beta(g^{-1}(p)) \\ &= W(\eta)(g^{-1}(p)). \end{aligned} \tag{8.5}$$

For $g \in \mathfrak{S}(M)$ and for all $\beta \in \mathcal{P}$, the value $g(\mathbb{1}_\alpha)(\beta) = \mathbb{1}_\alpha(g^{-1}(\beta))$ is 1, if $g(\alpha) = \beta$, and is 0 otherwise. Hence we have the equality

$$g(\mathbb{1}_\alpha) = \mathbb{1}_{g(\alpha)}. \tag{8.6}$$

For $g \in \mathfrak{S}(M)$, for $x \in \mathrm{F}(\mathcal{O}, \mathbb{Q})$,

$$\begin{aligned} g(\xi_x) &= \sum_{r\in\mathcal{O}} x(r) \sum_{p\in\mathcal{O}} D_{r,p}\mathbb{1}_{\{g(p),M\setminus g(p)\}} = \sum_{r\in\mathcal{O}} x(r) \sum_{g^{-1}(p)\in\mathcal{O}} D_{r,g^{-1}(p)}\mathbb{1}_{\{p,M\setminus p\}} \\ &= \sum_{r\in\mathcal{O}} x(r) \sum_{p\in\mathcal{O}} D_{g(r),p}\mathbb{1}_{\{p,M\setminus p\}} = \sum_{g^{-1}(r)\in\mathcal{O}} x(g^{-1}(r)) \sum_{p\in\mathcal{O}} D_{r,p}\mathbb{1}_{\{p,M\setminus p\}} \\ &= \sum_{r\in\mathcal{O}} g(x)(r) \sum_{p\in\mathcal{O}} D_{r,p}\mathbb{1}_{\{p,M\setminus p\}} = \xi_{g(x)}. \end{aligned} \tag{8.7}$$

For $g \in \mathfrak{S}(M)$ and $\alpha \in \mathcal{P}$,

$$g(\zeta_\alpha) = g(\mathbb{1}_\alpha) - g(\xi_{\Delta_\alpha}) = \mathbb{1}_{g(\alpha)} - \xi_{\Delta_{g(\alpha)}} = \zeta_{g(\alpha)}, \tag{8.8}$$

where the equality in the middle holds due to eq. (8.4), eq. (8.6) and eq. (8.7).

Lemma 8.4.1. *If $\eta_0 \in \ker W$ and $\eta_1 \in V_0$, then the equalities hold,*

$$\begin{aligned} \mathrm{Stab}(\eta_0 + \eta_1) &= \mathrm{Stab}(\eta_0) \cap \mathrm{Stab}(\eta_1), \\ \mathrm{Stab}_W(\eta_0 + \eta_1) &= \mathrm{Stab}_W(\eta_1) = \mathrm{Stab}(\eta_1). \end{aligned}$$

Proof. We first show that the spaces $\ker W$ and V_0 are invariant under the action of $\mathfrak{S}(M)$. Indeed, for $g \in \mathfrak{S}(M)$, if $\eta \in \ker W$, then for all $p \in \mathcal{O}$,

$$W(g(\eta))(p) \overset{(8.5)}{=} W(\eta)(g^{-1}(p)) = 0,$$

and hence $g(\eta) \in \ker W$. If $\eta \in V_0$, then for all $\alpha \in \mathcal{P} \setminus \mathcal{P}_2$, $g(\eta)(\alpha) = \eta(g^{-1}(\alpha)) = 0$, and thus $g(\eta) \in V_0$.

Now we prove the first equality. If $g \in \mathrm{Stab}(\eta_0) \cap \mathrm{Stab}(\eta_1)$, then $g(\eta_0) = \eta_0$ and $g(\eta_1) = \eta_1$. Hence $g(\eta_0 + \eta_1) = g(\eta_0) + g(\eta_1) = \eta_0 + \eta_1$ and thus $g \in \mathrm{Stab}(\eta_0 + \eta_1)$. Conversely, if $g \in \mathrm{Stab}(\eta_0 + \eta_1)$, then $g(\eta_0 + \eta_1) = \eta_0 + \eta_1$. Since $g(\eta_0) \in \ker W$ and $g(\eta_1) \in V_0$, by the uniqueness of the decomposition (see Proposition 8.3.4) $g(\eta_0) = \eta_0$ and $g(\eta_1) = \eta_1$, which means $g \in \mathrm{Stab}(\eta_0) \cap \mathrm{Stab}(\eta_1)$. Therefore, $\mathrm{Stab}(\eta_0) \cap \mathrm{Stab}(\eta_1) = \mathrm{Stab}(\eta_0 + \eta_1)$.

The second equality follows from the fact that $W(\eta_0 + \eta_1) = W(\eta_0) + W(\eta_1) = W(\eta_1)$ and for all $g \in \mathfrak{S}(M)$, $W(g(\eta_0+\eta_1)) = W(g(\eta_0)) + W(g(\eta_1)) = W(g(\eta_1))$.

Finally, we prove the third equality. The restriction of W on the subspace V_0 is a bijection by Proposition 8.3.4. If $g \in \mathrm{Stab}_W(\eta_1)$, then $W(g(\eta_1)) = W(\eta_1)$. The map $g(\eta_1)$ is in V_0. Hence, applying W^{-1} to both sides of equality, we get $g(\eta_1) = \eta_1$ and thus $g \in \mathrm{Stab}(\eta_1)$. Since $\mathrm{Stab}(\eta_1) \leq \mathrm{Stab}_W(\eta_1) \leq \mathrm{Stab}(\eta_1)$, we get the third equality in the statement. □

Recall that $\mathcal{P}_2$ is a set of partitions of the form $\{p, M \setminus p\}$, $p \in \mathcal{O}$. Define the map $\mathbb{1}_{\mathcal{P}_2} \in \mathrm{F}(\mathcal{P}, \mathbb{Q})$,

$$\mathbb{1}_{\mathcal{P}_2} = \sum_{\alpha \in \mathcal{P}_2} \mathbb{1}_\alpha.$$

Lemma 8.4.2. *Let $\eta \in \mathrm{F}(\mathcal{P}, \mathbb{Q})$. For all $c \in \mathbb{Q}$,*

$$\begin{aligned} \mathrm{Stab}(\eta) &= \mathrm{Stab}(\eta + c\mathbb{1}_{\mathcal{P}_2}), \\ \mathrm{Stab}_W(\eta) &= \mathrm{Stab}_W(\eta + c\mathbb{1}_{\mathcal{P}_2}). \end{aligned}$$

Proof. For all $g \in \mathfrak{S}(M)$,

$$g(\mathbb{1}_{\mathcal{P}_2}) = \sum_{\alpha \in \mathcal{P}_2} g(\mathbb{1}_\alpha) \overset{(8.6)}{=} \sum_{\alpha \in \mathcal{P}_2} \mathbb{1}_{g(\alpha)} = \sum_{g^{-1}(\alpha) \in \mathcal{P}_2} \mathbb{1}_\alpha = \mathbb{1}_{\mathcal{P}_2}.$$

We prove the second equality of the statement. If $g \in \mathrm{Stab}_W(\eta)$, then

$$\begin{aligned} W(g(\eta + c\mathbb{1}_{\mathcal{P}_2})) &= W(g(\eta) + cg(\mathbb{1}_{\mathcal{P}_2})) = W(g(\eta)) + W(cg(\mathbb{1}_{\mathcal{P}_2})) \\ &= W(\eta) + W(c\mathbb{1}_{\mathcal{P}_2}) = W(\eta + c\mathbb{1}_{\mathcal{P}_2}). \end{aligned}$$

Hence $g \in \mathrm{Stab}_W(\eta + c\mathbb{1}_{\mathcal{P}_2})$ and therefore $\mathrm{Stab}_W(\eta) \subseteq \mathrm{Stab}_W(\eta + c\mathbb{1}_{\mathcal{P}_2})$. From this, $\mathrm{Stab}_W(\eta + c\mathbb{1}_{\mathcal{P}_2}) \subseteq \mathrm{Stab}_W((\eta + c\mathbb{1}_{\mathcal{P}_2}) + (-c)\mathbb{1}_{\mathcal{P}_2})) = \mathrm{Stab}_W(\eta)$. The first equality is proven in the same way. □

Now we are ready to prove the main theorem of the chapter.

Proof of Theorem 8.2.1. Part (i). Let $\lambda \in \mathrm{F}(M, A^n)$ be an encoding map of the code C. From Proposition 8.3.3, we have to show that $\mathrm{Iso}(C) = \mathrm{Stab}_W(\eta_\lambda)$ is closed with respect to the action on $\mathcal{P}_2$. Since the bijection $\mathcal{O} \to \mathcal{P}_2$, $p \mapsto \{p, M \setminus p\}$ preserves the action of the group $\mathfrak{S}(M)$, we have to show that $\mathrm{Stab}_W(\eta_\lambda)$ is closed with respect to the action on $\mathcal{O}$. If $g \in \mathfrak{S}(M)$ preserves the orbits of $\mathrm{Stab}_W(\eta_\lambda)$ on $\mathcal{O}$, then so does g^{-1}, and for all $p \in \mathcal{O}$,

$$W(g(\eta_\lambda))(p) \overset{(8.5)}{=} W(\eta_\lambda)(g^{-1}(p)) = W(\eta_\lambda)(p).$$

Hence $g \in \mathrm{Stab}_W(\eta_\lambda)$, which means that $\mathrm{Stab}_W(\eta_\lambda)$ is closed with respect to the action on $\mathcal{O}$.

Part (ii). Let $\lambda \in \mathrm{F}(M, A^n)$ be an encoding map of the code C. From Proposition 8.3.4, there exists the unique decomposition of the multiplicity function $\eta_\lambda \in \mathrm{F}(\mathcal{P}, \mathbb{Q})$ into the sum of two maps $\eta_0 \in \ker W$ and $\eta_1 \in V_0$ with $\eta_\lambda = \eta_0 + \eta_1$.

From Proposition 8.3.3, $\mathrm{Stab}(\eta_\lambda) = \mathrm{Mon}(C)$ and $\mathrm{Stab}_W(\eta_\lambda) = \mathrm{Iso}(C)$. From Lemma 8.4.1, $\mathrm{Stab}(\eta_\lambda) = \mathrm{Stab}(\eta_0) \cap \mathrm{Stab}_W(\eta_\lambda)$. Finally, we have $\mathrm{Mon}(C) = \mathrm{Stab}(\eta_0) \cap \mathrm{Iso}(C)$.

Let us prove that $\mathrm{Stab}(\eta_0)$ is closed with respect to the action on $\mathcal{P} \setminus \mathcal{P}_2$. Let $g \in \mathfrak{S}(M)$ preserve the orbits of $\mathrm{Stab}(\eta_0)$ acting on $\mathcal{P} \setminus \mathcal{P}_2$. This means

that $\eta_0(\alpha) = \eta_0(g(\alpha))$ for all $\alpha \in \mathcal{P} \setminus \mathcal{P}_2$. Consider the expansion of the map η_0 in the basis ζ_β, $\beta \in \mathcal{P} \setminus \mathcal{P}_2$,

$$\eta_0 = \sum_{\beta \in \mathcal{P} \setminus \mathcal{P}_2} \eta_0(\beta)\zeta_\beta.$$

For $\alpha \in \mathcal{P}$,

$$\begin{aligned} g^{-1}(\eta_0)(\alpha) = \eta_0(g(\alpha)) &= \sum_{\beta \in \mathcal{P} \setminus \mathcal{P}_2} \eta_0(\beta)\zeta_\beta(g(\alpha)) \overset{(8.8)}{=} \sum_{\beta \in \mathcal{P} \setminus \mathcal{P}_2} \eta_0(\beta)\zeta_{g^{-1}(\beta)}(\alpha) \\ &= \sum_{\beta \in \mathcal{P} \setminus \mathcal{P}_2} \eta_0(g(\beta))\zeta_\beta(\alpha) = \sum_{\beta \in \mathcal{P} \setminus \mathcal{P}_2} \eta_0(\beta)\zeta_\beta(\alpha) = \eta_0(\alpha). \end{aligned}$$

Hence $g \in \mathrm{Stab}(\eta_0)$, and therefore $\mathrm{Stab}(\eta_0)$ is closed with respect to the action on $\mathcal{P} \setminus \mathcal{P}_2$.

Part (iii). Let $x \in \mathrm{F}(\mathcal{O}, \mathbb{Q})$ be a function that takes equal values on each orbit and different values on different orbits of H_2 acting on $\mathcal{O}$. From eq. (8.2) and eq. (8.7), $\mathrm{Stab}_W(\xi_x) = \{g \in \mathfrak{S}(M) \mid W(g(\xi_x)) = W(\xi_x)\} = \{g \in \mathfrak{S}(M) \mid g(x) = x\}$. For every $g \in H_2$, $g(x) = x$ and thus $H_2 \subseteq \mathrm{Stab}_W(\xi_x)$. Conversely, if $g \in \mathrm{Stab}_W(\xi_x)$, then $g(x) = x$ and thus g preserves the orbits of H_2. As in the proof of part (i), the group H_2 is closed with respect to the action on $\mathcal{O}$, and hence $g \in H_2$. Finally, $\mathrm{Stab}_W(\xi_x) = H_2$.

Let $\{X_1, \ldots, X_t\}$ be the set of orbits of H_1 acting on the set $\mathcal{P} \setminus \mathcal{P}_2$. Let $c_1, \ldots, c_t \in \mathbb{Q}$ be different nonnegative numbers and define the map

$$\eta_0 = \sum_{i=1}^{t} c_i \sum_{\alpha \in X_i} \zeta_\alpha.$$

For all $g \in H_1$,

$$g(\eta_0) = \sum_{i=1}^{t} c_i \sum_{\alpha \in X_i} g(\zeta_\alpha) \overset{(8.8)}{=} \sum_{i=1}^{t} c_i \sum_{\alpha \in X_i} \zeta_{g(\alpha)} = \sum_{i=1}^{t} c_i \sum_{g^{-1}(\alpha) \in X_i} \zeta_\alpha = \eta_0,$$

and thus $H_1 \leq \mathrm{Stab}(\eta_0)$. Conversely, if $g \in \mathrm{Stab}(\eta_0)$, then, for every $i \in \{1, \ldots, t\}$ and every $\beta \in X_i$, $\eta_0(g^{-1}(\beta)) = g(\eta_0)(\beta) = \eta_0(\beta) = c_i$. Hence $g^{-1}(\beta) \in X_i$ and thus $g^{-1}(X_i) = X_i$. Since H_1 is closed with respect to the action on $\mathcal{P} \setminus \mathcal{P}_2$, we have $g^{-1} \in H_1$ and thus $g \in H_1$. Hence $H_1 = \mathrm{Stab}(\eta_0)$.

Since $\eta_0 \in \ker W$ and $\xi_x \in V_0$, from Lemma 8.4.1, $\mathrm{Stab}_W(\eta_0 + \xi_x) = \mathrm{Stab}_W(\xi_x) = H_2$ and $\mathrm{Stab}(\eta_0 + \xi_x) = \mathrm{Stab}(\eta_0) \cap \mathrm{Stab}_W(\xi_x) = H_1 \cap H_2$.

There exist two nonnegative integers c, c' such that $c'(\eta_0 + \xi_x) + c\mathbb{1}_{\mathcal{P}_2}$ is non-zero, takes nonnegative integer values and its support contains $\mathcal{P}_2$. From Lemma 8.4.2, $\mathrm{Stab}_W(c'(\eta_0 + \xi_x) + c\mathbb{1}_{\mathcal{P}_2}) = \mathrm{Stab}_W(c'(\eta_0 + \xi_x)) = \mathrm{Stab}_W(\eta_0 + \xi_x) = H_2$ and $\mathrm{Stab}(c'(\eta_0 + \xi_x) + c\mathbb{1}_{\mathcal{P}_2}) = \mathrm{Stab}(c'(\eta_0 + \xi_x)) = \mathrm{Stab}(\eta_0 + \xi_x) = H_1 \cap H_2$.

From Proposition 8.3.1, there exists an injective map $\lambda : M \to A^n$ such that $\eta_\lambda = c'(\eta_0 + \xi_x) + c\mathbb{1}_{\mathcal{P}_2}$. Define $C = \lambda(M)$. By Proposition 8.3.3, $\mathrm{Iso}(C) = \mathrm{Stab}_W(\eta_\lambda) = H_2$ and $\mathrm{Mon}(C) = \mathrm{Stab}(\eta_\lambda) = H_1 \cap H_2 = H_1 \cap \mathrm{Iso}(C)$. □

8.5 Codes with 4 elements

There are two main reasons why the general approach fails for $m = 4$. The first reason is that for $m = 4$ the sets $\mathcal{P}_2$ and $\mathcal{O}$ have 3 and 6 elements correspondingly, whereas for $m \geq 5$ or $m = 3$, $|\mathcal{P}_2| = |\mathcal{O}| = \frac{m(m-1)}{2}$, which is crucial in several places in the proof. The second reason is that the matrix B is not invertible and the matrix D is not defined.

However, if $m = 4$ and $q \geq 3$, we still can use the basic idea and an analogue of Theorem 8.2.1 holds. For this, let us make several changes in the text of the chapter. Replace $\mathcal{P}_2$ with

$$\mathcal{P}_2' := \Big\{ \big\{ \{i\}, \{j\}, \{M \setminus \{i,j\}\} \big\} \;\Big|\; \{i,j\} \subset M \Big\}.$$

The set $\mathcal{P}_2'$ is well-defined since each of its elements has 3 classes, which is not greater than q.

Replace the matrices B and D with B' and D', for $p, t \in \mathcal{O}$, where

$$B'_{p,t} := \begin{cases} 1, & \text{if } |p \cap t| \neq 0; \\ 0, & \text{if } |p \cap t| = 0. \end{cases} \qquad D'_{p,t} := \begin{cases} \frac{1}{5}, & \text{if } |p \cap t| \neq 0; \\ -\frac{4}{5}, & \text{if } |p \cap t| = 0. \end{cases}$$

And replace the map ξ_x with

$$\xi'_x := \sum_{p=\{i,j\} \in \mathcal{O}} \sum_{r \in \mathcal{O}} D'_{r,p} x(r) \mathbb{1}_{\{\{i\},\{j\},M\setminus p\}}.$$

In such a way $|\mathcal{P}_2'| = |\mathcal{O}| = 6$ and the bijection $\mathcal{P}_2' \to \mathcal{O}, \{\{i\},\{j\},M\setminus\{i,j\}\} \mapsto \{i,j\}$ preserves the action of the group $\mathfrak{S}_4$. Also, B' is invertible and $B'D' = D'B' = I$, where I is the 6×6 identity matrix.

One can verify that Theorem 8.2.1, all the statements, equalities and proofs remain correct with these changes.

Consider the case $m = 4$ and $q = 2$. The set $\mathcal{P}$ contains 8 partitions and the set $\mathcal{O}$ contains 6 pairs. Fixing bases in $\mathrm{F}(\mathcal{P}, \mathbb{Q})$ and $\mathrm{F}(\mathcal{O}, \mathbb{Q})$, look at the $\mathbb{Q}$-linear map W as the following 6×8 matrix over $\mathbb{Q}$:

$$W = \left(\begin{array}{c|ccc|ccc} 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right).$$

The vertical lines separate the columns labeled by partitions from three different orbits under the action of $\mathfrak{S}_4$ on the set $\mathcal{P}$.

Proposition 8.5.1. *Let C be a binary code with 4 codewords. The groups $\mathrm{Iso}(C) \leq \mathfrak{S}_4$ and $\mathrm{Mon}(C) \leq \mathfrak{S}_4$ are equal and are closed with respect to the action on $\mathcal{O}$. For every subgroup $H \leq \mathfrak{S}_4$ that is closed with respect to the action on $\mathcal{O}$, there exists a binary code C with 4 codewords such that $\mathrm{Iso}(C) = \mathrm{Mon}(C) = H$.*

Proof. It is easy to calculate that $\ker W$ is a subspace of dimension 2 generated by $(1,0,0,0,0,0,0,0)^T$ and $(0,1,1,1,1,-1,-1,-1)^T$. Note that $\ker W$ is invariant under the action of $\mathfrak{S}_4$.

Let $\lambda : M \to \{0,1\}^n$ be an encoding map of C. Assume that $W(\eta_\lambda) = W(\eta_{g\lambda})$, or equivalently, $\eta_\lambda - \eta_{g\lambda} \in \ker W$, for some $g \in \mathfrak{S}_4$. In the proof of Proposition 8.3.3 we showed that $\eta_{g\lambda} = g(\eta_\lambda)$. Then, $24(\eta_\lambda - \eta_{g\lambda}) = \sum_{h\in\mathfrak{S}_4} h(\eta_\lambda - g(\eta_\lambda)) = \sum_{h\in\mathfrak{S}_4} h(\eta_\lambda) - \sum_{h\in\mathfrak{S}_4} h(\eta_\lambda) = 0$. Hence, $W(\eta_\lambda) = W(\eta_{g\lambda})$ implies $\eta_\lambda = \eta_{g\lambda}$ for all $g \in \mathfrak{S}_4$. By Proposition 8.3.2 and Proposition 8.3.3, $\mathrm{Iso}(C) = \mathrm{Mon}(C)$.

The fact that the groups $\mathrm{Iso}(C) = \mathrm{Mon}(C)$ are closed with respect to the action on $\mathcal{O}$ is proven in the same way as in Theorem 8.2.1 (i).

To prove the last statement, for each subgroup of $\mathfrak{S}_4$ closed with respect to the action on $\mathcal{O}$ we give the explicit code construction. Any binary code of cardinality 4, up to a monomial equivalence, has the following form,

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
0	1	0	0	0	1	1	1
0	0	1	0	0	1	0	0
0	0	0	1	0	0	1	0
0	0	0	0	1	0	0	1

,

where $x_1, \ldots, x_8$ are nonnegative integers; see Example 8.2.1 for more details. There exist 7, up to an automorphism of $\mathfrak{S}_4$, non-equivalent subgroups in $\mathfrak{S}_4$ that are closed with respect to the action on $\mathcal{O}$. The groups and corresponding multiplicity functions of the codes are given below.

Group	$\eta_\lambda = (x_1, \ldots, x_8)$
$\{e\}$	(0,1,2,3,4,0,0,0)
$\langle(12)\rangle \cong \mathfrak{S}_2$	(0,1,1,2,3,0,0,0)
$\langle(12),(123)\rangle \cong \mathfrak{S}_3$	(0,1,1,1,2,0,0,0)
$\langle(12),(34)\rangle \cong K_4$	(0,1,1,2,2,0,0,0)
$\langle(12)(34),(13)(24)\rangle \cong K_4$	(0,0,0,0,0,2,1,0)
$\langle(1234),(13)\rangle \cong D_8$	(0,0,0,0,0,1,0,1)
$\mathfrak{S}_4$	(0,1,1,1,1,0,0,0)

□

9. CONCLUSION

Summarizing the work done in my thesis, a new geometric approach for the extension problems in coding theory is introduced. The developed techniques allow to describe a linear code over a module alphabet in terms of configurations of submodules in an ambient module. The usage of this geometric language makes possible to reveal new properties of codes and weight preserving maps.

In particular, I prove an extension theorem for short codes over matrix module alphabets, for a large family of MDS codes, for codes over a PID module alphabet, and also I give alternative proofs for some well-known results in the subject. When an alphabet does not have an extension property, the geometric approach helps to build a code with unextendable isometry or weight preserving map.

A nice example of an unextendable linear code isometry that permutes coordinates of each codeword is given in Chapter 5. To show its existence, geometry, abstract algebra and combinatorics are combined together. The existence of such a code isometry automatically proves several very general properties of extendability of general weight preserving maps.

Another example of connections between linear algebra and combinatorics is given in Chapter 8. Describing a combinatorial code as a point in a vector space, I get the results similar to those obtained by Wood for linear codes. I think that the theory developed in Chapter 8 can be used in its order to improve the original result.

We end this conclusion by proposing several open problems that arose while preparing the present manuscript. The first two sections contain problems with a detailed explanation and some investigations that have not yet give any valuable result. The third section contains a list of other problems related to the subject of the thesis.

9.1 Weight preserving maps of the full space

In Chapter 5 we defined an extension property for a module alphabet equipped with a weight function $\omega : A^n \to \mathbb{Q}^t$ as an extension to a monomial map that preserves the weight ω, i.e., an $U(\omega)$-monomial map. However, it is not mentioned neither in the present thesis nor in other papers on this subject, that the given class of monomial maps is maximal that preserves the weight ω.

For the Hamming weight it is true that every Hamming isometry of the ambient space A^n is a monomial map both for combinatorial and linear cases

(see Theorem 2.1.2 and Proposition 2.1.1). A similar statement holds for the symmetrized weight composition (see Proposition 5.2.1). But it is not always the case for general weight functions. Consider the following example.

Example 9.1.1. Let $m = ab$ be a composite positive integer, where a, b are coprime. Let $\psi : \mathbb{Z}_a \oplus \mathbb{Z}_b \to \mathbb{Z}_m$ be an isomorphism of groups. Let $\omega_a : \mathbb{Z}_a \to \mathbb{Q}^t$ and $\omega_b : \mathbb{Z}_b \to \mathbb{Q}^t$ be two weights. Define for every $x \in \mathbb{Z}_m$ such that $x = \psi(y, z)$, where $y \in \mathbb{Z}_a$, $z \in \mathbb{Z}_b$,

$$\omega_m(x) = \omega_a(y) + \omega_b(z).$$

Define a $\mathbb{Z}_m$-linear map $f : \mathbb{Z}_m^2 \to \mathbb{Z}_m^2$ in the following way,

$$\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix} \xrightarrow{f} \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{matrix},$$

where the decomposition is from the isomorphism $\mathbb{Z}_m^2 = \mathbb{Z}_m \oplus \mathbb{Z}_m \xleftarrow{\psi \times \psi} \mathbb{Z}_a \oplus \mathbb{Z}_b \oplus \mathbb{Z}_a \oplus \mathbb{Z}_b$.

The map f preserves ω_m. Indeed, let $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_m$, calculate,

$$\begin{aligned} \omega_m((\alpha, \beta), (\gamma, \delta)) &= \omega_m(\alpha, \beta) + \omega_m(\gamma, \delta) = \omega_a(\alpha) + \omega_b(\beta) + \omega_a(\gamma) + \omega_b(\delta) \\ &= \omega_a(\alpha) + \omega_b(\delta) + \omega_a(\gamma) + \omega_b(\beta) = \omega_m(\alpha, \delta) + \omega_m(\gamma, \beta) \\ &= \omega_m((\alpha, \delta), (\gamma, \beta)) = \omega_m(f((\alpha, \beta), (\gamma, \delta))) \end{aligned}$$

But f is not $U(\omega_m)$-monomial, since, for example f maps $((1, 1), (0, 0))$ to $((1, 0), (0, 1))$.

Variations of the example for $\mathbb{Z}_m^n$, where $n > 2$, also exist. In the following statement we prove that the full group of ω-preserving linear maps on the ambient set is a subgroup of monomial maps for local ring alphabets.

Proposition 9.1.1. *Let R be a local ring (with identity), i.e., it has unique maximal ideal. Let $\omega : R \to \mathbb{Q}^+$ be a weight function with $\omega(r) = 0 \iff r = 0$. Every ω-preserving R-linear invertible map $h : R^n \to R^n$ is $U(\omega)$-monomial.*

Proof. Let I be the maximal ideal in R. Note that the group of units $\mathcal{U}(R) = R \setminus I$. Let $e_i \in R^n$ denote the vector with 1 on the ith position and 0 elsewhere. Assume that $h(e_i) = (a_1, \ldots, a_n)$, where $a_i \in I$. Then for every $r \in \operatorname{ann}_R(I)$, $h(re_i) = 0$, which means that $\ker h \neq 0$ and h is not invertible.

Without loss of generality, suppose that $h(e_1) = (a_1, \ldots, a_n)$ and $a_1 \in \mathcal{U}(R)$. Let $r \in \mathcal{U}(R)$ has the minimum weight $\omega(r)$ among all the elements in $\mathcal{U}(R)$. Calculate,

$$\omega(r) = \omega(h(re_1)) \geq \omega(ra_1).$$

Since $ra_1 \in \mathcal{U}(R)$, $\omega(ra_1) = \omega(r)$ and thus $a_2 = \cdots = a_n = 0$. The equality $h(e_1) = r^{-1}a_1e_1 = g_1e_1$ holds for $g_1 = r^{-1}a_1 \in \mathcal{U}(R)$.

For every $r \in R$, $\omega(r) = \omega(h(re_1)) = \omega(rg_1e_1) = \omega(rg_1)$. Considering the ring R as a module over itself, the group $\operatorname{Aut}_R(R)$ is isomorphic to the group

$\mathcal{U}(R)$, that is, linear automorphisms of R acts by multiplication on invertible elements in R. Hence $g_1 \in U(\omega) = \{g \in \mathcal{U}(R) \mid \forall r \in R,\ \omega(r) = \omega(rg)\}$.

Using the same arguments for other coordinates, h is an $U(\omega)$-monomial map. □

We suggest a new definition of an extension property for linear codes over a module alphabet bases on the categorical approach of [3]. We say that an R-module alphabet A has a $*$-*extension property* if for every positive integer n, every R-linear weight preserving map of a code $C \subseteq A^n$ extends to an R-linear weight preserving map of A^n. This definition differ from the classical definition of an extension property for some cases (see Example 9.1.1). The suggested problems are the following.

Problem 9.1.1. Describe those R-module alphabets that have a $*$-extension property.

Problem 9.1.2. Describe sufficient and necessary conditions on an R-module alphabet A and a weight function ω such that every R-linear ω-preserving map $h : A^n \to A^n$ is $U(\omega)$-monomial.

9.2 MDS combinatorial codes

In Chapter 4 we proved some facts about an extension property of MDS linear and group codes. However, as we mentioned in Remark 4.3.1, an analogue of the extension theorem may hold for some MDS combinatorial codes. Though we do not have any results for the moment, we give an idea of one possible approach to the solution of the extension problem for MDS combinatorial codes. For this we combine the geometric approach of Chapter 2 and combinatorial approach of Chapter 8.

Recall the notations of Chapter 8. Let $C \subseteq A^n$ be a code with m-elements and let $\lambda : M \to A^n$ be an encoding map of C, where $M = \{1, \dots, m\}$.

Let $\alpha_1, \dots, \alpha_n$ be partitions that correspond to the map λ (see Section 8.3.1 for more details). Let $f : C \to A^n$ be a map and let $\mu = f\lambda$. In the same way let $\beta_1, \dots, \beta_n$ be partitions that correspond to the map μ. All the partitions are in $\mathcal{P}$.

Recall that the map $\Delta_\alpha : \mathcal{O} \to \{0, 1\}$ maps a pair $p = \{i, j\} \in \mathcal{O}$ to 0 if i and j belong to the same class in α, and to 1 otherwise. The map Δ_α can be seen as a subset of $\mathcal{O}$, with $\Delta_\alpha(p) = 1$ means that $p \in \Delta_\alpha$.

It is easy to see, according to Proposition 8.3.2, that the map $f : C \to A^n$ is a Hamming isometry if and only if

$$\sum_{i=1}^{n} \mathbb{1}_{\Delta_{\alpha_i}} = \sum_{i=1}^{n} \mathbb{1}_{\Delta_{\beta_i}},$$

as functions on $\mathcal{O}$, and the map f extends to a monomial map if and only if the n-tuples $(\Delta_{\alpha_1}, \dots, \Delta_{\alpha_n})$ and $(\Delta_{\beta_1}, \dots, \Delta_{\beta_n})$ are equal. The last is equivalent

to the equality, $(\alpha_1, \ldots, \alpha_n) = (\beta_1, \ldots, \beta_n)$. This statement is similar to the statement of Proposition 2.3.1 for linear codes.

In the same way as we did in Chapter 4, we can characterize MDS combinatorial codes in terms of partitions α_i, $i \in \{1, \ldots, n\}$. The following we give without a proof. If the code C is (n, k) MDS, then for every set $I \subseteq \{1, \ldots, n\}$ of cardinality k,

$$\bigcup_{i \in I} \Delta_{\alpha_i} = \Delta_{\bigcap_{i \in I} \alpha_i} = \mathcal{O},$$

that holds if and only if $\bigcap_{i \in I} \alpha_i = \{\{1\}, \{2\}, \ldots \{n\}\}$. Here we assume that α_i is an element of the poset of all partitions with the partial order $\preceq$ "finer" (see Section 6.2).

Despite the fact that the properties of linear and combinatorial MDS codes are similar, an analogous result to Theorem 4.0.1 for MDS combinatorial codes does not hold in general. For the moment we do not have a general extension theorem for MDS combinatorial codes. The problem is the following.

Problem 9.2.1. Prove that an extension property holds for some classes of MDS combinatorial codes using the given characterization of MDS codes in terms of n-tuples of partitions.

9.3 Other problems

Problem 9.3.1. In Lemma 3.2.2 we proved that the length of the solutions (X, Y) of eq. (3.1) with $X \neq Y$ is not smaller than N_k. For $k = 1$, which corresponds to the case of vector spaces, we have a description of all such solutions with $n = N_1 = q + 1$. Describe for all $k \geq 2$ all such solution of the minimum length $n = N_k$.

Problem 9.3.2. For two-dimensional linear MDS codes over a vector space alphabet we found a bound on the minimum code length for which there exists an unextendable Hamming isometry (see Theorem 4.2.4). Find a similar bound for two-dimensional linear MDS codes over a module alphabet.

Problem 9.3.3. For every positive integer n describe all subgroups in $\mathrm{GL}_n(\mathbb{F}_q)$ that are closed with respect to the action on an n-dimensional vector space.

Problem 9.3.4. In Theorem 6.0.1 we showed that vector spaces does not have a G-pseudo-injectivity property, except for a few families. Describe the subgroups $G \leq \mathrm{GL}_n(\mathbb{F}_q)$ and subspaces in an n-dimensional vector space that violate the G-pseudo-injectivity property for vector spaces.

Problem 9.3.5. Find a connection between pseudo-injectivity and G-pseudo-injectivity. In particular, find a G-pseudo-injective module that is not pseudo-injective.

Problem 9.3.6. Prove or disprove extension theorem for weights that do not split into a sum of weight on coordinates (as for example, the rank weight) using the G-pseudo-injectivity criterion from Section 7.2.

Problem 9.3.7. Describe all the subgroups of $\mathfrak{S}_n$ that are closed with respect to the action on the sets of partitions $\mathcal{P}$, $\mathcal{P}_2$ and $\mathcal{P} \setminus \mathcal{P}_2$, which are defined in Chapter 8.

The reader may notice that in the present thesis the designed geometric tools are not applied properly for the case of linear codes over module alphabets equipped with general weight functions (except some negative results in Chapter 5). However it is possible, though it is more complicated than in the case of the Hamming weight. I also give (without a proof) two problems concerning classical linear codes but with different weight functions and cyclic group alphabets with the Lee weight. The statements seem to be correct, however, in the thesis they are considered as open problems. The complete result may appear in a future paper.

A classical linear code C is *projective* if every two different columns of C are linearly independent.

Problem 9.3.8. Let C be a projective $\mathbb{F}_q$-linear code in $\mathbb{F}_q^n$ with a non-constant weight $\omega : \mathbb{F}_q \to \mathbb{Q}$. Each $\mathbb{F}_q$-linear ω-preserving map extends to an $U(\omega)$-monomial map.

We call a $\mathbb{Z}_m$-linear code C *projective* if for every two different columns u, v of C (as elements of the $\mathbb{Z}_m$-module M) the following hold: for every $c \in \mathbb{Z}_m^*$, $u \neq cv$ and for every nonzero $c \in \mathbb{Z}_m$, $cv \neq 0 \in M$. Alternatively, C is projective if for every two different columns u, v of C the isomorphism holds $\langle u, v \rangle \cong \mathbb{Z}_m^2$.

Problem 9.3.9. Let $m \geq 2$ be a positive integer. Let C be a projective $\mathbb{Z}_m$-linear code in $\mathbb{Z}_m^n$. Each $\mathbb{Z}_m$-linear map that preserves the Lee weight extends to a $\{\pm 1\}$-monomial map.

BIBLIOGRAPHY

[1] F. W. Anderson and K. R. Fuller. *Rings and Categories of Modules*, volume 13 of *Graduate Texts in Mathematics*. Springer New York, New York, NY, 1992.

[2] A. Assem. On modules with cyclic socle. *Journal of Algebra and Its Applications*, 15(8), 2016.

[3] E. F. Assmus, Jr. The category of linear codes. *IEEE Trans. Inf. Theor.*, 44(2):612–629, Sept. 2006.

[4] S. V. Avgustinovich and F. I. Solov'eva. To the metrical rigidity of binary codes. *Problems of Information Transmission*, 39(2):178–183, Apr. 2003.

[5] A. Barra. *Equivalence Theorems and the Local-Global Property*. Doctoral dissertation, University of Kentucky, 2012.

[6] T. P. Berger. Isometries for rank distance and permutation group of Gabidulin codes. *IEEE Transactions on Information Theory*, 49(11):3016 – 3019, 2003.

[7] A. Beutelspacher. Blocking sets and partial spreads in finite projective spaces. *Geometriae Dedicata*, 9(4):425–449, 1980.

[8] K. Bogart, D. Goldberg, and J. Gordon. An elementary proof of the MacWilliams theorem on equivalence of codes. *Information and Control*, 37(1):19 – 22, 1978.

[9] P. G. A. Bonneau. *Codes et combinatoire*. PhD thesis, Université Pierre et Marie Curie, Paris, 1984.

[10] R. Bose and R. Burton. A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonald codes. *Journal of Combinatorial Theory*, 1(1):96 – 104, 1966.

[11] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-regular graphs*. Springer-Verlag, 1989.

[12] S. Cho. Minimal null designs of subspace lattice over finite fields. *Linear Algebra and its Applications*, 282(1):199–220, Oct. 1998.

[13] I. Constantinescu and W. Heise. On the concept of code-isomorphy. *Journal of Geometry*, 57(1-2):63–69, 1996.

[14] I. Constantinescu and W. Heise. A metric for codes over residue class rings. *Problems of Information Transmission*, 33:208–213, 1997.

[15] H. Q. Dinh and S. R. López-Permouth. On the equivalence of codes over finite rings. *Appl. Algebra Eng., Commun. Comput.*, 15(1):37–50, June 2004.

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

[17] J. D. Dixon and B. Mortimer. *Permutation Groups*, volume 163 of *Graduate texts in mathematics*. Springer, 1996.

[18] S. Dodunekov and I. Landgev. On near-mds codes. *Journal of Geometry*, 54(1-2):30–43, 1995.

[19] S. Dyshko. Geometric approach to the MacWilliams extension theorem for codes over modules. Manuscript submitted for publication in AAECC. Preprint available at `http://arxiv.org/abs/1507.05212v1`.

[20] S. Dyshko. Isometry groups of combinatorial codes. Preprint available at `https://arxiv.org/abs/1606.05268`.

[21] S. Dyshko. Minimal nontrivial solutions of the isometry equation. Submitted to Discrete Mathematics. Preprint available at `http://arxiv.org/abs/1501.02470v1`.

[22] S. Dyshko. When the extension property does not hold for vector space alphabets. Preprint available at `http://arxiv.org/abs/1512.06065v1`.

[23] S. Dyshko. MacWilliams extension theorem for MDS over a vector space alphabet. *Designs, Codes and Cryptography*, 2016.

[24] S. Dyshko. On extendability of additive code isometries. *Advances in Mathematics and Communications*, 10(1):45–52, 2016.

[25] S. Dyshko. When the extension property does not hold. *Journal of Algebra and Its Applications*, 2016.

[26] S. Dyshko, P. Langevin, and J. A. Wood. Deux analogues au dterminant de Maillet. *Comptes Rendus Mathematique*, 354(7):649–652, July 2016.

[27] S. El-Zanati, G. Seelinger, P. Sissokho, L. Spence, and C. V. Eynden. On λ-fold partitions of finite vector spaces and duality. *Discrete Mathematics*, 311(4):307 – 318, 2011.

[28] N. ElGarem, N. Megahed, and J. Wood. The extension theorem with respect to symmetrized weight compositions. In R. Pinto, P. Rocha Malonek, and P. Vettori, editors, *Coding Theory and Applications*, volume 3 of *CIM Series in Mathematical Sciences*, pages 177–183. Springer International Publishing, 2015.

[29] G. D. Forney, Jr. On the Hamming distance properties of group codes. *IEEE Transactions on Information Theory*, 38(6):1797–1801, Sept. 2006.

[30] E. M. Gabidulin. Theory of Codes with Maximum Rank Distance. *Problems of Information Transmission*, 21(1):3–16, 1985.

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

[32] M. Greferath. Cyclic codes over finite rings. *Discrete Mathematics*, 177(1):273–277, Dec. 1997.

[33] M. Greferath, T. Honold, C. M. Fadden, J. A. Wood, and J. Zumbrägel. MacWilliams' extension theorem for bi-invariant weights over finite principal ideal rings. *Journal of Combinatorial Theory, Series A*, 125:177–193, 2014.

[34] M. Greferath, A. Nechaev, and R. Wisbauer. Finite quasi-Frobenius modules and linear codes. *Journal of Algebra and Its Applications*, 03(03):247–272, 2004.

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

[36] M. Greferath and S. E. Schmidt. Linear Codes and Rings of Matrices. In M. Fossorier, H. Imai, S. Lin, and A. Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, number 1719 in Lecture Notes in Computer Science, pages 160–169. Springer Berlin Heidelberg, Nov. 1999.

[37] J. Gruska. *Quantum computing*. Advanced topics in computer science series. McGraw-Hill, London, 1999.

[38] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Sole. The Z4-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Transactions on Information Theory*, 40(2):301–319, Mar. 1994.

[39] B. Huppert. *Character theory of finite groups*. Number 25 in De Gruyter expositions in mathematics. Walter de Gruyter, Berlin ; New York, 1998.

[40] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary Stabilizer Codes Over Finite Fields. *IEEE Transactions on Information Theory*, 52(11):4892–4914, Nov. 2006.

[41] D. I. Kovalevskaya. On metric rigidity for some classes of codes. *Problems of Information Transmission*, 47(1):15–27, Mar. 2011.

[42] T. Y. Lam. *A First Course in Noncommutative Rings*. Springer, 1991.

[43] S. Lang. *Algebra*. Addison-Wesley series in mathematics. Addison-Wesley Publishing Company, Advanced Book Program, 1984.

[44] P. Langevin and J. A. Wood. The extension theorem for the lee and euclidean weights over $\mathbb{Z}/p^k\mathbb{Z}$. Preprint available at `http://homepages.wmich.edu/~jwood/eprints/twodet-v3.6-alt.pdf`.

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

[46] J. Luh. On the representation of vector spaces as a finite union of subspaces. *Acta Mathematica Academiae Scientiarum Hungarica*, 23:341–342, 1972.

[47] F. MacWilliams and N. Sloane. *The Theory of Error-Correcting Codes: Vol.: 1*. North-Holland Mathematical Library. North-Holland Publishing Company, 1977.

[48] F. J. MacWilliams. *Combinatorial Properties of Elementary Abelian Groups*. Ph.D. thesis, Radcliffe College, 1962.

[49] J. MacWilliams. Error-Correcting Codes for Multiple-Level Transmission. *Bell System Technical Journal*, 40(1):281–308, Jan. 1961.

[50] G. A. Miller. Groups in which all the operators are contained in a series of subgroups such that any two have only identity in common. *Bull. Amer. Math. Soc.*, 12(9):446–449, 06 1906.

[51] B. L. Osofsky. Rings all of whose finitely generated modules are injective. *Pacific Journal of Mathematics*, 14(2):645–650, 1964.

[52] G.-C. Rota. On the foundations of combinatorial theory I. Theory of Möbius functions. *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, 2(4):340–368, 1964.

[53] C. Satyanarayana. Lee metric codes over integer residue rings (Corresp.). *IEEE Transactions on Information Theory*, 25(2):250–254, Mar. 1979.

[54] S. Singh and S. Jain. On pseudo injective modules and self pseudo injective rings. *The Journal of Mathematical Sciences*, 2(1):125–133, 1967.

[55] F. Solov'eva, T. Honold, S. Avgustinovich, and W. Heise. On the extendability of code isometries. *Journal of Geometry*, 61(1-2):2–16, 1998.

[56] R. P. Stanley. *Enumerative Combinatorics: Volume 1*. Cambridge University Press, New York, NY, USA, 2nd edition, 2011.

[57] A. Terras. *Fourier Analysis on Finite Groups and Applications*. Cambridge University Press, Mar. 1999.

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

[59] H. Wielandt. *Permutation groups through invariant relations and invariant functions*. Dept. of Mathematics, Ohio State University, Columbus, 1969.

[60] R. Wisbauer. *Foundations of module and ring theory*, volume 3. CRC Press, 1991.

[61] J. Wood. Code equivalence characterizes finite Frobenius rings. *Proceedings of the American Mathematical Society*, 136(2):699–706, 2008.

[62] J. A. Wood. Isometry Groups of Additive Codes. Preprint. Available at `http://homepages.wmich.edu/~jwood/eprints/Wood-isometries.pdf`.

[63] J. A. Wood. Extension theorems for linear codes over finite rings. In T. Mora and H. Mattson, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 1255 of *Lecture Notes in Computer Science*, pages 329–340. Springer Berlin Heidelberg, 1997.

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

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

[66] J. A. Wood. The structure of linear codes of constant weight. *Electronic Notes in Discrete Mathematics*, 6:287 –296, 2001. WCC2001, International Workshop on Coding and Cryptography.

[67] J. A. Wood. Foundations of linear codes defined over finite modules: the extension theorem and the MacWilliams identities. In *Codes over rings*, volume 6 of *Ser. Coding Theory Cryptol.*, pages 124–190. World Sci. Publ., Hackensack, NJ, 2009.

[68] J. A. Wood. Isometry Groups of Additive Codes, 2015. Presented at AMS meeting, Loyola University, Chicago IL.

[69] J. Xu. *On closures of finite permutation groups*. PhD thesis, The University of Western Australia, 2005.

[70] E. Yaraneri. Intersection graph of a module. *Journal of Algebra and Its Applications*, 12(05):1250218, 2013.

APPENDIX

G-pseudo-injectivity of $\mathbb{F}_2^3$

```
#DEFINITIONS

import itertools
import copy

# This function returns a partition into orbits
# of an element g of a group G.
# Orbits are subsets of a vector space V.
def orbitsOfGroupElement(g, V, G):
    t = list(V)
    #initiating the resulting partition
    partition = []
    while len(t)>0:
        orbit = []
        #running through a cyclic subgroup generated by g
        for h in G.subgroup([g]):
            x = t[0]*h
            if not x in orbit:
                orbit.append(x)
        orbit.sort()
        partition.append(orbit)
        for v in orbit:
            t.remove(v)
    partition.sort()
    return partition

#removes duplicates from a (nonhashable) tuple
def removeDuplicates(a):
    b=[]
    for x in a:
        if x not in b:
            b.append(x)
    return b

# unite two orbits in a partition
def uniteTwoOrbits(partition, orbit1, orbit2):
    i=partition.index(orbit1)
    j=partition.index(orbit2)
    if i!=j:
        partition[i]=list(removeDuplicates(orbit1 + orbit2))
        del partition[j]

# returns an orbit that contains the given element x
def find(partition,x):
    for orbit in partition:
        if x in orbit:
            return orbit
```

```
#merges two partition into orbits
def mergePartitions(partition1, partition2):
    partition3 = copy.deepcopy(partition1)
    for orbit in partition2:
        for i in range(len(orbit)-1):
            uniteTwoOrbits(partition3,\
                find(partition3,orbit[i]),\
                find(partition3,orbit[i+1]))
    return partition3

#returns True if g preserves the orbits of orbs
def fixes(g, partition):
    for orbit in partition:
        for x in orbit:
            if x*g not in orbit:
               return False
    return True

#returns a closed group with the gives set of orbits
def makeClosure(partition, G):
    group = []
    for g in G:
        if fixes(g, partition):
            group.append(g)
    return group

#checks if two elements are in same orbit
def inSameOrbit(x,y,partition):
    for orbit in partition:
        if x in orbit and y in orbit:
            return True
    return False

#check if the map f extends to an element of the group
def isExtendable(x,fx,y,fy,group):
    for g in group:
        if x*g == fx and y*g == fy:
            return [g,True]
    return [0,False]


#MAIN PROGRAM

print("Initializing...")
#the dimension of the space
n=3
#the size of the finite field
q=2
#declaration of the finite field
```

```
F=GF(q)
#n by n invertible matrices over the finite field F
G=GL(n,F)
#space of n by n matrices over the finite field F
M=MatrixSpace(F,n,n)
#vector space F^n
V=VectorSpace(F,n)
#declaring two elements of the vector space a = (1,0,0)
#and b = (0,1,0)
a=V([1,0,0])
b=V([0,1,0])

print("Initialization of basic objects is finished\n"+
"Building partitions into orbits for cyclic groups...")

#Creating a dictionary of orbit partitions for quick access
P=dict()
for g in G:
    if a*g==a:
        orb=orbitsOfGroupElement(g,V,G)
        P[str(orb)]=orb

print("There are "+str(len(P))+
" different partitions into orbits for cyclic groups.\n"+
"Developing partitions into orbits...")

#calculating all possible orbits
flag=True
checked=[]
while(flag):
    flag=False
    t=dict()
    for key1,key2 in itertools.combinations(P,r=2):
        if not [key1,key2] in checked:
            partition3=mergePartitions(P[key1],P[key2])
            checked.append([key1,key2])
            for orb in partition3:
                orb.sort()
            partition3.sort()
            key3=str(partition3)
            if key3 not in P:
                t[key3]=partition3
                flag=True
    for key in t:
        P[key]=t[key]

print("There are "+str(len(P))+
" different partitions into orbits\nBuilding groups...")

#Now we start to build closed group for each orbit
```

```
setOfClosedGroups=[]
for key in P:
    setOfClosedGroups.append([P[key],\
        makeClosure(P[key],G)])

print("All groups are built.\nChecking each group...")

exampleFound = False
for partition, group in setOfClosedGroups:
    for c in V:
        if inSameOrbit(b,c,partition) and\
            inSameOrbit(a+b,a+c,partition):
                g, ans=isExtendable(a,a,b,c,group)
                if not ans:
                    print(c,g)
                    exampleFound = True
                    break
if not exampleFound:
    print("No counterexample found.")

print("The program finished.")

"""
Initializing...
Initialization of basic objects is finished
Building partitions into orbits for cyclic groups...
There are 17 different partitions into orbits
for cyclic groups.
Developing partitions into orbits...
There are 22 different partitions into orbits
Building groups...
All groups are built.
Checking each group...
No counterexample found.
The program finished.
"""
```

The SAGE source code can be found at https://github.com/dyshko/thesis.

Isometry groups of combinatorial binary codes

```
#this program calculates the groups Mon(C) and Iso(C)
#and outputs their sizes. The input code is represented
#by the set of columns and a multiplicity function:
#a vector that says how many columns of the corresponding
#type belong to the code.
#Since the considered codes have small cardinality
#and are over the binary alphabet {0,1}, it is
#implemented the brute-force algorithm

import itertools

#returns the Hamming distance between two codewords
def hamming_distance(cw1, cw2, mlt):
    return sum([mlt[i] for i in range(len(mlt)) if \
        cw1[i]!=cw2[i]])

#check if there is a Hamming isometry between two codes
#(second distance distribution is precalculated)
def isometry(code_new, code_dist, mlt):
    m = len(code_new)   #the number of rows
    for i in range(m):
        for j in range(i+1, m):
            if hamming_distance\
            (code_new[i], code_new[j], mlt)!=code_dist[i][j]:
                return False
    return True

#action of permutation
def act_perm(code, p):
    m = len(code)
    res = []
    for i in range(m):
        res.append(code[p[i]])
    return res

#code to string
def code_to_str(code, mlt):
    m = len(code)       #the number of rows
    columns = [list(x) for x in zip(*code)]
    for col in columns:
        if col[0]==1:
            for i in range(m):
                col[i]^=1
    columns, new_mlt = zip(*sorted(zip(columns, mlt)))
    return "".join([str(col) \
    for col in columns])+str(new_mlt)
```

```
#main
def sizes_of_groups(code, mlt):
        MON = []
        ISO = []
        N = len(code[0]) #size of the support
        m = len(code)   #the number of rows

        code_dist = [[0]*m for i in range(m)]
        for i in range(m):
                code_dist[i][i] = 0
                for j in range(i+1,m):
                        code_dist[i][j] =\
        code_dist[i][j] =\
        hamming_distance(code[i], code[j], mlt)

        code_str = code_to_str(code, mlt)

        for p in itertools.permutations(list(range(m))):
                code_new = act_perm(code, p)
                if isometry(code_new, code_dist, mlt):
                        ISO+=[p]
                        if code_to_str(code_new, mlt)\
                        ==code_str:
                                MON+=[p]
        print("#Mon(C) = "+str(len(MON))+ "\t #Iso(C)="\
        +str(len(ISO)))

########## INPUTS ######################

C1 = [
[1,0,0,0,0,1,1,1,1,0,0,0,0,0,0,0],
[0,1,0,0,0,1,0,0,0,1,1,1,0,0,0],
[0,0,1,0,0,0,1,0,0,1,0,0,1,1,0],
[0,0,0,1,0,0,0,1,0,0,1,0,1,0,1],
[0,0,0,0,1,0,0,0,1,0,0,1,0,1,1]
    ]

mlt11 =[0,1,2,3,4,6,5,4,3,4,3,2,2,1,0]

###############

C2 = [
[1,0,0,0,1,1,1],
[0,1,0,0,1,0,0],
[0,0,1,0,0,1,0],
[0,0,0,1,0,0,1]
    ]

mlt21 =[1,2,3,4,0,0,0]
```

```
mlt22 =[1,1,2,3,0,0,0]

mlt23 =[1,1,1,2,0,0,0]

mlt24 =[1,1,2,2,0,0,0]

mlt25 =[0,0,0,0,2,1,0]

mlt26 =[0,0,0,0,1,1,0]

mlt27 =[1,1,1,1,0,0,0]

#############

C3 = [
[0,0,0,0],
[1,1,0,0],
[1,0,1,0],
[1,0,0,1],
[0,1,1,0]
     ]

mlt31 = [1,1,1,1]

########## OUTPUT ######################

print("Code 1:")
sizes_of_groups(C1, mlt11)
print("Code 2:")
sizes_of_groups(C2, mlt21)
print("Code 3:")
sizes_of_groups(C2, mlt22)
print("Code 4:")
sizes_of_groups(C2, mlt23)
print("Code 5:")
sizes_of_groups(C2, mlt24)
print("Code 6:")
sizes_of_groups(C2, mlt25)
print("Code 7:")
sizes_of_groups(C2, mlt26)
print("Code 8:")
sizes_of_groups(C2, mlt27)
print("Code 9:")
sizes_of_groups(C3, mlt31)

"""
Code 1:
#Mon(C) = 1        #Iso(C)=120
Code 2:
#Mon(C) = 1        #Iso(C)=1
```

```
Code 3:
#Mon(C) = 2          #Iso(C)=2
Code 4:
#Mon(C) = 6          #Iso(C)=6
Code 5:
#Mon(C) = 4          #Iso(C)=4
Code 6:
#Mon(C) = 4          #Iso(C)=4
Code 7:
#Mon(C) = 8          #Iso(C)=8
Code 8:
#Mon(C) = 24         #Iso(C)=24
Code 9:
#Mon(C) = 6          #Iso(C)=12
"""
```

The Python source code can be found at https://github.com/dyshko/thesis.

Serhii DYSHKO

IMATH, Université de Toulon

Généralisations du Théorème d'Extension de MacWilliams

Résumé en français

Le fameux Théorème d'Extension de MacWilliams affirme que, pour les codes classiques, toute isométrie de Hamming linéaire d'un code linéaire se prolonge en une application monomiale. Cependant, pour les codes linéaires sur les alphabets de module, l'existence d'un analogue du théorème d'extension n'est pas garantie. Autrement dit, il existe des codes linéaires sur certains alphabets de module dont les isométries de Hamming ne sont pas toujours extensibles. Il en est de même pour un contexte plus général d'un alphabet de module muni d'une fonction de poids arbitraire. Dans la présente thèse, nous prouvons des analogues du théorème d'extension pour des codes construits sur des alphabets et fonctions de poids arbitraires. La propriété d'extension est analysée notamment pour les codes de petite longueur sur un alphabet de module de matrices, les codes MDS généraux, ou encore les codes sur un alphabet de module muni de la composition de poids symétrisée. Indépendamment de ce sujet, une classification des deux groupes des isométries des codes combinatoires est donnée. Les techniques développées dans la thèse sont prolongées aux cas des codes stabilisateurs quantiques et aux codes de Gabidulin dans le cadre de la métrique rang.

Mot clés : Théorème d'Extension de MacWilliams, application monomiale, isométrie de Hamming, code non-linéaire, codes sur alphabets de module, code additif, fonction de poids arbitraire, code quantique.

Generalizations of the MacWilliams Extension Theorem

Résumé en anglais

The famous MacWilliams Extension Theorem states that for classical codes each linear Hamming isometry of a linear code extends to a monomial map. However, for linear codes over module alphabets an analogue of the extension theorem does not always exist. That is, there may exists a linear code over a module alphabet with an unextendable Hamming isometry. The same holds in a more general context of a module alphabet equipped with a general weight function. Analogues of the extension theorem for different classes of codes, alphabets and weights are proven in the present thesis. For instance, extension properties of the following codes are studied: short codes over a matrix module alphabet, maximum distance separable codes, codes over a module alphabet equipped with the symmetrized weight composition. As a separate result, a classification of two isometry groups of combinatorial codes is given. The thesis also contains applications of the developed techniques to quantum stabilizer codes and Gabidulin codes.

Keywords : MacWilliams Extension Theorem, monomial map, Hamming isometry, nonlinear code, code over a module alphabet, additive code, general weight function, quantum code.