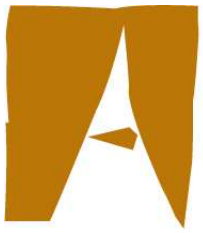

Universitat Autònoma de Barcelona

Departament d'Enginyeria de la Informació i de les Comunicacions

ON REED-MULLER AND RELATED QUATERNARY CODES

Submitted to Universitat Autònoma de Barcelona
in partial fulfillment of the requirements for the
degree of Doctor of Philosophy in Computer Science

by Cristina Fernández Córdoba

Bellaterra, June 2005

Directed by
Dr. Joaquim Borges i Ayats
and Dr. Kevin T. Phelps

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of Doctor of Philosophy.

Bellaterra, June 2005

Dr. Joaquim Borges i Ayats
(Adviser)

Dr. Kevin T. Phelps
(Adviser)

to whoever makes the most
difficult moments become
easier.

Abstract

In this dissertation, we will study deeply Reed-Muller codes together with two families of $\mathbb{Z}_4$-codes related to them. These families are $\mathcal{QRM}(r,m)$ and $\mathcal{ZRM}(r,m)$.

It is known that $\mathcal{QRM}(r,m)$ modulo 2 is exactly, the Reed-Muller code $RM(r,m)$. Moreover, the Kerdock code and its $\mathbb{Z}_4$-dual code, a Preparata-like code, are obtained as images of some $\mathcal{QRM}(r,m)$ codes via the Gray map. We will generalize such family of codes to the class of codes $\overline{\mathcal{QRM}}(r,m)$. Any code in this class modulo 2 is a Reed-Muller code and it will be proven that any Kerdock-like and Preparata-like code is the image of a code in $\overline{\mathcal{QRM}}(r,m)$ via the Gray map. The properties of codes in the class will be studied and we will calculate the rank and the dimension of the kernel of these codes. Moreover, we also give different constructions of codes in $\overline{\mathcal{QRM}}(r,m)$ and consider chain of codes in such class. We will determine some properties of such chains concerning the duality and minimum distance of codes in the chain.

Codes $\mathcal{ZRM}(r,m)$ were defined in order to determine the $\mathbb{Z}_4$-linearity of Reed-Muller codes. There were two different definitions of $\mathcal{ZRM}(r,m)$ codes (denoted $\mathcal{ZRM}(r,m)$ and $\mathcal{ZRM}^*(r,m)$) that coincides if and only if the related $RM(r,m)$ code is $\mathbb{Z}_4$-linear. Thus we calculate the rank and the dimension of the kernel of both $\mathcal{ZRM}(r,m)$ and $\mathcal{ZRM}^*(r,m)$ codes. Finally, we relate both codes with codes in $\overline{\mathcal{QRM}}(r,m)$ and Reed-Muller codes.

Acknowledgements

This dissertation is the result of many years of learning and effort. Many people have collaborated in the creation of this work and I would like to thank all of them.

This work had not been possible without the dedication of my advisers Quim Borges and Kevin T. Phelps. The main idea of this dissertation came up during my research stay in Auburn where professor Kevin T. Phelps welcomed me. He gave me the chance of going to Auburn and shared with me his time and knowledge.

Quim Borges has supervised the work in every moment. He has always encouraged me and has taught me, patiently, his way of doing research. I would like to thank both of them all our discussions even in the distance.

I thank all the members of the Department of Information and Communications Engineering for making the work place become more comfortable and pleasant. In particular, I thank Josep Rifà for introducing me in its research group and, together with Mercè Villanueva and Jaume Pujol, for their advises and talks about coding theory.

I also thank Joan Serra for his sincere support and for giving me the opportunity of working on Image compression. And, I special thank Guillermo Navarro, Fernando Garía and, above all, Francesc Aulí, who have been supporting me and cheering me up in difficult moments.

Finally, I would like to thank my family, Montse Jiménez and Luis Sánchez for their love and unconditional support.

To all of you, thank you very much.

Contents

Chapter 1

Introduction

The origin of codes was the aim of correcting errors on noisy communication channels. It was in the late 1940's when Golay, Hamming and Shannon studied that engineering problem from a mathematical point of view and that marked the beginning of today's coding theory.

Historically, linear codes have been the most studied types of codes. Due to their algebraic structure, they are easy to describe, construct, encode and decode. Whenever a code is not linear, there are two parameters or invariants of the code that give the information about how far is that code to be linear; these are the rank and the dimension of the kernel. It was around 1970 that were constructed some nonlinear codes having twice as many codewords as any known linear code with the same length and minimum distance. Among these codes, there are the Nordstrom-Robinson, Preparata and Kerdock codes.

About 20 years later, an important step in coding theory was achieved. It was proven that nonlinear codes mentioned above could be considered as the image under a called Gray map of additive codes over $\mathbb{Z}_4$ [HKC$^+$94]. They are called $\mathbb{Z}_4$-linear codes. The Preparata code is not a $\mathbb{Z}_4$-linear code but a code with the same parameters; it is called a Preparata-like code. It also was given that the $\mathbb{Z}_4$-dual code of the Kerdock code is the Preparata-like code mentioned above. In fact, there are many

nonequivalent codes with the same parameters of the Preparata code; that is many nonequivalents Preparata-like codes [Kan83]. $\mathbb{Z}_4$-dual code of any Preparata-like code is called a Kerdock-like code. Any additive Preparata-like and Kerdock-like code is $\mathbb{Z}_4$-linear code.

In 1989 propelinear codes were introduced [RBH89]. The difference with linear codes is that, given two codewords x and y, the sum of such codewords may not belong to the code but it belongs the sum of x and a permutation (associated to x) of y. Both linear and $\mathbb{Z}_4$-linear codes turn out to be propelinear codes. Among the most important propelinear codes are those being 1-perfect with an Abelian structure that corresponds to codes which are isomorphic to a subgroup of $\mathbb{Z}_2^k \times \mathbb{Z}_4^{\frac{n-k}{2}}$.

One of the simplest and most important families of linear codes are the Reed-Muller codes, $RM(r, m)$. Recall that some photographies of Mars were transmitted by the Mariner 9 spacecraft on 19 January 1972 using the first-order Reed-Muller code $RM(1, 5)$ (one of these pothografies can be found in [MS77, Figure 14.7]). The importance of these codes lies in the fact that they are relatively easy to encode and decode by using majority-logic circuits. Moreover, they are of mathematical interest due to the fact that they are related to finite affine and projective geometries. In general, $RM(r, m)$ are not $\mathbb{Z}_4$-linear codes. However, there are some values for the parameters r and m for which such codes are $\mathbb{Z}_4$-linear. There are two families of $\mathbb{Z}_4$-codes related to them: $\mathcal{QRM}(r, m)$ and $\mathcal{ZRM}(r, m)$ codes. Let $QRM(r, m)$ and $ZRM(r, m)$ denote their binary image under the Gray map.

The first family, $\mathcal{QRM}(r, m)$ codes, is important because Preparata-like and Kerdock codes are $QRM(r, m)$ codes. The inverse image of Preparata-like and Kerdock-like codes under the Gray map are called quaternary Preparata-like and Kerdock-like codes respectively. $RM(r, m)$ codes are obtained from $\mathcal{QRM}(r, m)$ codes by applying the modulo 2 map. The second family was defined to prove the $\mathbb{Z}_4$-linearity of Reed-Muller codes, whenever they are $\mathbb{Z}_4$-linear. The purpose of this dissertation is to study deeply both families of codes and establish the relationship between them together with Reed-Muller codes.

Firstly, due to the fact that Preparata-like and Kerdock codes are $QRM(r,m)$ codes and there are nonequivalent Preparata-like and Kerdock-like codes, we generalize $\mathcal{QRM}(r,m)$ codes to the class $\overline{\mathcal{QRM}}(r,m)$. All quaternary Preparata-like and Kerdock-like codes belong to $\overline{\mathcal{QRM}}(r,m)$ and, any code $\mathcal{C}$ in this class modulo 2 is a Reed-Muller code. Image under the Gray map of codes in $\overline{\mathcal{QRM}}(r,m)$ are not linear codes in general. Thus, we would like to establish which is the rank and the dimension of the kernel of codes in the class $\overline{\mathcal{QRM}}(r,m)$. In particular, we would obtain the rank and the dimension of the kernel of the family of codes $\mathcal{QRM}(r,m)$.

Related to the $\mathbb{Z}_4$-linearity of $RM(r,m)$ codes, we would like to determine which is the minimum $\mathbb{Z}_4$-linear code containing $RM(r,m)$ codes. $\mathcal{ZRM}(r,m)$ codes are defined such that $\phi(\mathcal{ZRM}(r,m-1)) = RM(r,m))$ when $RM(r,m)$ is $\mathbb{Z}_4$-linear. We would like to determine their rank and their dimension of the kernel and prove that the minimum $\mathbb{Z}_4$-linear code containing $RM(r,m)$ is, in fact, $\phi(\mathcal{ZRM}(r,m))$.

The organization of this dissertation is the following.

Chapter 2 is an overview of coding theory in general. It contains basic definitions that will be used along the whole dissertation. There are, in particular, definitions and some properties of linear codes, 1-perfect and propelinear codes. The $\mathbb{Z}_4$-codes are studied in Chapter 3. The Gray map and its extensions are shown and the binary image of these codes via the Gray map is considered. After that, the theory of additive codes is given in Chapter 4. Starting from association schemes, we then introduce some particular types of additive codes: $\mathbb{Z}_{2k}$-codes and binary mixed group codes. Some of the most important class of additive codes, the 1-perfect additive codes and extended 1-perfect additive codes, will be presented in Subsections 4.4 and 4.5 respectively. Last subsection, 4.6, corresponds to the punctured extended 1-perfect $\mathbb{Z}_4$-linear codes. The existence, the rank and the dimension of the kernel are established for all these 1-perfect codes.

In Chapter 5, first of all we will review definitions, known properties and constructions of Reed-Muller codes. Then, we will present the known statements about their $\mathbb{Z}_4$-linearity and will study the minimum $\mathbb{Z}_4$-code containing $\phi^{-1}(RM(r,m))$ for

some specific extended Gray map ϕ. That way, we obtain an upper bound of the number of codewords of the minimum $\mathbb{Z}_4$-linear code containing $RM(r,m)$ codes.

Even though there are some contributions about Reed-Muller codes in Chapter 5 (specially, the part concerning quaternary codes), Chapters 6 and 7 are the main core of this work.

The family of $\mathcal{QRM}(r,m)$ codes are studied in Chapter 6. We introduce the class $\overline{\mathcal{QRM}}$ and present definitions, properties and several constructions of codes in this class. Then, we establish the rank and the dimension of the kernel of codes in this class. Finally, we develop some construction of chains of codes in $\overline{\mathcal{QRM}}$ and we describe some of their properties.

In Chapter 7 we review the different definitions of $\mathcal{ZRM}$ codes. In the literature there are two different definitions ([HKC$^+$94], [Wan97]) of the family of $\mathcal{ZRM}$ codes. Both families of codes are denoted $\mathcal{ZRM}(r,m)$ and $\mathcal{ZRM}^*(r,m)$. We establish that the families $\mathcal{ZRM}(r,m)$ and $\mathcal{ZRM}^*(r,m)$ only coincide when the associated Reed-Muller code is both linear and $\mathbb{Z}_4$-linear. Otherwise we have that the binary images $ZRM^*(r,m)$ and $ZRM(r,m)$ of $\mathcal{ZRM}^*(r,m)$ and $\mathcal{ZRM}(r,m)$ respectively, satisfy that $\langle ZRM^*(r,m)\rangle = ZRM(r,m)$. We prove that, for all r, $ZRM(r,m)$ are linear codes. $\mathcal{ZRM}^*(r,m)$ are not linear codes and we compute the rank and the dimension of the kernel.

Finally, in Chapter 8 we summarize the obtained results and give the conclusions of the dissertation together with the open problems and future lines of research.

Chapter 2

Coding theory

In this chapter we will give basic definitions and known results about general codes which will be used in the subsequent chapters. Apart form general definitions in Section 2.1, we will focus on some particular types of codes. First, an overview of linear codes is given in Section 2.2. The next section is about 1-perfect codes: definitions and existence, description of STS and invariants related to these codes, constructions and, finally, some results about their rank and their dimension of the kernel. Section 2.4 concludes the chapter with propelinear codes.

2.1 Basic definitions

Let $\mathbb{F}_q^n$ be a vector space of dimension n over the Galois Field $\mathbb{F}_q = GF(q)$, where $q \geq 2$ is a prime power. A subset C of $\mathbb{F}_q^n$ is called a code of length n, and the elements $c \in C$ are codewords. When C is a linear subspace of $\mathbb{F}_q^n$, C is called a linear code; in that case, the sum of any two codewords is also a codeword. If C is a subgroup of $\mathbb{F}_q^n$ then C is called a group code. Unless stated otherwise, we shall assume that $q = 2$; so that $GF(2) = \mathbb{F}_2$, and hence, we denote by $\mathbb{Z}_2^n$ the additive group of $\mathbb{F}^n = \mathbb{F}_2^n$. $C \subset \mathbb{F}^n$ is called a binary code.

A code C is called a systematic code if there exist coordinates $i_1, \cdots, i_k$, such that

C restricted to these coordinates generates $\mathbb{F}^k$ and $|C| = 2^k$.

The Hamming distance between vectors $x, y \in \mathbb{F}^n$ is the number of coordinates in which x and y differ. We will denote the Hamming distance by $d(\ ,\ )$. The Hamming weight of a vector x is the number of nonzero coordinates and it is denoted by $\mathrm{wt}(x)$. We define the Hamming weight by means of the Hamming distance as $\mathrm{wt}(x) = d(x, \mathbf{0})$, where $\mathbf{0}$ is the all-zeroes vector. If $C \subset \mathbb{F}^n$ is a binary code, then we assume, unless it is said otherwise, that $\mathbf{0} \in C$.

The metric used in codes as subsets of $\mathbb{F}^n$ will be the Hamming metric. Other no-Hamming metrics can be found in [Mar01] .

For $X \subset \mathbb{F}^n$ and $v \in \mathbb{F}^n$, we define the distance of v to X, denoted by $d(v, X)$, as the minimum distance of v to any vector in X:

$$d(v, X) = min\{d(v, x)|x \in X\}.$$

Let C be a code. The minimum distance of C is

$$d_C = min\{d(x, y)|x, y \in C, x \neq y\},$$

and the minimum weight of C is

$$\mathrm{wt}_C = min\{\mathrm{wt}(x)|x \in C,\ x \neq \mathbf{0}\}.$$

We denote d_C as d when there is no ambiguity.

Let A_i be the number of codewords of Hamming weight i in C, then $\{A_0, \cdots, A_n\}$ is called the weight distribution of C. The weight enumerator of C is defined as the polynomial

$$W_C(X, Y) = \sum_{i=0}^{n} A_i X^{n-i} Y^i. \tag{2.1}$$

W_C is an homogeneous polynomial of degree n in X and Y. There is another way of writing this polynomial:

$$W_C(X, Y) = \sum_{c \in C} X^{n-\mathrm{wt}(c)} Y^{\mathrm{wt}(c)}. \tag{2.2}$$

The error correcting capability e of a code C is $e = \left\lfloor \frac{d-1}{2} \right\rfloor$. In this case, we say that C is e-error correcting.

Consider the translate classes of C, $C + x = \{y + x | y \in C\}$, where $x \in \mathbb{F}^n$. If C is linear then the translate classes are also called cosets. Each vector of $\mathbb{F}^n$ of weight less or equal to e is in a different translate of C. A code C is called distance invariant if the weight distribution of $C+x$ is the same for any $x \in C$. If C is distance invariant and $\mathbf{0} \in C$ then the minimum weight and the minimum distance coincide.

For $u = (u_1, \cdots, u_n),\ v = (v_1, \cdots, v_n) \in \mathbb{F}^n$, the scalar product between u and v is $u \cdot v = u_1 v_1 + \cdots + u_n v_n$. If $u \cdot v = 0$ then u and v are called orthogonal. Let C be a code, we define the orthogonal code of C, denoted by $C^\perp$, as the set of vectors which are orthogonal to all codewords of C

$$C^\perp = \{u \in \mathbb{F}^n | u \cdot c = \mathbf{0}\ \forall c \in C\}.$$

When C is a linear code, $C^\perp$ is called the dual of the code C.

If $C \subseteq C^\perp$ then C is called a self-orthogonal code and, if $C = C^\perp$ then C is called a self-dual code.

Two structural properties of codes are the rank and the kernel. The rank of C, $rank(C)$, is the dimension of the subspace spanned by C. If C is a code of length n and $rank(C) = n$, then we say that C is a full-rank code. The kernel of C is defined as

$$ker(C) = \{x \in C | C = C + x\};$$

and it is the set of vectors in C that leave C invariant under translation. In general, if $\mathbf{0} \in C$, then $ker(C)$ is a linear subspace. C can be written as the union of cosets of $ker(C)$, and $ker(C)$ is the largest such linear code for which this is true (see [BGH83]). The dimension of the kernel of C is denoted by $dim(ker(C))$. If C is linear, then $ker(C) = C$ and $rank(C) = dim(ker(C))$. In some sense, the rank and kernel of a code give some information on its linearity.

The group of coordinate permutations $\pi : C \longrightarrow C$ is denoted by $Aut(C)$. An isometry of a binary code is a distance-preserving 1-1 mapping $\varphi : C \longrightarrow C$. An

isometry φ of $\mathbb{F}^n$ can always be represented by a translation plus a coordinate permutation, i.e., $\varphi(y) = x + \pi(y)$ (see [BE48]). Isometries of a code form a group, $Iso(C)$. Given two codes, $C_1,\ C_2$, we say that these codes are isomorphic if there exists a coordinate permutation π such that $C_1 = \pi(C_2)$. C_1 is equivalent to C_2 if there exist an isometry φ such that $C_1 = \varphi(C_2)$.

Let C be a code in $\mathbb{F}^n$ and $\star$ an operation defined in C. We will write $(C, \star)$ to emphasize this operation. Assume the operation $\star$ induces an action $\star : C \times \mathbb{F}^n \longrightarrow \mathbb{F}^n$. The action $\star$ is a Hamming-compatible action if

$$d(x, x \star v) = \mathrm{wt}(v), \tag{2.3}$$

for all $x \in C$ and for all $v \in \mathbb{F}^n$.

A binary code $(C, \star)$ of length n is a Hamming-compatible group code if $(C, \star)$ is a group and it is possible to extend $\star : C \times \mathbb{F}^n \longrightarrow \mathbb{F}^n$ to a Hamming-compatible action.

2.2 Linear codes

Let $C \subset \mathbb{F}^n$ be a code. If C is a linear code we will denote it by $C(n, k)$, where n is the length of the code and k is its dimension, that is, the dimension of the subspace C in $\mathbb{F}^n$. The number of codewords is $|C| = 2^k$. Note that $rank(C) = dim(ker(C)) = k$.

If C is a linear code, then $C + x = C$ for all $x \in C$; hence, every linear code is a distance-invariant code. As a consequence, the minimum weight and distance coincide. We can also consider the code as $(C, +)$, where $+$ is the usual sum of vectors in $\mathbb{F}^n$, that is, a Hamming-compatible group code.

Let C be a linear code. As C is a linear subspace in $\mathbb{F}^n$ of dimension k, there exist k linearly independent codewords $x_1, \cdots, x_k$ in C such that

$$C = < x_1, \cdots, x_k >,$$

where $x_i = (x_{i1}, \cdots x_{in}) \in C$. So, the matrix

$$G = \begin{pmatrix} x_{11}, & \cdots, & x_{1n} \\ \vdots & \vdots & \vdots \\ x_{i1}, & \cdots, & x_{in} \\ \vdots & \vdots & \vdots \\ x_{k1}, & \cdots, & x_{kn} \end{pmatrix} \tag{2.4}$$

is called a generator matrix of $C(n,k)$. In this way, any codeword $c \in C$ is given by a linear combination of the rows of G

$$c = \lambda_1 x_1 + \cdots + \lambda_k x_k,$$

that is,

$$c = (\lambda_1, \cdots, \lambda_k)G,$$

where $\lambda_1, \cdots, \lambda_k \in \mathbb{F}$.

The dual code $C^\perp$ has dimension $n-k$; in fact, it is a linear code $C^\perp(n, n-k)$. Let H be a generator matrix of $C^\perp$. $x \in \mathbb{F}^n$ is a codeword of C if and only if $xH^t = \mathbf{0}$, where H^t denotes the transposed matrix of H. H is called a parity check matrix of the code C. Moreover, if G is the generator matrix of C, then G is the parity check matrix of $C^\perp$.

A linear code is a systematic code if it has a generator matrix that contains the identity matrix of dimension k. We assume, without loss of generality, that the identity matrix is given by the first k coordinates. Let C be a binary linear systematic code with generator matrix

$$G = \left(\begin{array}{c|c} Id & P \end{array} \right)$$

where Id is the $(k \times k)$ identity matrix and P is a $\big(k \times (n-k)\big)$ matrix. Then, a parity check matrix of C is the matrix given by

$$H = \left(\begin{array}{c|c} P^\perp & Id \end{array} \right)$$

where Id is the $\big((n-k) \times (n-k)\big)$ identity matrix.

Example 2.2.1. *Hamming codes.*

A Hamming code $\mathcal{H}_r$ is a linear code $\mathcal{H}_r(n = 2^r - 1, k = 2^r - 1 - r)$ with minimum distance $d = 3$, for $r \in \{2, 3, ...\}$. The $\big((n-k) \times n\big)$-matrix, H, with columns all the different non-zero vectors of length $n - k$ is a parity check matrix of $\mathcal{H}_r$. Then,

$$\mathcal{H}_r = \{x \in \mathbb{F}^n | xH^t = 0\}$$

Let $r = 3$, then $n = 7$ and $k = 4$. Let H be a parity check matrix of $\mathcal{H}_3$:

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

A generator matrix of $\mathcal{H}_3$ is

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

The codewords of $\mathcal{H}_3$, generated by the rows of G, are:

0000000	1111111
1000011	0111100
0100101	1011010
0010110	1101001
1110000	0001111
0011001	1100110
0101010	1010101
1001100	0110011

Note that the weight distribution of $\mathcal{H}_3$ is

$$\{1, 0, 0, 7, 7, 0, 0, 1\}.$$

The following theorem, that can be found in [MS77], shows that the weight enumerator of the dual code $C^{\perp}(n, n-k)$ of a binary linear code $C(n,k)$ is uniquely determined by a linear transformation of the weight enumerator of $C(n,k)$.

Theorem 2.1 (MacWilliams identity). *Let $C(n,k)$ be a linear code and $C^{\perp}(n, n-k)$ its dual, then*

$$W_{C^{\perp}}(X,Y) = \frac{1}{|C|} W_C(X+Y, X-Y).$$

Example 2.2.2. *Let $\mathcal{H}_3(7,4)$ be the Hamming code defined in Example 2.2.1. Then*

$$W_{\mathcal{H}_3}(X,Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7$$

$$W_{\mathcal{H}_3^{\perp}}(X,Y) = X^7 + 7X^3Y^4$$

It is easy to check that these weight enumerators verify the MacWilliams identity.

For more information about Hamming codes and linear codes in general, see [MS77].

2.3 Perfect codes

A binary code C of length n is perfect if for some integer $r \geq 0$ every $x \in \mathbb{F}^n$ is within distance r from exactly one codeword of C. Note that this definition coincides with the one given in the last section with $r = e$. C will be called perfect e-error correcting code or e-perfect code to emphasize the parameter e.

It is shown in [Tie73] and [ZL73] that the only binary perfect codes of length n are:

- trivial codes:
  - $\mathbb{F}^n$: $d = 1$ and $e = 0$.
  - $\{x\}$: $e = n$.
- repetition code, $\{\mathbf{0}, \mathbf{1}\}$ (and equivalents): n odd, $d = n$ and $e = \dfrac{n-1}{2}$.

- binary Golay code: $n = 23$, $d = 7$ and $e = 3$.

- 1-perfect codes: $n = 2^m - 1$, $d = 3$ and $e = 1$.

For any $m \geq 2$, there exists a Hamming code of length $n = 2^m - 1$. Moreover, if C is a 1-perfect code, then the weight distribution of C is the same as the weight distribution of a Hamming code with the same length. For $n = 3$, the Hamming code is, in fact, the repetition code of length 3. If $n = 7$, then the Hamming code is the only 1-perfect code up to equivalence. In the case $e = 3$, the Golay code is also unique up to equivalence (see [Ple68],[Sno73],[DG75]). Thus, the only parameters for which there exists nonequivalent binary perfect codes are $e = 1$ and $n = 2^m - 1$ with $m \geq 4$.

2.3.1 STS and invariants of 1-perfect codes

A 1-perfect linear code of length $n = 2^m - 1$ is equivalent to a Hamming code. The nonlinear 1-perfect codes are, however, not fully classified. There are many invariants of 1-perfect codes that are used to study these codes and to try to distinguish between nonisomorphic 1-perfect codes.

The two main invariants of such codes, even though they do not classify them completely, are the rank and the dimension of the kernel. They were defined in Section 2.1 and, due to the importance of these invariants, they are studied in greater details along the dissertation. Other invariants are those related to the Steiner triple systems. To give these invariants, it is necessary to define the Steiner triple system and see its relationship with 1-perfect codes.

A Steiner triple system is an ordered pair (V, B) where V is a finite set of points called vertices, and B is a set of 3-subsets of V called blocks such that each pair of elements of V is contained in exactly one block of B. If $n = |V|$, then we say that n is the order of the Steiner triple system and it is denoted by $STS(n)$ or simply, STS.

Example 2.3.1. *Let* $V = \{1, 2, \cdots, 7\}$ *be the set of vertices and*

$$B = \{(1, 6, 7), (2, 5, 7), (3, 5, 6), (1, 2, 3), (3, 4, 7), (2, 4, 6), (1, 4, 5)\}.$$

be the set of blocks. Then, (V, B) *is a Steiner triple system of order* 7 *and it is called the projective plane of order* 2 *or the Fano plane. The Figure 2.1 shows this* $STS(7)$.

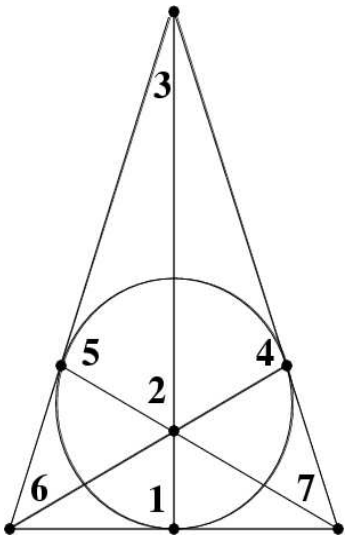

Figure 2.1: STS(7)

Given two $STS(n)$, (V, B) and (V, B'), we say that they are isomorphic if there exists a permutation π on the set V such that $B = \pi(B')$.

Proposition 2.2 ([AJMJ67],[GvT75]). *If* C *is a* 1*-perfect code of length* n *containing the zero vector, then the minimum weight codewords (of weight* 3*) in the code form an* $STS(n)$ *by considering blocks as* $\{(i, j, k)\}$ *where* (i, j, k) *are the support of all the codewords of weight* 3 *in* C.

The STS obtained in this way is denoted STS_0.

Example 2.3.2. *Consider the Hamming code $\mathcal{H}_3$ of Example 2.2.1. The following table shows the codewords of weight 3 in $\mathcal{H}_3$ and the blocks related to them:*

$$\begin{aligned} 1000011 &- (1,6,7) \\ 0100101 &- (2,5,7) \\ 0010110 &- (3,5,6) \\ 1110000 &- (1,2,3) \\ 0011001 &- (3,4,7) \\ 0101010 &- (2,4,6) \\ 1001100 &- (1,4,5) \end{aligned}$$

From $\mathcal{H}_3$, it yields the $STS(7)$ (V,B), with $V=\{1,2,\cdots,7\}$, and

$$B=\{(1,6,7),(2,5,7),(3,5,6),(1,2,3),(3,4,7),(2,4,6),(1,4,5)\}.$$

Note that this $STS(7)$ coincides with the one given in 2.3.1. In fact, $STS(7)$ is unique up to isomorphism.

Let C be a 1-perfect code. Let $v \in C$. The set of codewords $w \in C$ at distance three from v is a Steiner triple system, denoted by STS_v, taking as the set of blocks B the support of all the vectors $v+w$, where w is at distance 3 from v.

Note that starting from a 1-perfect code C, we can obtain different STS's; for instance, STS_0, STS_v, etc. These STS's may or may not be unique. In that sense, we will give some algebraic results that limit the possibilities of the STS's obtained.

Proposition 2.3. *([Bor98]) A 1-perfect code C of length $n \geq 3$ is a linear code if and only if*

$$STS_v = STS_w, \text{ for all } v,w \in C.$$

Proposition 2.4. *([Bor98]) Let C be 1-perfect code of length $n \geq 3$ with kernel $ker(C)$. If $v \in ker(C)+w$, for $v,w \in C$, then $STS_v = STS_w$.*

If two codes C, C' are isomorphic, then the Steiner triple systems obtained from C and C' by Proposition 2.2 are isomorphic and the invariants related to them coincide.

Nevertheless, two nonisomorphic codes can give the same STS and, hence, the same invariants. In this way, invariants related with STS's give information about the nonisomorphism of 1-perfect codes.

On the other hand, the number of nonisomorphic $STS(n)$ (see [MPR83]), $N(n)$, is given by

$$N(n) = n^{n^2(1/6+o(1))}.$$

Hence, there are 80 nonisomorphic $STS(15)$, that are listed in [WCC19], but for $n = 31$ there are $\approx 10^{200}$ nonisomorphic STS's. That way, the only invariants related with STS's given in this section are those related to $STS(15)$.

There are some invariants that do not distinguish completely the nonisomorphic STS's. Among these invariants, in [MPR83] we can find the cycle vector, cycles through elements, the compact train or the representative k-coloring of triples. Also in [Dej94] we find the STS-graph invariant, $H(C)$, that belongs to this class.

Now we will list some complete invariants of STS's which allow us to distinguish completely nonisomorphic STS's. The first complete invariants were the cycle structure and trains that appeared in [MPR83]. Later, we can find fragments in [LeV95] and the characteristic vector in [Rif99]. Finally, in [DD02] there is a refinement of $H(C)$, $H_{ker(C)}(C)$, called the STS-graph of C modulo the kernel.

2.3.2 Constructions of 1-perfect codes

Nonlinear 1-perfect codes were first constructed by Vasil'ev. A generalization of the Vasil'ev construction was given by Mollard. Other constructions of nonlinear 1-perfect codes have been subsequently presented by Phelps, Solov'eva and Bauer *et al.* Some of these constructions will be shown in this section. To obtain more information about constructions of 1-perfect codes, see [EV94] and [Vil01].

A code C of length $n + 1 = 2^m$ is extended perfect if it is obtained from a perfect code of length n by extending with either an even or odd parity coordinate.

Vasil'ev construction

For $v \in \mathbb{F}^n$, define $p(v) = \mathrm{wt}(v) \pmod 2$. Let C_n be a 1-perfect code of length $n = 2^m - 1$. Let $f : C_n \longrightarrow \{0, 1\}$ be an arbitrary mapping such that $f(\mathbf{0}) = 0$ and $f(c_1) + f(c_2) \neq f(c_1 + c_2)$ for all c_1, c_2 and $c_1 + c_2 \in C_n$.

Proposition 2.5 ([Vas62]). *The code C_{2n+1} defined by*

$$C_{2n+1} = \{(v|v + c|p(v) + f(c)) : v \in \mathbb{F}^n, c \in C_n\},$$

where $|$ denotes the concatenation, is perfect.

Mollard gives a construction that is, in a sense, a generalization of the one given in Proposition 2.5. It is defined as follows.

Let $x = (x_{11}, x_{12}, \cdots, x_{1n_2}, x_{21}, x_{22}, \cdots, x_{n_1n_2}) \in \mathbb{F}^{n_1n_2}$. Define the generalized functions $p_1(x) = (\sigma_1, \cdots, \sigma_{n_1}) \in \mathbb{F}^{n_1}$ and $p_2(x) = (\sigma'_1, \cdots, \sigma'_{n_2}) \in \mathbb{F}^{n_2}$ by setting $\sigma_i = \sum_{j=1}^{n_2} x_{ij}$ and $\sigma'_j = \sum_{i=1}^{n_1} x_{ij}$. Let C_1 and C_2 be two 1-perfect codes of lengths n_1 and n_2, respectively. Let $f : C_1 \longrightarrow \mathbb{F}^{n_2}$ be an arbitrary mapping.

Proposition 2.6 ([Mol86]). *The code F defined by*

$$F = \{(x|c_1 + p_1(x)|c_2 + p_2(x) + f(c_1)) : x \in \mathbb{F}^{n_1n_2}, c_1 \in C_1, c_2 \in C_2\}$$

is a 1-perfect code of length $n = n_1n_2 + n_1 + n_2$.

Note that for $n_2 = 1$ it coincides with the Vasil'ev construction.

Doubling construction

The following construction of 1-perfect codes of length $2n+1$ from 1-perfect codes of length n is due to Phelps and Solov'eva.

Let e_i be the vector with 1 in the coordinate i and 0 elsewhere. Let $X \subset \mathbb{F}^n$ and $Y \subset \mathbb{F}^m$. Then, the direct sum of X and Y, denoted by $X \oplus Y \in \mathbb{F}^{n+m}$ is as follows:

$$X \oplus Y = \{(x, y)|x \in X, y \in Y\}$$

Let C_1 be a 1-perfect code of length n and let C_2^* be an extended 1-perfect code of length $n+1$.

Proposition 2.7 ([Phe83], [Sol81]). *The code*

$$C = (C_1 \oplus C_2^*) \bigcup_{i=1}^{n} (C_1 + e_i \oplus (C_2 + e_{\pi(i)})^*),$$

where π is a permutation on the set $\{1, 2, \cdots, n\}$, is a 1-perfect code of length $2n+1$.

The next proposition gives a more general variant of the above construction.

Let $\mathbb{E}^n$ be the set of all even weight vectors of $\mathbb{F}^n$. Let $C_0^*, C_1^*, \cdots, C_n^*$ and $D_0^*, D_1^*, \cdots, D_n^*$ be partitions of $\mathbb{E}^{n+1}$ and $\mathbb{F}^{n+1} \backslash \mathbb{E}^{n+1}$ respectively, into extended 1-perfect codes by extending with an even parity coordinate the first ones and with an odd parity coordinates the second ones. Let π be a permutation on the set $\{0, 1, \cdots, n\}$.

Proposition 2.8 ([Phe83], [Sol81]). *The code C defined by*

$$\bigcup_{i=1}^{n} C = \{(c|d) : c \in C_i^*, d \in D_{\pi(i)}^*\}$$

is an extended 1-perfect code of length $2n+2$.

Puncturing any coordinate of C yields a 1-perfect code of length $2n+1$.

Switching construction

This construction consists of starting with a 1-perfect code C of length n and switching out one specially selected set of codewords $S \subset C$ for another set of vectors S'. The resulting code $C' = (C \backslash S) \cup S'$ is a 1-perfect code.

The first approach of this construction was due to Solov'eva in 1988 (see [Sol88]). Others approaches can be found in [Sol00], [AS97] and [PL95]. We will present the one due to Phelps and LeVan.

For a 1-perfect code C of length n, we define the minimum distance graph of C as a graph $G(C) = (C, E)$ with the codewords in C as vertices and edges $[x, y] \in E$ if and only if $d(x, y) = 3$.

We define a subgraph $G_i(C) = (C, E_i)$ as the subset E_i of all the edges in $G(C)$ where the codewords x and y disagree at the i^{th} coordinate (see [Sol88]).

Define T_i to be the linear subcode of a Hamming code, H, generated by the codewords of weight 3 having a 1 in the i^{th} component. There will be a path from x to y in $G_i(H)$ if and only if there is a sequence of codewords of weight 3 $t_1, t_2, \cdots, t_s \in T_i$ such that $x + t_1 + t_2 + \cdots + t_s = y$, that is equivalent to $y \in T_i + x$. Thus, $T_i + x$ is a component of $G_i(H)$.

Proposition 2.9 ([PL95]). *Given a Hamming code $\mathcal{H}_m$ of length $n = 2^m - 1$, let T_i be the linear subcode of $\mathcal{H}_m$, $x_i \in \mathcal{H}_m$. Then*

$$C = (\mathcal{H}_m \backslash (T_i + x_i)) \cup (T_i + x_i + e_i)$$

is a nonlinear 1-perfect code of length n, $\forall i \in \{1, \cdots, n\}$.

2.3.3 Rank and kernel of 1-perfect codes

Let C be a 1-perfect code. We have seen that if C is linear, then $dim(ker(C))$ is equal to the dimension of the code. When C is a nonlinear code, then

$$dim(ker(C)) \leq \log_2|C| - 2$$

Moreover, as 1-perfect codes are diametrically opposite, then **0** and **1** belong to the kernel and hence, $dim(ker(C))$ is at least 1. Indeed, if $n = 2^m - 1$ is the length of the code, then $dim(ker(C)) \in \{1, 2, \cdots, 2^m - m - 3\}$ or $dim(ker(C)) = 2^m - m - 1$ and C is a linear code.

Etzion and Vardy proved in [EV94] that there exist 1-perfect codes with any possible rank. In [PL95] Phelps and LeVan obtained 1-perfect codes with kernels of all possible sizes:

$$rank(C) \in \{n-m, \cdots, n\}$$

$$dim(ker(C)) \in \{1, 2, \cdots, n-m-2, n-m\}$$

and they are related. The natural question, appeared in [EV98], was for which pairs of values (r, k) there exist a 1-perfect codes having $rank(C) = r$ and $dim(ker(C)) = k$.

There are some theorems in [VP02] that establish the exact upper and lower bounds on the kernel dimension by means of the rank of codes of length $n = 2^m - 1$ except for the case $rank(C) = n$ and $m \geq 4$. Lately, in [EV98], it is shown that for $m \geq 10$ this upper bound is tight for full-rank codes. Finally, Solov'eva *et al.* have determined in [AHS03] all allowable parameters (r, k) except to in the case of full-rank codes $(r = n)$.

2.4 Propelinear codes

In 1989 the propelinear structure was introduced in [RBH89] with the purpose of studying the algebraic structure of completely regular codes (not necessarily linear codes) associated with distance-regular e-latticed graphs. Lately, this structure was studied apart from graphs, in propelinear codes, as we will do in this dissertation.

Let C be a subset of $\mathbb{F}^n$ and let $\mathcal{S}_n$ denote the symmetric group of permutations of the set $\{1, 2, \cdots, n\}$. Let $\pi \in \mathcal{S}_n$. For any vector $v = (v_1, \cdots, v_n) \in \mathbb{F}^n$, we write $\pi(v)$ to denote the vector $(v_{\pi^{-1}(1)}, \cdots, v_{\pi^{-1}(n)})$. We will denote the identity permutation by Id.

Definition 2.4.1. *$C \subseteq \mathbb{F}^n$ is called a propelinear code if $\forall v \in C$ there exists $\pi_v \in \mathcal{S}_n$ such that:*

i) $\forall c \in C : v + \pi_v(c) \in C$,

ii) $\forall c \in C : \pi_v \circ \pi_c = \pi_m$, *where* $m = v + \pi_v(c)$.

2.4.1 Algebraic structure of propelinear codes

Let C be a propelinear code. Given $x, y \in C$ we define the binary operation $\star$ as

$$x \star y = x + \pi_x(y). \tag{2.5}$$

The operation $\star$ is closed in C and for all $x \in C$ we have that $x \star y = x \star z$ if and only if $y = z$ and hence, $C \star C = C$. The vector $\mathbf{0}$ is always a codeword in C with permutation associated $\pi_0 = Id$, the identity permutation. Thus, as we can see in ([RBH89]), $(C, \star)$ is a group, which is not Abelian in general, with $\mathbf{0}$ as the identity element, and $x^{-1} = \pi_x^{-1}(x)$ as the inverse element of $x \in C$. The set $\Pi = \{\pi_x |\ x \in C\}$ is a subgroup of $\mathcal{S}_n$ with the usual composition of permutations. There are different ways to refer to a propelinear code C: (C, Π) is used to emphasize the permutation group Π whereas $(C, \star)$ is used to emphasize the operation $\star$. A general propelinear code is only denoted by C.

Note that if $\Pi = \{Id\}$, then C is a linear code. Hence, it is clear that every linear code is a propelinear code. However, it is possible to construct a linear code with different propelinear structures as we can see in ([PR97b]).

Let $(C, \star)$ be a propelinear code. For any $x \in C$ define $\phi_x : C \longrightarrow C$ by $\phi_x(y) = x \star y = x + \pi_x(y)$, for $y \in C$. $\phi_x \in Iso(C)$ for all $x \in C$. The following statements can be found in [PR02].

Lemma 2.10. *Let $(C, \star)$ be a propelinear code. $G = \{\phi_x | x \in C\}$ is a subgroup of $Iso(C)$.*

Proof: The operation in G is the composition of isometries; that is, $\phi_x\phi_y(z) = \phi_x(y + \pi_y(z)) = x + \pi_x(y + \pi_y(z)) = x \star y + \pi_x\pi_y(z) = x \star y + \pi_{x\star y}(z) = \phi_{x\star y}(z)$. $\phi_{\mathbf{0}}$ is the identity element and $\phi_x^{-1} = \phi_{x^{-1}}$, where $x^{-1} = \pi_x^{-1}(x)$.

∎

Proposition 2.11. *Let $(C, \star) \subset \mathbb{F}^n$ be a group. C is a propelinear code if and only if the group $Iso(C)$ contains a regular subgroup acting transitively on C.*

Proof: Let $(C, \star)$ be a propelinear code. By Lemma 2.10, $G = \{\phi_x | x \in C\}$ is a subgroup of $Iso(C)$. By definition of G it is clear that $|G| = |C|$. Now, given $w, v \in C$ there exist $x \in C$, $x = w \star v^{-1}$, such that $w = \phi_x(v)$:

$$\phi_x(v) = x + \pi_x(v) = w + \pi_w(v^{-1}) + \pi_w\pi_{v^{-1}}(v) = w + \pi_w(v^{-1}) + \pi_w(v^{-1}) = w.$$

Hence, G is a regular subgroup acting transitively on C.
Conversely, assume $Iso(C)$ contains a regular subgroup, G, acting transitively on C. Therefore $|C| = |G|$, and, for $x \in C$ there exist a unique $\phi \in G$ such that $x = \phi(0)$. Let call $\phi_x = \phi$, where $x = \phi(0)$. For $x \in C$, define $\pi_x(v) = x + \phi_x(v)$ and $x \star v = x + \pi_x(v) = \phi_x(v)$. With this operation, we claim that $(C, \star)$ is a propelinear code. First of all, we have to prove that $\forall x, v \in C$, $x + \pi_x(v) \in C$, but it is clear due to the fact that $x + \pi_x(v) = \phi_x(v)$ and $\phi_x \in Iso(C)$. Finally, we have to check that $\pi_x\pi_y = \pi_{x\star y}$. Note that $\phi_x\phi_y(0) = \phi_x(\phi_y(0)) = \phi_x(y) = x \star y = \phi_{x\star y}(0)$ by definition of ϕ, and hence $\phi_x\phi_y = \phi_{x\star y}$. Now, for all $v \in C$, $\pi_x\pi_y(v) = \pi_x(y + \phi_y(v)) = \pi_x(y) + \pi_x(\phi_y(v)) = x + \phi_x(y) + x + \phi_x(\phi_y(v)) = \phi_x(y) + \phi_x\phi_y(v) = x \star y + \phi_{x\star y}(v) = \pi_{x\star y}(v)$; hence, $\pi_x\pi_y = \pi_{x\star y}$. ∎

2.4.2 Translation-invariant propelinear codes

The operation defined in (2.5), $\star : C \times C \longrightarrow C$, can be extended to

$$\begin{array}{rcl} \star : C \times \mathbb{F}^n & \longrightarrow & \mathbb{F}^n \\ (u, v) & \longrightarrow & u \star v = u + \pi_u(v) \end{array}$$

Lemma 2.12. *If $(C, \star)$ is a propelinear code, then:*

$$d(u, v) = d(x \star u, x \star v),\ \forall x \in C,\ \forall u, v \in \mathbb{F}^n.$$

Proof: The claim is trivial and can be found in [RBH89] and [BR99]. ∎

Corollary 2.13. *A binary propelinear code $(C, \star)$ is a Hamming-compatible group code.*

Proof: Let $(C, \star)$ be a binary propelinear code. By Lemma 2.12 for every $x \in C$, $v \in \mathbb{F}^n$

$$d(x, x \star v) = d(\mathbf{0}, v) = \mathrm{wt}(v).$$

Therefore, the action $\star$ is Hamming compatible and hence $(C, \star)$ is a Hamming-compatible group code. ∎

A propelinear code $(C, \star)$ is a translation-invariant code if

$$d(x, y) = d(x \star u, y \star u);\ \forall x, y \in C,\ \forall u \in \mathbb{F}^n.$$

Translation-invariant codes have been studied by J. Pujol and J. Rifà in [PR97b] where we find the characterization of conditions of propelinear codes to be translation-invariant and a classification of these codes. Now we will show some of these results.

Lemma 2.14. *Let $(C, \star)$ be a propelinear code of length n. C is translation-invariant if and only if for all $x \in \mathbb{F}^n$ and for all $u \in C$*

$$wt(u) = d(x, u \star x).$$

As a corollary of this lemma, we obtain the following necessary condition for a propelinear code to be a translation-invariant code.

Corollary 2.15. *If C is translation-invariant propelinear code of length n, then $|C| = 2^k$, for some $k \leq n$.*

For examples of non-translation-invariant propelinear codes see [PR97b].

A translation-invariant propelinear code C is a subgroup of the group $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$, where $k_1 + 2k_2 + 4k_3 = n$ is the length of the code and Q_8 is the non Abelian quaternion group of eight elements (see [PR97b]). In this way, we make a partition of the set of coordinates $\{1, \cdots, n\}$ in three subsets, X, Y, Z, such that:

- $|X| = k_1$, $|Y| = 2k_2$ and $|Z| = 4k_3$
- $C_X = \{(c_{i_1}, \cdots, c_{i_{k_1}}) | (c_1, \cdots, c_n) \in C, i_1, \cdots, i_{k_1} \in X\}$, is a linear code,
  $C_Y = \{(c_{i_1}, \cdots, c_{i_{2k_2}}) | (c_1, \cdots, c_n) \in C, i_1, \cdots, i_{2k_2} \in Y\}$ is a $\mathbb{Z}_4$-code and
  $C_Z = \{(c_{i_1}, \cdots, c_{i_{4k_3}}) | (c_1, \cdots, c_n) \in C, i_1, \cdots, i_{4k_3} \in Z\}$ is a quaternion code.

We will say that such a code C, is a code of type (k_1, k_2, k_3). Note that a code of type $(k_1, 0, 0)$ is a linear code and a code of type $(0, k_2, 0)$ is a $\mathbb{Z}_4$-linear code. Moreover, as Q_8 is not Abelian, every translation-invariant Abelian propelinear code is of type $(k_1, k_2, 0)$.

Example 2.4.1 ([PR97b]). *Let $a = (1,0,1,0)$ and $b = (1,0,0,1)$ be in $\mathbb{F}^4$ with permutations associated $\pi_a = (1,2)(3,4)$ and $\pi_b = (1,3)(2,4)$ respectively. Notice that*

$$a^4 = Id,\ a^2 = b^2,\ a \star b \star a = b.$$

The propelinear code C generated by a and b is called the quaternion propelinear code and it is isomorphic to the quaternion group Q_8:

$$\begin{aligned}(C, \Pi) =< (a, \pi_a), (b, \pi_b) >= \ & \{(\mathbf{0}, Id), (a, \pi_a), \\ & (a^2, Id), (a^3, \pi_a), \\ & (b, \pi_b), (a \star b, \pi_{a\star b}), \\ & (a^2 \star b, \pi_b), (a^3 \star b, \pi_{a\star b})\}\end{aligned}$$

C is of type $(0,0,1)$.

A code C not only have a unique representation as a code of type (k_1, k_2, k_3); that is, there exist codes of type (k_1, k_2, k_3) that can be also seen as codes of type $(k_1', k_2', k_3') \neq (k_1, k_2, k_3)$. The Hamming code of length 7 is a 1-perfect linear code and, hence, a translation-invariant propelinear code of type $(7, 0, 0)$. In [PR97b], it is shown that the Hamming code of length 7 is also a code of type $(3, 2, 0)$ and a code of type $(3, 0, 1)$.

Example 2.4.2. *The Hamming code $\mathcal{H}_3$ defined in Example 2.2.1 is isomorphic to the following translation-invariant propelinear codes:*

- $$\begin{aligned}(C_1, \Pi) = \ < \ & ((1,0,0,0,0,1,1), Id), \\ & ((0,1,0,0,1,0,1), Id), \\ & ((0,0,1,0,1,1,0), Id), \\ & ((0,0,0,1,1,1,1), Id) >\end{aligned}$$

C_1 *is a linear code of type* $(7, 0, 0)$.

- $$\begin{aligned}(C_2, \Pi) = \; < \; & ((1,0,1,0 \,|\, 1,0,0), (1,2)(3,4)), \\ & ((1,0,0,1 \,|\, 0,1,0), (1,2)(3,4)), \\ & ((1,1,1,1 \,|\, 1,1,1), Id) >\end{aligned}$$

  C_2 *is of type* $(3, 2, 0)$ *where the first four coordinates make up a* $\mathbb{Z}_4$*-linear code and the last three coordinates correspond to the linear ones.*

- $$\begin{aligned}(C_3, \Pi) = \; < \; & ((1,0,1,0 \,|\, 1,0,0), (1,2)(3,4)), \\ & ((1,0,0,1 \,|\, 0,1,0), (1,3)(2,4)), \\ & ((1,1,1,1 \,|\, 1,1,1), Id) >\end{aligned}$$

  C_3 *is of type* $(3, 0, 1)$. *As in the last code, the three last coordinates are linear but in this case, the first coordinates make up a quaternion code. Notice that this code is not Abelian:*

$$a \star b = (1,1,0,0,1,1,0) \neq (0,0,1,1,1,1,0) = b \star a.$$

Finally, within translation-invariant propelinear codes, we would like to characterize those codes being 1-perfect. The different available values (k_1, k_2, k_3) of such codes were given in[PR97b].

Let $C \subset \mathbb{F}^n$ be a 1-perfect translation-invariant propelinear code of type (k_1, k_2, k_3) and length n. There are some conditions over k_1, k_2 and k_3:

- $k_1 \neq 0$, because n is odd.
- $k_3 \leq 1$.
- If $k_3 = 1$, $k_2 = 0$.

Let C be a 1-perfect translation-invariant propelinear code of type (k_1, k_2, k_3). If $k_3 > 0$ then, necessarily, $k_3 = 1$ and also $k_2 = 0$; hence, C is of type $(n - 4, 0, 1)$.

From [BR99] $n = 2^t - 1$, with $t \geq 3$; moreover, there is only one 1-perfect propelinear code of type $(n-4, 0, 1)$.

Theorem 2.16 ([PR97b]). *Let C be a 1-perfect translation-invariant propelinear code of type (k_1, k_2, k_3). If $k_3 > 0$, then C is the Hamming code of length 7 and of type $(3, 0, 1)$.*

Let C be a 1-perfect translation-invariant propelinear code. If the length of the code is $n \geq 7$ then, by Theorem 2.16, $k_3 = 0$ or C is a Hamming code of length 7 and it also has an structure of type $(7, 0, 0)$ or $(3, 2, 0)$. If the length of the code is 3, then it has a propelinear structure of type $(1, 1, 0)$. Then, if C is a 1-perfect translation-invariant propelinear code of length n, C is a code of type $(k, \frac{n-k}{2}, 0)$ with an Abelian structure and it is isomorphic to a subgroup of $\mathbb{Z}_2^k \times \mathbb{Z}_4^{\frac{n-k}{2}}$.

Chapter 3

$\mathbb{Z}_4$-codes

Recently, $\mathbb{Z}_4$-codes have appeared in a large number of articles, for instance [HKC$^+$94], [BSBM97], [AGOS99], [BSC95], [CMKH96], ... There are, basically, two different motivations to study these codes. Firstly, the best known nonlinear binary codes such as the Nordstrom-Robinson, Kerdock, Preparata, Goethals, and Delsarte-Goethals codes contain a larger number of codewords than any known linear codes with a fixed block size. Hammons, Kumar, Caldermark, Sloane, and Sole [HKC$^+$94] discovered that these codes have a structure of $\mathbb{Z}_4$-codes via the Gray map. And secondly, it was shown that self-dual $\mathbb{Z}_4$-codes are closely related to unimodular lattices via Construction A_4 (see, for example [BSC95] or [HSG99]).

This chapter is organized as follows. Section 3.1 include weights, distances and weight enumerators. The different extensions of the usual Gray map is given in Section 3.2. Then, binary images under the Gray map of quaternary codes are studied in Section 3.3, and the linearity of such codes in Section 3.4. Cyclic codes over $\mathbb{Z}_4$ and Galois rings are presented in Section 3.5 to conclude, in Section 3.6 with the most important example of cyclic code over $\mathbb{Z}_4$, the Kerdock code and, moreover, its $\mathbb{Z}_4$-dual code, the Preparata-like code.

3.1 Weights and distances

A quaternary code, or $\mathbb{Z}_4$-code, $\mathcal{C}$ of length n is a linear block code over $\mathbb{Z}_4$; that is, $\mathcal{C}$ is an additive code of $\mathbb{Z}_4^n$. We define different weights in $\mathbb{Z}_4$ apart from the Hamming weight, wt() defined in chapter 2, namely the Lee weight and the Euclidean weight. The Lee weights of the elements $0, 1, 2$, and 3 of $\mathbb{Z}_4$ are $0, 1, 2$, and 1, respectively, and the *Lee weight* $\mathrm{wt}_L(x)$ of $x \in \mathcal{C}$ is the rational sum of the Lee weights of its components. We define the Lee distance as we defined the Hamming distance by means of the Hamming weight; in this sense, the Lee distance, $d_L(x, y)$ of two vectors $x, y \in \mathcal{C}$ is $\mathrm{wt}_L(x - y)$.

In the literature about $\mathbb{Z}_4$-codes, there are different definitions for the Euclidean distance and the Euclidean weight. We show two versions where the weights of the elements of $\mathbb{Z}_4$ are different from each other.

Usually, when the $\mathbb{Z}_4$-codes are used in communications, the elements $0, 1, 2$ and 3 in $\mathbb{Z}_4$ are represented, respectively, as $i^0 = 1$, $i^1 = i$, $i^2 = -1$ and $i^3 = -i$ in the complex plane. In this way, in [HKC+94] and [Wan97], $d_E^2(i^a, i^b)$ is defined as the square of the usual Euclidean distance between i^a and i^b in the complex plane. If $x = (x_1, \ldots, x_n) \in \mathbb{Z}_4^n$, then $i^x = (i^{x_1}, \ldots, i^{x_n})$. Thus, the square of the Euclidean distance between two vectors $x, y \in \mathcal{C}$ is given by

$$d_E^2(i^x, i^y) = \sum_{j=1}^{n} d_E^2(i^{x_j}, i^{y_j}).$$

With this definition Zhe-Xian Wan obtained the Lee distance from the Euclidean distance as

$$d_L(x, y) = \frac{1}{2} d_E^2(i^x, i^y).$$

Another definition was introduced in [BS94] (see also [BSC95]). The Euclidean weight of the elements $0, 1, 2$, and 3 of $\mathbb{Z}_4$ are respectively $0, 1, 4$ and 1, and the Euclidean weight of an element $x \in \mathcal{C}$, $\mathrm{wt}_E(x)$, is the rational sum of the Euclidean

weights of its components. Hence, the Euclidean distance between two vectors $x, y \in \mathcal{C}$, $d_E(x, y)$, is $\mathrm{wt}_E(x - y)$.

Note that the Euclidean weights of the elements $0, 1, 2$ and 3 of $\mathbb{Z}_4$ given in the first definition are, respectively, $0, \sqrt{2}, 2$ and $\sqrt{2}$ which are not the same values as those given in the second one. The first definition is used with modulations while the second one is used with lattices. In this section, we are going to use the first one that is the one related with the Lee distance.

In the previous chapter, we defined the minimum (Hamming) weight and distance. Similarly we define

$$min\{\mathrm{wt}_L(c)|c \in \mathcal{C}\ , c \neq 0\},\ min\{d_L(c, c')|c, c' \in \mathcal{C}\ , c \neq c'\}$$

and

$$min\{\mathrm{wt}_E(c)|c \in \mathcal{C}\ , c \neq 0\},\ min\{d_E(c, c')|c, c' \in \mathcal{C}\ , c \neq c'\}$$

to be the minimum Lee weight and distance and the minimum Euclidean weight and distance of $\mathcal{C}$, respectively.

For all $x, y \in \mathbb{Z}_4^n$, $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ we define the inner product of x and y by

$$x \cdot y = x_1 y_1 + \cdots + x_n y_n \bmod 4.$$

Hence, the notions of dual code ($\mathcal{C}^\perp$), self-orthogonal code ($\mathcal{C} \subseteq \mathcal{C}^\perp$), and self-dual code ($\mathcal{C} = \mathcal{C}^\perp$) are defined in the standard way (see [MS77]).

A self-dual $\mathbb{Z}_4$-code with Euclidean weight divisible by eight is called a Type II code.

Two codes are equivalent if one can be obtained from the other by permuting coordinates and (if necessary) changing the signs of certain coordinates. The automorphism group $Aut(\mathcal{C})$ of $\mathcal{C}$ is the group of all coordinate permutations and sign-changes that preserve the set of codewords. Codes differing by only a permutation coordinates are called permutation-equivalent.

Any $\mathbb{Z}_4$-code $\mathcal{C}$ is permutation-equivalent to a code $\mathcal{C}'$ with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2C \end{pmatrix},$$

where A and C are matrices over $\mathbb{Z}_2$ and B is a matrix over $\mathbb{Z}_4$. We say that $\mathcal{C}$ is of type $4^{k_1}2^{k_2}$. Notice that $\mathcal{C}$ is of type $4^{k_1}2^{k_2}$ if and only if $|\mathcal{C}| = 2^{2k_1+k_2}$ and the number of order 2 codewords is $2^{k_1+k_2}$

We can obtain the type of a $\mathbb{Z}_4$-linear code when vectors in the generator matrix have some specific properties. This is the case of the following lemma.

Lemma 3.1. *Let $v_1, \ldots, v_{k_1}, u_1, \ldots, u_{k_2}$ be k_1+k_2 linearly independent binary vectors. Then, the $\mathbb{Z}_4$-code generated by the matrix G with row vectors $v_1, \ldots, v_{k_1}$, $2u_1, \ldots, 2u_{k_2}$ is of type $4^{k_1}2^{k_2}$.*

Proof: In particular, $v_1, \ldots, v_{k_1}$ are linearly independent binary vectors and the matrix with row vectors $v_1, \ldots, v_{k_1}$ is permutation equivalent to a matrix of the form

$$\begin{pmatrix} I_{k_1} & A \end{pmatrix}$$

As $v_1, \ldots, v_{k_1}, u_1, \ldots, u_{k_2}$ are linearly independent binary vectors, then the matrix with these vectors as row vectors is permutation-equivalent to a matrix of the form

$$\begin{pmatrix} I_{k_1} & A_1 & B_1 \\ 0 & I_{k_2} & C_1 \end{pmatrix},$$

where $A = (A_1 \;\; B_1)$.

Similarly, we obtain that the matrix with row vectors $2v_1, \ldots, 2v_{k_1}, 2u_1, \ldots, 2u_{k_2}$ is permutation-equivalent to a matrix of the form

$$\begin{pmatrix} 2I_{k_1} & 2A_1 & 2B_1 \\ 0 & 2I_{k_2} & 2C_1 \end{pmatrix}.$$

Therefore the $\mathbb{Z}_4$-linear code, C, generated by G is the $\mathbb{Z}_4$-linear code generated by the matrix with row vectors $v_1, \ldots, v_{k_1}, 2v_1, \ldots, 2v_{k_1}, 2u_1, \ldots, 2u_{k_2}$ that is

permutation-equivalent to a code with generator matrix

$$\begin{pmatrix} I_{k_1} & A_1 & B_1 \\ 2I_{k_1} & 2A_1 & 2B_1 \\ 0 & 2I_{k_2} & 2C_1 \end{pmatrix}.$$

Note that the code generated by the last matrix coincides with the code generated by

$$\begin{pmatrix} I_{k_1} & A_1 & B_1 \\ 0 & 2I_{k_2} & 2C_1 \end{pmatrix},$$

and, therefore, C is of type $4^{k_1}2^{k_2}$. ∎

3.1.1 Weight enumerators

Let $\mathcal{C}$ be a $\mathbb{Z}_4$-code of length n. There are different weight enumerators related to the code $\mathcal{C}$. First, we define the complete weight enumerator (or c.w.e.) of $\mathcal{C}$ by

$$cwe_{\mathcal{C}}(W, X, Y, Z) = \sum_{c \in \mathcal{C}} W^{n_0(c)} X^{n_1(c)} Y^{n_2(c)} Z^{n_3(c)},$$

where $n_k(c)$ is the number of components of $c = (c_1, \ldots, c_n) \in \mathcal{C}$ that are congruent to $k \pmod 4$. Two codes differing by only a permutation of coordinates have the same c.w.e., but equivalent codes may have different c.w.e.'s. We define then the symmetrized weight enumerator (or s.w.e.), which is the appropriate weight enumerator for an equivalence class of codes. The s.w.e. is obtained by identifying X and Z in the c.w.e.:

$$swe_{\mathcal{C}}(W, X, Y) = cwe_{\mathcal{C}}(W, X, Y, X).$$

The Lee weight enumerator of $\mathcal{C}$ given by

$$Lee_{\mathcal{C}}(W, X) = \sum_{c \in \mathcal{C}} W^{2n - \mathrm{wt}_L(c)} X^{\mathrm{wt}_L(c)}$$

is obtained from the s.w.e. as

$$Lee_{\mathcal{C}}(W, X) = swe_{\mathcal{C}}(W^2, WX, X^2).$$

It is a homogeneous polynomial of degree $2n$. Finally, the Hamming weight enumerator is also obtained from the s.w.e. as

$$Ham_{\mathcal{C}}(W,X) = swe_{\mathcal{C}}(W,X,X).$$

The MacWilliams identity gives the weight enumerator for the dual code $\mathcal{C}^{\perp}$ in terms of the weight enumerator for the code $\mathcal{C}$ ([MS77],[HKC+94],[Wan97]):

$$cwe_{\mathcal{C}^{\perp}}(W,X,Y,Z) =$$
$$\frac{1}{|\mathcal{C}|} cwe_{\mathcal{C}}(W+X+Y+Z, W+iX-Y-iZ, W-X+Y-Z, W-iX-Y+iZ),$$

$$swe_{\mathcal{C}^{\perp}}(W,X,Z) = \frac{1}{|\mathcal{C}|} swe_{\mathcal{C}}(W+2X+Y, W-Y, W-2X+Y),$$

$$Lee_{\mathcal{C}^{\perp}}(W,X) = \frac{1}{|\mathcal{C}|} Lee_{\mathcal{C}}(W+X, W-X),$$

$$Ham_{\mathcal{C}^{\perp}}(W,X) = \frac{1}{|\mathcal{C}|} Ham_{\mathcal{C}}(W+3X, W-X).$$

3.2 The Gray map

It is known (see [HKC+94]) that binary codes such as the Nordstrom-Robinson, Kerdock, Preparata, Goethals, and Delsarte-Goethals codes have a structure of $\mathbb{Z}_4$-codes via the Gray map. This mapping provides a one-to-one correspondence between a $\mathbb{Z}_4$-code and a binary code. We will give the definition, applications and properties of this important mapping.

First of all we will introduce the following three maps α, β and γ from $\mathbb{Z}_4$ to $\mathbb{Z}_2$ by the following table:

c	$\alpha(c)$	$\beta(c)$	$\gamma(c)$
0	0	0	0
1	1	0	1
2	0	1	1
3	1	1	0

Note that α can be defined as the map

$$\alpha(x) = x \bmod 2. \tag{3.1}$$

Clearly, α is an additive group homomorphism from $\mathbb{Z}_4$ to $\mathbb{Z}_2$. For each element $x \in \mathbb{Z}_4$ we have

$$x = \alpha(x) + 2\beta(x), \text{ and}$$

$$\alpha(x) + \beta(x) + \gamma(x) = 0 \bmod 2, \text{ for all } x \in \mathbb{Z}_4.$$

Note that $\gamma(x)$ can be expressed as $\gamma(x) = \alpha(x) + \beta(x) \bmod 2$.

Now we define the Gray map in terms of β and γ as follows:

$$\varphi(x) = (\beta(x), \gamma(x)) \text{ for all } x \in \mathbb{Z}_4.$$

We obtain the following map:

$$\begin{array}{ccc} \mathbb{Z}_4 & \xrightarrow{\varphi} & \mathbb{Z}_2^2 \\ 0 & \longrightarrow & 00 \\ 1 & \longrightarrow & 01 \\ 2 & \longrightarrow & 11 \\ 3 & \longrightarrow & 10 \end{array} \tag{3.2}$$

We construct binary codes from quaternary codes using the extended Gray map $\phi : \mathbb{Z}_4^n \longrightarrow \mathbb{Z}_2^{2n}$ given by

$$\phi(c) = (\varphi(c_1), \ldots, \varphi(c_n)),$$

where $c = (c_1, \ldots, c_n)$.

In the literature, one can find, basically, two different extensions of the Gray map. The first one can be found in [BR99], [BPR03], [BPRZ03], etc, and it is given by

$$\phi(c) = (\beta(c_1), \gamma(c_1), \ldots, \beta(c_n), \gamma(c_n)), \tag{3.3}$$

and the second one (see, for example, [HKC$^+$94] and [Wan97]) is defined as

$$\phi(c) = (\beta(c_1), \ldots, \beta(c_n), \gamma(c_1), \ldots, \gamma(c_n)), \tag{3.4}$$

where $c = (c_1, \ldots, c_n)$.

In fact, if $c = (c_1, \ldots, c_n)$, any coordinate permutation of

$$(\beta(c_1), \gamma(c_1), \ldots, \beta(c_n), \gamma(c_n))$$

can be considered as an extension of the Gray map. That way, if ϕ_1 and ϕ_2 are two different extensions of the Gray map, then there exists a coordinate permutation $\pi \in \mathcal{S}_{2n}$ such that $\phi_1 = \pi \circ \phi_2$. In general, the properties concerning ϕ that will be given in this chapter are true for any extension of the Gray map. In that case, we will talk about a general Gray map or simply, the Gray map. Unless it is said otherwise ϕ will denote a general Gray map. Whenever a specific extension of the Gray map is needed we will refer to the exact arrangement of coordinates.

Let ϕ be an extended Gray map. If $\mathcal{C}$ is a quaternary code, then $C = \phi(\mathcal{C})$ is the binary image of $\mathcal{C}$ under ϕ. We say that a binary code C is $\mathbb{Z}_4$-linear if its coordinates can be arranged so that it is the image under the extended Gray map ϕ of a quaternary code. Notice that this definition is equivalent to say that there exist a different extended Gray map $\phi' = \pi \circ \phi$, $\pi \in \mathcal{S}_{2n}$, and a quaternary code $\mathcal{C}$, such that $C = \phi'(\mathcal{C})$.

The Gray map has the property that adjacent elements in $\mathbb{Z}_4$ differ by only one binary digit. It is an important fact useful in communications systems employing quadrature phase-shift keying (QPSK) (see Fig. 3.1). The advantage of using a general Gray map in QPSK is that, when a codeword over $\mathbb{Z}_4$ is transmitted across an additive white Gaussian noise channel, errors most likely to occur are those causing a single erroneously decoded information bit.

The most important property of the Gray map is that ϕ is a weight-preserving map from ($\mathbb{Z}_4^n$, wt_L), to ($\mathbb{Z}_2^{2n}$,wt); i.e.:

$$\mathrm{wt}_L(x) = \mathrm{wt}(\phi(x)),\ \forall x \in \mathbb{Z}_4^n,$$

and ϕ is also a distance-preserving map from ($\mathbb{Z}_4^n$, d_L), to ($\mathbb{Z}_2^{2n}$,d); i.e.:

$$d_L(x, y) = d(\phi(x), \phi(y)),\ \forall x, y \in \mathbb{Z}_4^n.$$

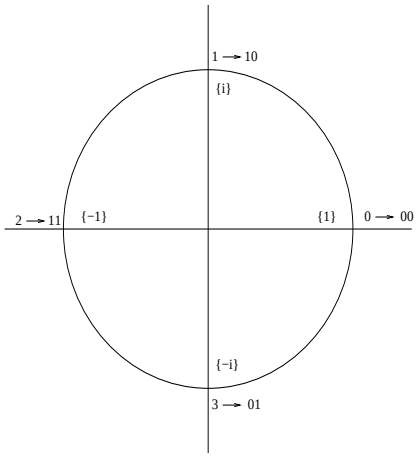

Figure 3.1: QPSK

The minimum Lee weight and distance of $\mathcal{C}$ are equal to the minimum Hamming weight and distance of $C = \phi(\mathcal{C})$, respectively.

The following examples provide $\mathbb{Z}_4$-linear codes with propelinear structure by means of the Gray map. They can be found in [BR99].

Example 3.2.1. *Let φ be the Gray map defined in (3.2). For all $\varphi(i) \in \mathbb{Z}_2^2$, where $i \in \mathbb{Z}_4$, we define the coordinate permutation $\sigma_i = (12)^i$. $(\varphi(\mathbb{Z}_4), \star)$ is a propelinear code, where*

$$\varphi(i) \star \varphi(j) = \varphi(i) + \sigma_i(\varphi(j)).$$

For example:

$$10 \star 01 = 10 + (12)^3(01) = 10 + 10 = 00 \in \varphi(\mathbb{Z}_4).$$

It is easy to verify that, for $i = 1, \cdots, 4$, $\varphi(i) = \varphi(1)^i = \varphi(1) \star \varphi(1) \star \cdots$ i times, and also

$$\varphi(i) \star \varphi(j) = \varphi(1)^i \star \varphi(1)^j = \varphi(1)^{i+j} = \varphi(i+j).$$

Hence, the operation $\star$ can also be defined as:

$$x \star y = \varphi(\varphi^{-1}(x) + \varphi^{-1}(y)),$$

where $x, y \in \varphi(\mathbb{Z}_4)$ and $+$ is the usual sum in $\mathbb{Z}_4$. With this definition,

$$10 \star 01 = \varphi(3+1) = \varphi(0) = 00.$$

Example 3.2.2. *Every $\mathbb{Z}_4$-code is a propelinear code: Let $C = \phi(\mathcal{C})$ be a $\mathbb{Z}_4$-code where $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$. From the last example, $(\varphi(\mathbb{Z}_4), \star)$ is a propelinear code and it is easy to check that $(\phi(\mathbb{Z}_4^n), \star)$ is also a propelinear code and, consequently, $(C, \star)$ is a propelinear code where*

$$x \star y = \phi(\phi^{-1}(x) + \phi^{-1}(y)) \tag{3.5}$$

is the operation defined in $\phi(\mathbb{Z}_4^n)$.

3.3 Binary images of a quaternary code

Let $\mathcal{C}$ be a quaternary code. Due to the linearity, $\mathcal{C}$ is distance invariant with respect to the Lee weight. Hence, the binary image of $\mathcal{C}$, $C = \phi(\mathcal{C})$ is distance invariant.

From a quaternary code $\mathcal{C}$, we can define its dual code $\mathcal{C}^\perp$. Since in general $C = \phi(\mathcal{C})$ is not linear, it need not have a dual. We define then the $\mathbb{Z}_4$-dual of $\phi(\mathcal{C})$ to be the code $C_\perp = \phi(\mathcal{C}^\perp)$. We have the following diagram

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\phi} & C = \phi(\mathcal{C}) \\ {\scriptstyle dual}\downarrow & & \\ \mathcal{C}^\perp & \xrightarrow{\phi} & C_\perp = \phi(\mathcal{C}^\perp) \end{array}$$

that is not a commuting diagram in general. We call the binary codes $C = \phi(\mathcal{C})$ and $C_\perp = \phi(\mathcal{C}^\perp)$ formally dual. If $\mathcal{C}$ is a self-dual code over $\mathbb{Z}_4$, then $\phi(\mathcal{C})$ is a formally self-dual code, that is, a binary code whose weight enumerator is invariant under the MacWilliams transform. We can give some information of $C_\perp$ in terms of C by the binary MacWilliams identity.

Theorem 3.2. *Let $\mathcal{C}$ and $\mathcal{C}^\perp$ be dual $\mathbb{Z}_4$-codes, and let $C = \phi(\mathcal{C})$ and $C_\perp = \phi(\mathcal{C}^\perp)$ be their binary images. Then, the weight enumerators $W_C(X,Y)$ and $W_{C_\perp}(X,Y)$ of C and $C_\perp$, respectively, are related by the binary MacWilliams identity*

$$W_{C_\perp}(X,Y) = \frac{1}{|C|} W_C(X+Y, X-Y).$$

Proof: See [HKC+94]. ∎

If $\{A_0, \ldots, A_{2n}\}$ is the weight distribution of C, then its MacWilliams transform is the weight distribution $\{A'_0, \ldots, A'_{2n}\}$ of $C_\perp$ and the MacWilliams transform of $\{A'_0, \ldots, A'_{2n}\}$ is exactly $\{A_0, \ldots, A_{2n}\}$.

Hence, if $\mathcal{C}$ is a $\mathbb{Z}_4$-code and $C = \phi(\mathcal{C})$, then C and $C_\perp$ are distance invariant and the weight distribution of C and $C_\perp$ are the MacWilliams transforms of each other.

3.4 Linearity conditions

Recall that a binary code C is called $\mathbb{Z}_4$-linear if, up to coordinate permutation, it is the binary image of a quaternary code. In this section, we will give necessary and sufficient conditions for a binary code to be $\mathbb{Z}_4$-linear and for a $\mathbb{Z}_4$-linear code to be a binary linear code.

Let $x \in \mathbb{Z}_4$, we defined $\varphi(x)$ as $(\beta(x), \gamma(x))$ (φ defined in (3.2)). Note that $\varphi(-x) = (\gamma(x), \beta(x))$. Let $\sigma' = (12) \in S_2$, then $\sigma'(\varphi(x)) = \varphi(-x)$. We define the swap map, σ, as the product of all transpositions permuting the two binary coordinates, corresponding to each $\mathbb{Z}_4$ coordinate. Notice that σ is related to the extension of the Gray map.

Example 3.4.1. *Let ϕ be the Gray map defined in (3.4). Therefore, σ is defined as*

$$\sigma : (u_1, \ldots, u_n, v_1, \ldots, v_n) \longrightarrow (v_1, \ldots, v_n, u_1, \ldots, u_n). \tag{3.6}$$

Note that if $c = (c_1, \ldots, c_n) \in \mathbb{Z}_4^n$, *then*

$$\sigma(\phi(c)) = \sigma((\beta(c_1), \ldots, \beta(c_n), \gamma(c_1), \ldots, \gamma(c_n))) = (\gamma(c_1), \ldots, \gamma(c_n), \beta(c_1), \ldots, \beta(c_n)) = \phi(-c).$$

It is easy to check that if ϕ is a general Gray map, then $\sigma(\phi(x)) = \phi(-x)$. As a consequence, σ is a fixed-point-free involution in the automorphism group of C.

First, we will give necessary and sufficient conditions for a binary code to be $\mathbb{Z}_4$-linear in the following theorem.

Theorem 3.3 ([HKC$^+$94]). *A binary, not necessarily linear, code* C *of even length is* $\mathbb{Z}_4$*-linear if and only if its coordinates can be arranged so that*

$$u, v \in C \Longrightarrow u + v + (u + \sigma(u)) \cdot (v + \sigma(v)) \in C,$$

where σ *is the swap map and* $\cdot$ *is defined by*

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n). \tag{3.7}$$

Hence, if C is a binary linear code of even length, then C is $\mathbb{Z}_4$-linear if and only if its coordinates can be arranged so that

$$u, v \in C \Longrightarrow (u + \sigma(u)) \cdot (v + \sigma(v)) \in C.$$

Let ϕ be an extended Gray map. Now we will give some linearity conditions related to ϕ. Let $\mathcal{C}$ be a quaternary code and $C = \phi(\mathcal{C})$. Let $x, y \in \mathcal{C}$. Consider the following property (see [BPRZ03]):

$$\phi(x) + \phi(y) = \phi(x + y + 2xy), \tag{3.8}$$

where $2xy$ is $2x \cdot y$.

Note that if $x, y \in \mathcal{C}$, then

$$\phi(2x + y) = \phi(2x) + \phi(y). \tag{3.9}$$

C is a linear code if and only if for all pair of codewords $x, y \in \mathcal{C}$, we obtain $\phi(x) + \phi(y) \in C$. By (3.9), if $x \in \mathcal{C}$ is an order 2 codewords; that is, all nonzero coordinate have value 2, then $\phi(x) + \phi(y) = \phi(x + y) \in C$. In general, if x and y are codewords in $\mathcal{C}$, then $\phi(x) + \phi(y) \in C$ if and only if $\phi(x + y + 2xy) \in C$ (by (3.8)) or, equivalently, $2xy \in \mathcal{C}$.

The following theorem shows when the binary image of a $\mathbb{Z}_4$-linear code is linear.

Theorem 3.4. *The binary image $C = \phi(\mathcal{C})$ of a $\mathbb{Z}_4$-linear code $\mathcal{C}$ is linear if and only if*

$$x, y \in \mathcal{C} \Longrightarrow 2xy \in \mathcal{C}.$$

This Theorem can be found in [HKC+94], where instead of use $2xy$, it is given the equivalent expression $2\alpha(x) \cdot \alpha(y)$.

3.5 Cyclic codes over $\mathbb{Z}_4$ and Galois Rings

A cyclic code of length n can be defined as an ideal in the ring of polynomials modulo $X^n - 1$. A cyclic code of length n over the field $\mathbb{F}_q = GF(q)$ consists then, of all multiplies of a certain generator polynomial $g(X)$ which is the monic polynomial of least degree in the code and it is divisor of $X^n - 1$. If n and q are relative prime, then zeros of $X^n - 1$ lie in the field $GF(q^m)$, where m is the least positive integer such that n divides $q^m - 1$. Then, to study cyclic codes over $\mathbb{F}_q$ we consider the Galois field $GF(q^m)$.

Similarly, to study cyclic codes over $\mathbb{Z}_4$ of length $n = 2^m - 1$ we construct the Galois ring $GR(4^m)$ that is an extension of degree m of $\mathbb{Z}_4$ containing an n^{th} root of unity. Constructions of $GR(4^m)$ and all the statements in this subsection are in [HKC+94] and [Wan97].

Note that $GR(4^m)$ is not a field, it contains zero divisors. We will construct $GR(4^m)$ in two different ways: as an extension $\mathbb{Z}_4[\xi]$ of $\mathbb{Z}_4$, where ξ is an n^{th} root of unity or as a residue classes of $\mathbb{Z}_4[X]$ modulo $X^n - 1$.

Let $h_2(X) \in \mathbb{Z}_2[X]$ be a primitive irreducible polynomial of degree m. There is a unique monic polynomial $h(X) \in \mathbb{Z}_4[X]$ of degree m such that $h(X) \equiv h_2(X) \bmod 2$ and $h(X)$ divides $X^n - 1 \bmod 4$ (see [CS95]). The polynomial $h(X)$ is a primitive basic irreducible polynomial. The way to find this polynomial by means of $h_2(X)$ is the following. We write $h_2(X)$ as $e(X) - d(X)$ where $e(X)$ contains even powers and $d(X)$ the odd ones. Now, we obtain $h(X)$ from $h(X^2) = \pm(e^2(X) - d^2(X))$. Finally, let ξ be a root of $h(X)$, so that $\xi^n = 1$. Then, $GR(4^m)$ is defined to be $\mathbb{Z}_4[\xi]$. Any element $c \in \mathbb{Z}_4[\xi]$ can be represented as $(c_0, \ldots, c_{n-1})$, where

$$c = \sum_{i=0}^{n-1} c_i \xi^i.$$

$h(X)$ is called the Hensel lift of $h_2(X)$. The presented method is the Graeffe's method that is used to find a polynomial whose roots are the squares of the roots of $h_2(X)$.

On the other hand, $\mathcal{R} = GR(4^m)$ can be considered as

$$\mathcal{R} = \frac{\mathbb{Z}_4[X]}{(X^n - 1)}.$$

Codewords $c = (c_0, \ldots, c_{n-1})$ in $\mathcal{C}$ can be represented as polynomials in $\mathcal{R}$ as

$$c(X) = \sum_{i=0}^{n-1} c_i X^i.$$

A cyclic code $\mathcal{C}$ is an ideal in the domain $\mathcal{R}$. In fact, $\mathcal{R}$ is a principal ideal domain [CS95], and therefore, $\mathcal{C} =< g(X) >$, where $g(X) \in \mathcal{R}$ is the generator polynomial of the code.

Example 3.5.1. *Let* $h_2(X) = X^6 + X^5 + X^4 + X + 1$. *Then,* $e(X) = (X^6 + X^4 + 1)$, $d(X) = (-X^5 - X)$ *and* $h(X^2) = e^2(X) - d^2(X) = X^{12} + X^{10} + X^8 + 2X^6 + 2X^4 - X^2 + 1$. *Hence, the Hensel lift of* $h_2(X)$ *is*

$$h(X) = X^6 + X^5 + X^4 + 2X^3 + 2X^2 - X + 1.$$

Note that $h(X) = h_2(X) \bmod 2$. $h(X)$ *generates a* $\mathbb{Z}_4$*-code of length* $n = 2^6 - 1 = 63$.

Let f be the Frobenius map from R to R the ring automorphism defined as

$$\begin{array}{ccc} R & \xrightarrow{f} & F \\ c = a + 2b & \longrightarrow & c^f = a^2 + 2b^2 \end{array}$$

The relative trace from R to $\mathbb{Z}_4$ is defined by

$$T(c) = c + c^f + c^{f^2} + \cdots + c^{f^{m-1}},\ c \in R. \tag{3.10}$$

3.6 Preparata-like and Kerdock-like codes

The Preparata codes were introduced by Preparata in 1968 (see [Pre68]). This family of nonlinear binary codes are 2-error correcting codes and generalize the Nordstrom-Robinson code. For $m \geq 4$, m even, the extended Preparata code of length 2^m denoted by P_m is a binary nonlinear code with parameters

$$(n, d, M) = (2^m, 6, 2^{2^m - 2m}),$$

which is a union of $2^{(m-1)(m-2)/2}$ cosets of $RM(m-3, m)$ in $RM(m-2, m)$, where $RM(r, m)$ is the r-th order Reed-Muller code studied deeply in Chapter 5. P_m has twice as many codewords as the 2-error correcting code BCH with the same length. Actually, P_m has the maximum possible number of codewords in a binary code of length 2^m and minimum distance 6. The weight distribution of the family of Preparata codes were given in 1969 in [SZZ71].

In 1972, another class of codes given by Kerdock generalized the Nordstrom-Robinson code [Ker72]. For $m \geq 4$, m even the extended Kerdock code of length 2^m, denoted by K_m is a nonlinear code with parameters

$$(n, d, M) = (2^m, 2^{m-1} - 2^{(m-2)/2}, 2^{2m}),$$

which is the union of 2^{m-1} cosets of $RM(1, m)$ in $RM(2, m)$.

From now on, both codes, extended Preparata and extended Kerdock will be called Preparata and Kerdock, respectively.

Two relevant facts strongly suggested that P_m and K_m were dual in some arithmetic sense. First, the fact that

$$RM(1,m) \subset K_m \subset RM(2,m),$$

$$RM^{\perp}(2,m) = RM(m-3,m) \subset P_m \subset RM(m-2,m) = RM^{\perp}(2,m).$$

The second fact, and the most important, is that in [Ker72] and [SZZ72] it was found that the weight enumerator of P_m is the MacWilliams transform of the weight enumerator of K_m (see [MS77]).

Let $x \to x^{\sigma}$ be an automorphism of $\mathbb{F}$, i.e., σ is a power of 2. We require that both $x \to x^{\sigma+1}$ and $x \to x^{\sigma-1}$ are one-to-one mappings, i.e., $(\sigma \pm 1, 2^m - 1) = 1$. (This is true, for example, for $\sigma = 2$).

For the admissible values of σ we shall define a code $P(\sigma)$ of length $2n+2 = 2^{m+1}$. The codewords will be described by pairs (X, Y) where $X \subset \mathbb{F}$, $Y \subset \mathbb{F}$. As usual we interpret the pair (X, Y) as the corresponding pair of characteristic functions, i.e., as a $(0,1)$-vector of length 2^{m+1}. We shall let the zero element of $\mathbb{F}$ correspond to the first position in the X-part.

Definition 3.6.1. *The Preparata code $\bar{P}(\sigma)$ of length 2^{m+1} consist of the codewords described by all pairs (X, Y) satisfying*

a) $|X|$ *is even,* $|Y|$ *is even,*

b) $\sum_{x \in X} x = \sum_{y \in Y} y$,

c) $\sum_{x \in X} x^{\sigma+1} + \left(\sum_{x \in X} x\right)^{\sigma+1} = \sum_{y \in Y} y^{\sigma+1}$.

The code $P(\sigma)$ is obtained by deleting the first coordinate.

Last definition is an alternative definition of Preparata code given in [BVLW83] that generalize these codes. Actually, the usual definition of the Preparata codes coincides with last definition for $\sigma = 2$:

$$P_m = P(2).$$

There are nonequivalents codes given in the last generalized definition ([Kan83]). All the codes $P(\sigma)$ have the same weight enumerator (Goethals) and they have the same parameters as the original Preparata code ([SZZ71]). They will be called Preparata-like codes. The Preparata-like code differs from the standard Preparata one in the fact that it is not a subcode of an extended Hamming code (for length $n \geq 32$) but of a nonlinear code with the same weight distribution as the extended Hamming code ([SZZ73]).

In [HKC$^+$94], it is shown that Kerdock codes are extended cyclic codes over $\mathbb{Z}_4$. These codes are linear codes over the integers modulo 4. The known fact that the weight distributions of the Kerdock and Preparata codes are the MacWilliams transform of each other would suggest that theses codes are duals in some more algebraic sense. In the same paper, it is proven that the $\mathbb{Z}_4$-dual code of a Kerdock code is not a Preparata code but a Preparata-like code.

Let $h(X) \in \mathbb{Z}_4[X]$ be a primitive basic polynomial of degree m and let $g(X)$ be the reciprocal polynomial to $(X^n - 1)/\big((X-1)h(x)\big)$, where $n = 2^m - 1$.

Theorem 3.5 ([HKC$^+$94]). *Let $\mathcal{K}^-$ be the cyclic code of length n over $\mathbb{Z}_4$ with generator polynomial $g(X)$, and let $\mathcal{K}$ be obtained from $\mathcal{K}^-$ by adjoining a zero-sum check symbol. Then for odd $m \geq 3$ the binary image $K_{m+1} = \phi(\mathcal{K})$ of $\mathcal{K}$ under the Gray map is a nonlinear code, of length 2^{m+1}, with 4^{m+1} words and minimal distance $2^m - 2^{(m-1)/2}$, that is equivalent to the Kerdock code. This code is distance invariant.*

Theorem 3.6 ([HKC$^+$94]). *Let $\mathcal{P}^-$ be the cyclic code of length $n = 2^m - 1$ with generator polynomial $h(X)$, and let $\mathcal{P}$ be obtained from $\mathcal{P}^-$ by adjoining a zero-sum check symbol, so that $\mathcal{P} = \mathcal{K}^\perp$. Then for odd $m \geq 3$ the binary image $P_{m+1} = \phi(\mathcal{P})$ of $\mathcal{P}$ under the Gray map is a nonlinear code of length $\ell = 2^{m+1}$, with $2^{\ell-2m-2}$ codewords and minimal distance 6. This code is distance invariant and its weight distribution is the MacWilliams transform of the weight distribution of the Kerdock code of the same length.*

For odd $m \geq 3$, $\mathcal{K}$ is called the quaternary Kerdock code, $\mathcal{P}$ is the quaternary

Preparata-like code and $P_{m+1} = \phi(\mathcal{P})$ is a Preparata-like code.

Example 3.6.1. *The polynomial* $h(X) = X^6 + X^5 + X^4 + 2X^3 + 2X^2 - X + 1$ *given in Example 3.5.1 is the generator polynomial of the code* $\mathcal{P}^-$ *where* $\mathcal{P}$ *is the Preparata-like code of length* 64.

Following theorems gives generator matrices of quaternary Kerdock and Preparata-like codes.

Theorem 3.7 ([HKC$^+$94]). *Let* $R = \mathbb{Z}_4[\xi]$ *be the Galois ring* $GR(4^m)$ *where* ξ *is a basic primitive root of unity, so that* $\xi^n = 1$, $n = 2^m - 1$. *The* $(m+1) \times 2^m$ *matrix*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \cdots & \xi^{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ b_{1\infty} & b_{11} & b_{12} & \cdots & b_{1n-1} \\ b_{2\infty} & b_{21} & b_{22} & \cdots & b_{2n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ b_{m\infty} & b_{m1} & b_{m2} & \cdots & b_{mn-1} \end{pmatrix} \tag{3.11}$$

is a generator matrix of $\mathcal{K}$, *where* ξ^j *is replaced in the second matrix by the m-tuple* $(b_{1j}, \ldots, b_{mj})$ *given by* $\xi^j = b_{1j} + b_{2j}\xi + \cdots + b_{mj}\xi^{m-1}$.

Corollary 3.8. *Matrix given in (3.11) is the parity check matrix of* $\mathcal{P}$.

The Kerdock and the Preparata-like codes of length 16, $m + 1 = 4$, coincide, giving the Nordstron-Robinson code. In this case, the code $\mathcal{K}$ is called the octacode. As the Kerdock and the Preparata-like codes are duals of each other, the octacode is a self-dual code; in fact, it is the unique self-dual quaternary code of length 16 and minimal Lee weight 6.

Theorem 3.9. *The Nordstrom-Robinson code is the binary image of the octacode under the Gray map.*

Lately, it was found in [BPRZ03] that any additive Preparata-like code is $\mathbb{Z}_4$-linear code. The $\mathbb{Z}_4$-dual codes of such codes are called Kerdock-like codes that are,

therefore, $\mathbb{Z}_4$-linear codes. The rank and the kernel of these codes are computed and the results are included in Sections 6.2.1 and 6.2.2.

Even though original Preparata codes are not $\mathbb{Z}_4$-linear codes, they have a group propelinear structure as it was given in [PR97b] using Definition 3.6.1. Moreover, both classes of codes, $\mathbb{Z}_4$-linear Preparata-like and $\mathbb{Z}_4$-linear Kerdock-like, have structure of propelinear codes.

Chapter 4

Additive codes

We will introduce additive codes by means of association schemes as it was introduced by Delsarte (see [DL98]). Some kind of additive codes as linear codes or $\mathbb{Z}_4$-codes were studied in previous chapters. In this chapter, we will deal with codes that can be considered, in some sense, as a generalization of linear and $\mathbb{Z}_4$-codes. First, we introduce $\mathbb{Z}_{2k}$-codes in Section 4.2. We generalize the Gray map φ, and define an operation $\cdot$, so that $(\varphi(\mathbb{Z}_{2k}), \cdot)$ is a Hamming-compatible code. Codes over $\mathbb{Z}_{2k}$ have structure as propelinear codes but, in general, these codes are not translation-invariant codes. Codes as subgroups of $\mathbb{Z}_{2i_1}^{k_1} \times \cdots \times \mathbb{Z}_{2i_r}^{k_r}$ are introduced in Section 4.3. Their algebraic structure and their binary image will be studied and it will be given for which cases such images are 1-perfect.

The different structure, the rank, and the dimension of the kernel of 1-perfect additive codes and extended 1-perfect additive codes are given in Section 4.4 and 4.5. If $\mathcal{C}$ is a 1-perfect additive code, then the extended code $\mathcal{C}^\star$ is an extended 1-perfect $\mathbb{Z}_4$-linear or additive non $\mathbb{Z}_4$-linear code. Finally, codes obtained by puncturing a binary coordinate of an extended 1-perfect additive codes are considered in Section 4.6.

4.1 Association schemes

Let X be a finite set of cardinality n and let $R = \{R_0, R_1, \cdots, R_d\}$ be a set of nonempty binary relations on X (i.e. $R_i \subseteq X^2$) forming a partition of the Cartesian square X^2 of X. We shall use N_i to denote the set $N_i = \{x \in X | (0, x) \in R_i\}$.

Definition 4.1.1. *The pair (X, R) is called an association scheme of class d on X if:*

(i) $R_0 = \{(x, x) | x \in X\}$,

(ii) $R_i^t = R_j$, *where* $R_i^t = \{(x, y) \in X^2 | (y, x) \in R_i\}$, *for* $i, j \in \{0, \cdots, d\}$,

(iii) for $i, j, k \in \{0, \cdots, d\}$, *the number of* $z \in X$ *such that* $(x, z) \in R_i$ *and* $(z, y) \in R_j$ *is a constant number whenever* $(x, y) \in R_k$ *and it is denoted* p_{ij}^k. *The numbers* p_{ij}^k *are called intersection numbers.*

There are more restrictions to an association scheme that are useful in coding-theory. If the condition (ii) is replaced by

(ii') $R_i^t = R_i$

then (X, R) is called a symmetric or Bose-Mesner association scheme. Moreover, when $p_{ij}^k = p_{ji}^k$ for all i, j, k, the association scheme is commutative.

From now on, an association scheme (X, R) is a symmetric commutative association scheme of class d on X. For more information about general association schemes see [DL98] and [BI84].

Example 4.1.1. *Let $X = \mathbb{F}_q^n$ be the n^{th} Cartesian power of the finite alphabet $\mathbb{F}_q$, with $|\mathbb{F}_q| = q \geq 2$. Let $x = (x_1, \cdots, x_n), y = (y_1, \cdots, y_n) \in X$. The Hamming distance between x, y is $d(x, y) = |\{j \in \{0, 1, \cdots, n\} \mid x_j \neq y_j\}|$. Hence, (X, R) with $d(x, y)$ is a symmetric class association scheme called the Hamming scheme and denoted by H_q^n.*

Let (X, R) be an association scheme where X has an Abelian group structure. (X, R) is a translation-invariant association scheme if for all $R_i \in R$

$$(x, y) \in R_i \Longrightarrow (x + z, y + z) \in R_i$$

for all $z \in X$.

Note that the Hamming scheme is a translation-invariant association scheme due to the fact that $d(x, y) = d(x + z, y + z)$.

Let Y be a nonempty subset of the point set X of a Hamming scheme $(X, R) = H_q^n$. Then, Y is a code. The inner distribution of Y in an n-class association scheme (X, R) is the rational $(n + 1)$-tuple $(a_0, \cdots, a_n)$ where $|Y|a_i$ counts the number of pairs of points in Y^2 (codewords) that belong to the relation R_i:

$$a_i = a_i(Y) = \frac{1}{|Y|}|Y^2 \cap R_i|, \quad \text{for } i \in \{0, \cdots, n\}.$$

If (X, R) is a Hamming scheme, H_q^n, then a code Y in (X, R) is a q-ary code of length n. The inner distribution of Y is its (Hamming) distance distribution. In this case, $|Y|a_i$ counts the pairs of codewords x, y with $d(x, y) = i$. If Y is a linear code in H_q^n, then the inner distribution of Y is none other than its weight distribution.

An additive code, Y, in a translation-invariant association scheme (X, R) is a subgroup of X. The weight of an element $x \in X$ is the number $\mathrm{wt}(x) = k$ such that $x \in N_k$. The weight distribution of the code $Y \subset X$ is the vector $(a_0, \cdots, a_n)$ defined by

$$a_i = |Y \cap N_i|$$

and coincides with the inner distribution. The numbers a_k such that $a_k \neq 0$ are called the weights of the code. The degree of an additive code is the number of its distinct nonzero weights.

4.2 $\mathbb{Z}_{2k}$-codes

The results in this section were presented in [BFR01].

Let $\mathcal{C}$ be a subgroup of $(\mathbb{Z}_{2k}^n, +)$ for some $k, n \geq 1$, where $+$ is the usual addition in $\mathbb{Z}_{2k}$ extended coordinatewise. We say that $\mathcal{C}$ is a $\mathbb{Z}_{2k}$-modulo code or, briefly, a $\mathbb{Z}_{2k}$-code. If $k = 1$, then $\mathcal{C}$ is a linear code and if $k = 2$, $\mathcal{C}$ is a $\mathbb{Z}_4$-code or a quaternary code.

We define the Lee weight and the Euclidean weight as a generalization of the definition given for $\mathbb{Z}_4$-codes. The Lee weight of an element $i \in \mathbb{Z}_{2k}$ is $min\{|i|, |2k - i|\}$ and the Lee weight $\mathrm{wt}_L(x)$ of $x \in \mathcal{C}$ is the rational sum of the Lee weights of its components. We define the Lee distance $d_L(x, y)$ of two vectors $x, y \in \mathcal{C}$ as $\mathrm{wt}_L(x - y)$. The Euclidean weight of an element $i \in \mathbb{Z}_{2k}$ is $min\{i^2, (2k - i)^2\}$ and the Euclidean weight of $x \in \mathcal{C}$, $\mathrm{wt}_E(x)$, is the rational sum of the Euclidean weights of its components. Hence, the Euclidean distance between two vectors $x, y \in \mathcal{C}$, $d_E(x, y)$, is $\mathrm{wt}_E(x - y)$. Note that for $k = 2$, these definitions corresponds with the ones given for $\mathbb{Z}_4$-codes.

For all $x, y \in \mathbb{Z}_{2k}^n$, $x = (x_1, \cdots, x_n)$, $y = (y_1, \cdots, y_n)$ we define the inner product of x and y by

$$x \cdot y = x_1 y_1 + \cdots + x_n y_n \mod 2k.$$

Definitions of minimum weight and distance, dual code, self-orthogonal code, and self-dual code are the ones given in Chapter 3.

Two $\mathbb{Z}_{2k}$-codes are equivalent if one can be obtained from the other by permuting coordinates and (if necessary) changing the signs of certain coordinates. Codes differing by only a permutation of coordinates are called permutation-equivalent.

Let $\mathcal{C}$ be a $\mathbb{Z}_{2k}$-code of length n. The complete weight enumerator (or c.w.e.) of $\mathcal{C}$ is

$$cwe_{\mathcal{C}}(X_0, X_1, \cdots, X_{2k-1}) = \sum_{c \in \mathcal{C}} X_0^{n_0(c)} X_1^{n_1(c)} \cdots X_{2k-1}^{n_{2k-1}(c)},$$

where $n_i(c)$ is the number of components of $c = (c_1, \cdots, c_n) \in \mathcal{C}$ that are congruent to i modulo $2k$. As in the case of $\mathbb{Z}_4$-codes, the appropriate weight enumerator for

an equivalence class of codes is the symmetrized weight enumerator:

$$swe_{\mathcal{C}}(X_0, X_1, \cdots, X_{2k-1}) = \sum_{c \in \mathcal{C}} X_0^{n'_0(c)} X_1^{n'_1(c)} \cdots X_k^{n'_k(c)},$$

where $n'_i(c)$ is the number of components of $c = (c_1, \cdots, c_n) \in \mathcal{C}$ that are congruent to $\pm i$ modulo $2k$.

4.2.1 Generalizations of the Gray map

There are different ways of giving a generalization of the standard Gray may. For instance, Carlet gives in [Car97] a generalization to $\mathbb{Z}_{2^k}$. We will give one preserving the basic property that the distance between the images of two consecutive elements is exactly one. In this section we will see that any $\mathbb{Z}_{2k}$-code accepts a representation as a propelinear code via this generalization of the Gray map.

Consider the modulo $\mathbb{Z}_k$ and let $c \in \mathbb{Z}_k$. c can be written as $c = \alpha(c) + 2r$, where $\alpha(c) = c \bmod 2$ and $r \in \mathbb{N}$. Define:

$$\beta_1(c) = \cdots = \beta_r(c) = 1$$

$$\beta_{r+1}(c) = \cdots = \beta_{t-1}(c) = 0,$$

where $t = \left\lfloor \frac{k}{2} \right\rfloor$. Let $\gamma(c)$ the parity check of the vector

$$(\alpha(c), \beta_1(c), \cdots, \beta_{t-1}(c))$$

For each element $c \in \mathbb{Z}_k$ we have

$$c = \alpha(c) + 2(\beta_1(c) + \cdots + \beta_{t-1}(c)), \text{ and}$$

$$\alpha(c) + \beta_1(c) + \cdots + \beta_{t-1}(c) + \gamma(c) = 0 \text{ modulo } 2.$$

Now we define the extended Gray map in terms of β_i and γ as follows:

$$\varphi(c) = (\beta_1(c), \cdots, \beta_{t-1}(c), \gamma(c)), \text{ for all } c \in \mathbb{Z}_k.$$

Example 4.2.1.

$$\begin{array}{ccc} \mathbb{Z}_8 & \xrightarrow{\varphi} & \mathbb{Z}_2^4 \\ 0 & \longrightarrow & 0000 \\ 1 & \longrightarrow & 0001 \\ 2 & \longrightarrow & 1001 \\ 3 & \longrightarrow & 1000 \\ 4 & \longrightarrow & 1100 \\ 5 & \longrightarrow & 1101 \\ 6 & \longrightarrow & 1111 \\ 7 & \longrightarrow & 1110 \end{array}$$

Note that $d(\varphi(0), \varphi(k-1)) \neq 1$, for $k > 2$. In fact,

$$d(\varphi(0), \varphi(k-1)) = \begin{cases} t, & \text{if } t \text{ odd or } k = 3, \\ t-1, & \text{otherwise.} \end{cases}$$

As in $\mathbb{Z}_4$-codes, this generalization is useful to work in communications systems employing quadrature phase-shift keying (QPSK). Distance between two consecutive elements is one but distance between the first and the last element is at least the maximum minus 1.

If we want a generalization preserving the property that the distance between images of two consecutives elements in $\mathbb{Z}_k$ is 1, then $d(\varphi(0), \varphi(k-1)) = 1$. In that case, k has to be even ([BFR01]), so we will write $\mathbb{Z}_{2k}$. We define the second generalization of the Gray map as $\varphi : \mathbb{Z}_{2k} \longrightarrow \mathbb{Z}_2^k$ such that:

$$\begin{array}{ll} (i) & \varphi(i) = (\mathbf{0}^{(k-i)} \mid \mathbf{1}^{(i)}) \quad \forall i = 0, \ldots, k-1, \textit{and} \\ (ii) & \varphi(i+k) = \varphi(i) + \mathbf{1}^{(k)} \quad \forall i = 0, \ldots, k-1. \end{array} \tag{4.1}$$

Example 4.2.2.

$$\begin{array}{ccc} \mathbb{Z}_8 & \xrightarrow{\varphi} & \mathbb{Z}_2^4 \\ 0 & \longrightarrow & 0000 \\ 1 & \longrightarrow & 0001 \\ 2 & \longrightarrow & 0011 \\ 3 & \longrightarrow & 0111 \\ 4 & \longrightarrow & 1111 \\ 5 & \longrightarrow & 1110 \\ 6 & \longrightarrow & 1100 \\ 7 & \longrightarrow & 1000 \end{array}$$

Note that this Gray map, φ, is distance-preserving and weight-preserving. In Section 4.2.2 we will see more properties of this mapping.

Finally, we will see a generalization that can be found in [KS02]. Let $c \in \mathbb{Z}_{2^k}$, and consider its 2-adic expansion

$$c = \sum_{i=0}^{k-1} a_i(c)2^i,$$

where $a_i(c)$ is the i^{th} bit of c represented as a k bit integer. We define

$$b_i(c) = \begin{cases} a_{i+1}(c) + a_i(c), & \text{if } i < k-1, \\ a_{k-1}(c), & \text{if } i = k-1. \end{cases}$$

Then we define the Gray map as follows:

$$\varphi(c) = (b_1(c), \cdots, b_{k-1}(c)), \text{ for all } c \in \mathbb{Z}_{2^k}.$$

Example 4.2.3.

$$\begin{array}{ccc} \mathbb{Z}_8 & \xrightarrow{\varphi} & \mathbb{Z}_2^3 \\ 0 & \longrightarrow & 000 \\ 1 & \longrightarrow & 100 \\ 2 & \longrightarrow & 110 \\ 3 & \longrightarrow & 010 \\ 4 & \longrightarrow & 011 \\ 5 & \longrightarrow & 111 \\ 6 & \longrightarrow & 101 \\ 7 & \longrightarrow & 001 \end{array}$$

This mapping has the property that the image of Z_{2^k} has the lowest length. Note that $d(2^k - 1, 0) = 1$, but, in general, φ is not a distance-preserving mapping as we can see in the above example:

$$3 = d_L(4, 7) \neq d(\varphi(4), \varphi(7)) = 2.$$

4.2.2 $\mathbb{Z}_{2k}$-codes as propelinear codes

We have seen that linear codes are propelinear codes. Also $\mathbb{Z}_4$-codes are propelinear codes (Example 3.2.2). Now we will use the generalization of the Gray map given in (4.1) to see that any $\mathbb{Z}_{2k}$-code is a propelinear code.

We denote by $|$ the concatenation, i.e. if $x = (x_1, \ldots, x_r)$ and $y = (y_1, \ldots, y_s)$, then $(x \mid y) = (x_1, \ldots, x_r, y_1, \ldots, y_s)$. If $\pi_x \in \mathcal{S}_r$ and $\pi_y \in \mathcal{S}_s$, then the permutation $\pi = (\pi_x|\pi_y) \in \mathcal{S}_{r+s}$ is defined as

$$\pi(x|y) = (\pi_x(x)|\pi_y(y)).$$

Definition 4.2.1. *Let φ be the Gray map defined in (4.1). For any two elements $\varphi(i), \varphi(j) \in \varphi(\mathbb{Z}_{2k})$, define the product*

$$\varphi(i) \cdot \varphi(j) = \varphi(i) + \sigma_i(\varphi(j)), \tag{4.2}$$

where

$$\sigma_i = (1, k, k-1, \ldots, 2)^i \tag{4.3}$$

(i.e. i left shifts), for all vector $\varphi(i)$, $i = 0, \ldots, 2k-1$.

Lemma 4.1. *Let φ be the Gray map defined in (4.1). Let $i \in \mathbb{Z}_{2k}$ and $\cdot$ the product defined in (4.2). Then,*

$$\varphi(i) = \varphi(1)^i.$$

Proof: It is easy to verify that $\varphi(i) = \varphi(i-1) \cdot \varphi(1) = \varphi(1) \cdot \varphi(i-1)$. Appliying this repeadly yields the result. ∎

Using this lemma is easy to check that the operation defined in 4.2 can be written as:

$$\varphi(i) \cdot \varphi(j) = \varphi(i+j)$$

Proposition 4.2. *$(\varphi(\mathbb{Z}_{2k}), \cdot)$ is a group, with φ and $\cdot$ defined in (4.1) and (4.2) respectively.*

Proof: We have that

$$(\varphi(i) \cdot \varphi(j)) \cdot \varphi(\ell) = (\varphi(1)^i \cdot \varphi(1)^j) \cdot \varphi(1)^\ell = \varphi(1)^{i+j+\ell} = \varphi(i) \cdot (\varphi(j) \cdot \varphi(\ell)),$$

for all $i, j, \ell \in \mathbb{Z}_{2k}$. Therefore, the operation is associative.

It is clear that $\mathbf{0}^{(k)} = \varphi(0)$ acts as the identity element. Moreover, given $\varphi(i) \in \varphi(\mathbb{Z}_2^k)$, we have that

$$\varphi(i) \cdot \varphi(k-i) = \varphi(1)^{i+k-i} = \varphi(1)^k = \varphi(k) = \varphi(0) = \mathbf{0}^{(k)}.$$

∎

Theorem 4.3. *Let $\varphi : \mathbb{Z}_{2k} \longrightarrow \mathbb{Z}_2^\ell$ be a Gray map. If $(\varphi(\mathbb{Z}_{2k}), \cdot)$ is a Hamming-compatible code where $\cdot$ is the operation defined in (4.2) then, φ is unique up to coordinate permutation.*

Proof: See [BFR01] ∎

From now on, we will consider the map defined in (4.1) as the (unique) generalization of the Gray map being Hamming-compatible (see 2.3).

Definition 4.2.2. *We define the extended map* $\phi : \mathbb{Z}_{2k}^n \longrightarrow \mathbb{Z}_2^{kn}$ *such that* $\phi(j_1, \ldots, j_n) = (\varphi(j_1), \ldots, \varphi(j_n))$*, where* φ *is defined in (4.1). Finally, we define the permutations* $\pi_x = (\sigma_{j_1} | \cdots | \sigma_{j_n})$*, for* $x = \phi(j_1, \ldots, j_n)$*, where* σ_i *is defined in (4.3).*

Note that if $k = 1$, then ϕ is the identity map and, if $k = 2$, then ϕ is as defined in (3.4).

Next theorem will prove that given a $\mathbb{Z}_{2k}$-code of length n, there exists a propelinear code of lenght kn such that both codes are isomorphic. The isomorphism between them extends the usual structure in $(\mathbb{Z}_{2k},+)$ to the propelinear structure in $(\mathbb{Z}_2^k,\cdot)$.

Theorem 4.4. *If* $\mathcal{C}$ *is a* $\mathbb{Z}_{2k}$*-code, then* $\phi(\mathcal{C})$ *is a propelinear code with associated permutation* π_x *for all codeword* $x \in \phi(\mathcal{C})$*.*

Proof: Let $x = \phi(j_1, \ldots, j_n) = (\varphi(j_1), \ldots, \varphi(j_n))$ and $y = \phi(i_1, \ldots, i_n) = (\varphi(i_1), \ldots, \varphi(i_n))$ be two codewords. Then,

$$x + \pi_x(y) = (\varphi(j_1) + \sigma_{j_1}(\varphi(i_1)), \ldots, \varphi(j_n) + \sigma_{j_n}(\varphi(i_n)).$$

For any coordinate, say r, we have that

$$\varphi(j_r) + \sigma_{j_r}(\varphi(i_r)) = \varphi(1)^{j_r}\varphi(1)^{i_r} = \varphi(1)^{j_r+i_r} = \varphi(j_r + i_r).$$

Thus,

$$x+\pi_x(y) = (\varphi(j_1+i_1), \ldots, \varphi(j_n+i_n)) = \phi((j_1, \ldots, j_n)+(i_1, \ldots, i_n)) = \phi(\phi^{-1}(x)+\phi^{-1}(y)).$$

Therefore, it is clear that $x + \pi_x(y) \in \phi(\mathcal{C})$.

On the other hand, the associated permutation of $\phi(j_r + i_r)$ is

$$\sigma_{j_r+i_r} = (1, k, k-1, \ldots, 2)^{j_r+i_r} = \sigma_{j_r} \circ \sigma_{i_r},$$

hence, if $z = x + \pi_x(y)$, then $\pi_z = \pi_x \circ \pi_y$. ∎

Corollary 4.5. *The map $\phi : (\mathcal{C}, +) \longrightarrow (\phi(\mathcal{C}), \star)$ is a group isomorphism, where $x \star y = x + \pi_x(y)$ for all $x, y \in \phi(\mathcal{C})$.*

Proof: As we have seen in the previous proof, $x \star y = \phi(\phi^{-1}(x) + \phi^{-1}(y))$ and, clearly, ϕ is bijective. ∎

In [PR97b] it is shown that linear and $\mathbb{Z}_4$-linear codes are translation-invariant. Now, we show that for $k > 2$ any $\mathbb{Z}_{2k}$-code, viewed as a binary propelinear code, is not translation-invariant according to the classification given in [PR97b].

Proposition 4.6. *If $k > 2$ and $\mathcal{C} \in \mathbb{Z}_{2k}^n$, then $\phi(\mathcal{C})$ is a propelinear but not translation-invariant code.*

Proof: Consider the vector $z = (1, 0, \ldots, 0, 1) \in \mathbb{F}^k$. Then, it is easy to check that $d(\mathbf{0}^{(k)} \star z, \varphi(1) \star z) = 3 \neq d(\mathbf{0}^{(k)}, \varphi(1)) = 1$. ∎

Now we will show that it is not possible to generalize the MacWilliams identity given in (3.2) to $\mathbb{Z}_{2k}$ if $k > 2$. This result is the conclusion of some discussion with Patrick Solé and Ling San. Firstly, we will see the existence of a self-dual code in $\mathbb{Z}_{2k}$ for every $k \geq 1$.

Proposition 4.7. *(cf. [BDHO99]) There exists a self-dual code C of length n over $\mathbb{Z}_{2k}$ if n is a multiple of eight.*

Proof: Consider the matrix

$$(\ I_4 \ , \ M_4 \ ),$$

where I_4 is the identity matrix of order 4 and

$$M_4 = \begin{pmatrix} a & b & c & d \\ b & -a & -d & c \\ c & d & -a & -b \\ d & -c & b & -a \end{pmatrix},$$

then $M_4 \cdot {M_4}^t = (a^2 + b^2 + c^2 + d^2) I_4$ over $\mathbb{Z}$. From Lagrange's theorem on sums of squares, there are elements a, b, c, d of $\mathbb{Z}$ such that $1 + a^2 + b^2 + c^2 + d^2 = 4k$ for any

k with $k > 0$. The integers a, b, c, d are necessarily less that or equal to $2k$ so there exist a, b, c, d of $\mathbb{Z}_{2k}$ such that $1 + a^2 + b^2 + c^2 + d^2 = 4k$ for $k > 0$. Therefore these elements a, b, c, d of $\mathbb{Z}_{2k}$ give that the matrix (I_4 , M_4) generates a self-dual code of length 8 over $\mathbb{Z}_{2k}$ for any positive k. ∎

Theorem 4.8. *Let $\mathcal{C}$ and $\mathcal{C}^\perp$ be dual $\mathbb{Z}_{2k}$-codes, and $C = \phi(\mathcal{C})$ and $C_\perp = \phi(\mathcal{C}^\perp)$ be their binary images. Then, the weight enumerators $W_C(X, Y)$ and $W_{C_\perp}(X, Y)$ of C and $C_\perp$ respectively, are related by the binary MacWilliams identity*

$$W_{C_\perp}(X, Y) = \frac{1}{|C|} W_C(X + Y, X - Y) \tag{4.4}$$

if and only if $k = 1, 2$; that is, C is linear or $\mathbb{Z}_4$-linear.

Proof: If $k = 1$ or 2 then, by Theorem 2.1 and Theorem 3.2 the MacWilliams identity holds. Let $\mathcal{C}$ be a self-dual code of length a multiple of eight in $\mathbb{Z}_{2k}$ (it exists by Proposition 4.7). Let $C = \phi(\mathcal{C})$ and $C_\perp = \phi(\mathcal{C}^\perp) = C$. When $X = Y = 1$, we obtain from (4.4) the following result

$$|C_\perp| = \frac{1}{|C|} 2^{kn}$$

and, hence, $|C| = \sqrt{2^{kn}}$. As $\mathcal{C}$ is a self-dual code, $|\mathcal{C}| = \sqrt{(2k)^n}$. Finally, $|\mathcal{C}| = |C|$ if and only if $2^k = 2k$ and it is true only for cases $k = 1$ and $k = 2$. ∎

4.3 Binary mixed group codes

Definition 4.3.1. *A general mixed group code C is an additive subgroup of $G_1 \times \cdots \times G_r$, where $G_1, \ldots, G_r$ are finite groups. We say that a binary code C of length n is a mixed group code of type $(\mathbb{Z}_{2i_1}^{k_1}, \ldots, \mathbb{Z}_{2i_r}^{k_r})$ and length n if $C = \phi(\mathcal{C})$, where $i_1, \cdots, i_r$ are the minimum values such that $\mathcal{C}$ is a subgroup of $\mathbb{Z}_{2i_1}^{k_1} \times \cdots \times \mathbb{Z}_{2i_r}^{k_r}$ and $\sum_{j=1}^{r} i_j k_j = n$. We denote $\mathcal{C} \leq \mathbb{Z}_{2i_1}^{k_1} \times \cdots \times \mathbb{Z}_{2i_r}^{k_r}$.*

Proposition 4.9. *Let C be a mixed group code of type $(\mathbb{Z}_{2i_1}^{k_1}, \ldots, \mathbb{Z}_{2i_r}^{k_r})$ and length n. Then, C is a propelinear code.*

Proof: $C = \phi(\mathcal{C})$ where $\mathcal{C} \leq \mathbb{Z}_{2i_1}^{k_1} \times \cdots \times \mathbb{Z}_{2i_r}^{k_r}$. Then $\mathcal{C} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_r$, with $\mathcal{C}_j \leq \mathbb{Z}_{2i_j}^{k_j}$. We can write $\phi(\mathcal{C})$ as $(\phi_1(\mathcal{C}_1), \cdots, \phi_r(\mathcal{C}_r))$ with $\phi_j : \mathbb{Z}_{2i_j}^{k_j} \longrightarrow \mathbb{Z}_2^{k_j i_j}$ as in definition 4.2.2. We will denote $x \in C$ as $(x_1|\cdots|x_r)$ where $x_j \in \phi_j(\mathcal{C}_j)$. By Theorem 4.4, $\phi_j(\mathcal{C}_j)$ is a propelinear code. Hence, we define the permutation π_x as $(\pi_{x_1}|\cdots|\pi_{x_r})$, where π_{x_j} is the permutation associated to x_j in $\phi_j(\mathcal{C}_j)$. Now it is easy to verify that C is a propelinear code with permutation associated π_x for all $x \in C$. ∎

Let $(C, \star)$ be a propelinear code where C is a mixed group code of type $(\mathbb{Z}_{2i_1}^{k_1}, \ldots, \mathbb{Z}_{2i_r}^{k_r})$. By Theorem 4.4 and Corollary 4.5, it is easy to check that the operation $\star$ is given by

$$x \star y = \phi\big(\phi_1^{-1}(x_1) + \phi_1^{-1}(y_1), \cdots, \phi_r^{-1}(x_r) + \phi_r^{-1}(y_r)\big), \tag{4.5}$$

where $x = (x_1, \cdots, x_r), y = (y_1, \cdots, y_r) \in C$.

Theorem 4.10. *Let C be a binary mixed group code of type $(\mathbb{Z}_{2i_1}^{k_1}, \ldots, \mathbb{Z}_{2i_r}^{k_r})$ and length n. If C is 1-perfect, then C is of type $(\mathbb{Z}_2^k, \mathbb{Z}_4^{(n-k)/2})$ for some $k \in \mathbb{N}$.*

Proof: Let C be a binary mixed group code of type $(\mathbb{Z}_{2i_1}^{k_1}, \ldots, \mathbb{Z}_{2i_r}^{k_r})$. Assume there exists $j \in \{1, \cdots, r\}$ such that $i_j > 2$. Without loss of generality we will assume $j = 1$ and $k_j = 1$.

Let $x = (10\cdots01|0\cdots0|\cdots|0\cdots0) \in \mathbb{F}^n$. If C is 1-perfect, then there exists $y \in \mathcal{C}$ such that $d(x, \phi(y)) \leq 1$. As the minimum weight in C is 3 and the distance of x must be at most 1, the only possibility is $i_1 = 3$ and $\phi(y) = (111|0\cdots0|\cdots|0\cdots0)$, therefore $\mathcal{C} = G_1 \times \cdots \times G_r$ where G_1 is a subgroup of $\mathbb{Z}_6$ and $3 \in G_1$. The only subgroups of $\mathbb{Z}_6$ that contain 3 are $\{0, 3\}$ and $\mathbb{Z}_6$. We assume $G_1 = \mathbb{Z}_6$; otherwise, $G_1 = \{0, 3\}$ would be isomorphic to $\mathbb{Z}_2$. Let $u = (101100\cdots0)$, $v = (101010\cdots0) \in \mathbb{F}^n$ (where customary commas have been deleted); $u, v \notin C$. The only codewords at distance 1 of u and v are, respectively, $(111100\cdots0)$ and $(111010\cdots0)$ but the distance beetwen them is 2 which is not possible if C is 1-perfect. ∎

The last theorem shows that the only 1-perfect binary mixed group codes of type $(\mathbb{Z}_{2i_1}^{k_1}, \ldots, \mathbb{Z}_{2i_r}^{k_r})$ are translation-invariant propelinear codes of type $(k, \dfrac{n-k}{2})$.

4.4 1-perfect additives codes

An additive code of length n is a subgroup of $(\mathbb{F}^n, \star)$, where $(\mathbb{F}^n, \star)$ is a translation-invariant Abelian group. Notice that this definition coincides with the one given in the last section using association schemes (see also [BCN89]).

Theorem 4.11. *Let $(\mathbb{F}^n, \star)$ a Hamming-compatible group (see 2.3). The following sentences are equivalents:*

(i) $(\mathbb{F}^n, \star)$ is an Abelian group.

(ii) $\star$ is a translation-invariant operation.

(iii) $\mathbb{F}^n$ is isomorphic to $\mathbb{Z}_2^k \times \mathbb{Z}_4^{\frac{n-k}{2}}$, for some k.

From last theorem, if $(\mathbb{F}^n, \star)$ is a Hamming-compatible Abelian group and C is a subgroup of $\mathbb{F}^n$; that is, an additive code then, C can be considered as a translation-invariant propelinear code of type $(k_1, k_2, 0)$. If $\mathbb{F}^n$ is isomorphic to $\mathbb{Z}_2^k \times \mathbb{Z}_4^{\frac{n-k}{2}}$ then, C is of type $(k, (n-k)/2, 0)$ or, simply, $(k, (n-k)/2)$.

Let $(C, \star)$ be an additive code of length n and type $(k, \frac{n-k}{2})$. We make a partition of the set of coordinates $\{1, \cdots, n\}$ in only two subsets, X, Y, where $|X| = k$ are the coordinates in $\mathbb{Z}_2$ and $|Y| = n - k$ are the binary coordinates of the $\mathbb{Z}_4$ part. We suppose $X = \{1, 2, \cdots, k\}$ without loss of generality.

Every vector $v \in \mathbb{F}^n$ can be written as $v = (v_X | v_Y)$, where $|$ denotes the concatenation of coordinates. If $v_Y = (v_Y^{(1)}, \cdots, v_Y^{(n-k)})$ we suppose that its coordinates are well ordered in $\mathbb{Z}_4^{\frac{n-k}{2}}$; that is

$$\phi^{-1}(v_Y) = (\varphi^{-1}(v_Y^{(1)}, v_Y^{(2)}), \cdots, \varphi^{-1}(v_Y^{(n-k-1)}, v_Y^{(n-k)})), \tag{4.6}$$

where φ is the Gray map (3.2) and ϕ is the extended Gray map defined in (3.3). In all this section, the extended Gray map used ϕ will be the one defined in(3.3).

The operation $\star$ defined in (2.5) is extended to $\mathbb{F}^n$, considering $\mathbb{F}^n$ as $\mathbb{Z}_2^k \times \mathbb{Z}_4^{\frac{n-k}{2}}$ in the following way: If $v = (v_1, \cdots, v_n), u = (u_1, \cdots, u_n) \in \mathbb{F}^n$, then

$$\begin{aligned} v \star u = \big(&v_1 + u_1, \cdots, v_k + u_k, \\ &\phi(\phi^{-1}(v_{k+1}, v_{k+2}) + \phi^{-1}(u_{k+1}, u_{k+2})), \cdots, \phi(\phi^{-1}(v_{n-1}, v_n) + \phi^{-1}(u_{n-1}, u_n))\big), \end{aligned} \tag{4.7}$$

where the sum is modulo 2 in the first k coordinates, modulo 4 in the last ones and ϕ is the extended Gray map.

Theorem 4.12. *Let C be a 1-perfect additive code of type $(k, \frac{n-k}{2})$, where $n = 2^t - 1$ and $t \geq 3$. Then, there exists a natural number r, such that $2 \leq r \leq t \leq 2r$ and*

(i) $k = 2^r - 1$; that is, C is of type $(2^r - 1, 2^{t-1} - 2^{r-1})$,

(ii) $\Omega \cong \mathbb{Z}_2^{2r-t} \times \mathbb{Z}_4^{t-r}$, where Ω is the quotient group $\mathbb{F}^n/C$.

In the group $\Omega = \mathbb{F}^n/C$ every element has order 2 or 4, and hence, it is clear that $\Omega \cong \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ for some natural numbers α, β. The proof of these theorems can be found in [BR99].

From Theorem 4.12 we obtain the following table where we find all the different parameters of n and k of 1-perfect additive codes :

t	$n = 2^t - 1$	r	$k = 2^r - 1$	types: $(k, \frac{n-k}{2})$
2	3	1, 2	1, 3	$(1,1), (3,0)$
3	7	2, 3	3, 7	$(3,2), (7,0)$
4	15	2, 3, 4	3, 7, 15	$(3,6), (7,4), (15,0)$
5	31	3, 4, 5	7, 15, 31	$(7,12), (15,8), (31,0)$
6	63	3, 4, 5, 6	7, 15, 31, 63	$(7,28), (15,24), (31,16), (63,0)$
...	...	...	...	...

Table 4.1: Type of 1-perfect additive codes

Note that for $n = 3$ we obtain two different types $(1,1)$ and $(3,0)$ refering to the same code: the trivial code of length 3, $\{(000), (111)\}$. At the end of Section 2.4.2, we saw that the Hamming code of length 7 has different algebraic structures as an

additive code: $(3,2)$ and $(7,0)$. Only in the cases $n=3$ and $n=7$ there are two codes having the same set of codewords, up to coordinate permutation, but having different algebraic structure. We will see that there are no more cases.

Let us show that two additives codes of the same length n but with different algebraic structures are non isomorphic for $n>7$.
Assume C_1 and C_2 are 1-perfect additive codes of length $n>7$ and of type $(k,\frac{n-k}{2})$ and $(l,\frac{n-l}{2})$, respectively. Assume that there is a coordinate permutation $\sigma\in\mathcal{S}_n$, such that $C_1=\sigma(C_2)=C$. Let $\star$ be the operation such that $(C,\star)$ is isomorphic to a subgroup of $\mathbb{Z}_2^k\times\mathbb{Z}_4^{\frac{n-k}{2}}$ and let $\perp$ be the operation such that $(C,\perp)$ is isomorphic to a subgroup of $\mathbb{Z}_2^l\times\mathbb{Z}_4^{\frac{n-l}{2}}$.

Theorem 4.13. *Let $(C,\star)$ be a 1-perfect additive code of type $(k,\frac{n-k}{2})$ and $(C,\perp)$ be a 1-perfect additive code of type $(l,\frac{n-l}{2})$. Then it is not possible that $l<k$ and $n>7$.*

Proof: (see [BR99]). ∎

We have seen the parameters n,k allowed in order for a code to be a 1-perfect additive code of type $(k,\frac{n-k}{2})$ and, for a fixed length n, we know in which cases these codes are non isomorphic. Now we will see some results about the existence of these codes.

Let r and t be natural numbers such that $2\leq r\leq t\leq 2r$. Consider $\mathbb{F}^n$ with the additive propelinear structure such that it is isomorphic to the group $\mathbb{Z}_2^{2^r-1}\times\mathbb{Z}_4^{2^{t-1}-2^{r-1}}$ and has the coordinates as in (4.6). Let G be the group $\mathbb{Z}_2^{2r-t}\times\mathbb{Z}_4^{t-r}$. There exists an application

$$\vartheta:\mathbb{F}^n\longrightarrow G \tag{4.8}$$

such that:

(i) $\vartheta(e_i)\neq\vartheta(e_j)$, $\forall i,j=1\cdots,n$ such that $i\neq j$, and $\vartheta(\mathbf{0})=0$.

(ii) $\vartheta(e_i)=-\vartheta(e_j)\iff e_i\star e_j=0$.

(iii) For all vector $x = e_{i_1} \star \cdots \star e_{i_t} \in \mathbb{F}^n$,

$$\vartheta(x) = \sum_{j=1}^{t} \vartheta(e_{i_j}).$$

Moreover, the map $\vartheta : \mathbb{F}^n \longrightarrow G$ is well-defined and it is an homomorphism onto.

The following theorem gives a method to find any 1-perfect additive code with admissible parametres. The proof can be found in [BR99] and, previously, in [Rif99] with a slightly different notation.

Theorem 4.14. *With the previous definition of G and $\vartheta : \mathbb{F}^n \longrightarrow G$, $C = Ker(\vartheta)$ is a 1-perfect additive code of type $(2^r - 1, 2^{t-1} - 2^{r-1})$.*

Now we will see that the 1-perfect additive code constructed in this way is unique, up to isomorphism, with the given parametres.

Proposition 4.15. *For all r and t, such that $2 \leq r \leq t \leq 2r$, there is exactly one 1-perfect additive code of type $(2^r - 1, 2^{t-1} - 2^{r-1})$, up to isomorphism.*

Proof: See [BR99]. ∎

With Theorem 4.14 and Proposition 4.15 we have seen the existence and the uniqueness of 1-perfect additive codes. As a conclusion, we give the exact number of 1-perfect additive codes of length $n = 2^t - 1$. If $n = 3, 7$; that is, $t = 2, 3$, there is a unique 1-perfect additive code, up to isomorphism. If $n \geq 15$ $(t > 3)$, the number of such codes is exactly $\left\lfloor \frac{t+2}{2} \right\rfloor$.

The unicity means that if ϑ' is another homomorphism of $\mathbb{F}^n$ onto G such that $C' = ker(\vartheta')$ then there exists a permutation $\tau \in \mathcal{S}_n$ such that $\tau(C) = C'$ and $\vartheta' = \vartheta\tau$.

4.4.1 Rank and kernel

In Section 2.3.3 we have seen some bounds of the rank and the dimension of the kernel of 1-perfect codes in general. In this section, we will see the values that arise these

invariants in the case of 1-perfect additive codes. All theorems and propositions given in this section can be found in [PR02].

Let C be a propelinear code. Let C_π be the set

$$C_\pi = \{a \in C | \pi_a = \pi\}$$

Lemma 4.16. *Let C be an additive code. Let $\sigma \in \mathcal{S}_n$ be the swap map (see Section 3.4). Then $\sigma \in Aut(C)$. Moreover, if C is 1-perfect then, $C_\sigma \subset ker(C)$.*

Proposition 4.17. *If C is a non-linear 1-perfect additive code then the dimension of C_{Id} is $2^{t-1} + 2^{r-1} - r - 1$.*

Proposition 4.18. *If C is a 1-perfect binary additive code then, either $ker(C) = C_{Id} = C$ when C is linear or $ker(C) = C_{Id} \cup C_\sigma$ when C is not linear. In the first case, $dim(ker(C)) = dim(C_{Id})$ and in the second case $dim(ker(C)) = dim(C_{Id}) + 1$.*

As a corollary of these two propositions, we obtain the following theorem.

Theorem 4.19. *Let C be a binary 1-perfect additive code of type $(2^r - 1, 2^{t-1} - 2^{r-1})$, the kernel $ker(C)$ of C has dimension:*

$$dim(ker(C)) = \begin{cases} 2^r - r - 1, & \text{if } t = r, \\ 2^{r-1} + 2^{t-1} - r, & \text{if } t \neq r. \end{cases}$$

Theorem 4.20. *Let C be a binary 1-perfect additive code of type $(2^r - 1, 2^{t-1} - 2^{r-1})$, of length $n = 2^t - 1$, where $t \geq 4$, then the rank of C is:*

$$rank(C) = n - r = 2^t - r - 1.$$

In the following table, we can see the parameters of the rank and the kernel of 1-perfect additive codes:

t	r	type: $(k, \frac{n-k}{2})$	$dim(ker(C))$	$rank(C)$
2	$1, 2$	$(1, 1), (3, 0)$	$3, 3$	$3, 3$
3	$2, 3$	$(3, 2), (7, 0)$	$4, 4$	$4, 4$
4	$2, 3, 4$	$(3, 6), (7, 4), (15, 0)$	$8, 9, 11$	$13, 12, 11$
5	$3, 4, 5$	$(7, 12), (15, 8), (31, 0)$	$17, 20, 26$	$28, 27, 26$
6	$3, 4, 5, 6$	$(7, 28), (15, 24), (31, 16), (63, 0)$	$33, 36, 43, 57$	$60, 59, 58, 57$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

Table 4.2: Rank and dimension of the kernel of 1-perfect additive codes

4.5 Extended 1-perfect additive codes

Let C be a code of length n. The extended code $C^\star$ of C is a code of length $n+1$ obtained from C by adding the parity check coordinate.

For all this section, let C be a binary additive code of length n of type (α, β).

Theorem 4.21. *If $C^\star$ is an extended 1-perfect additive code of length $n+1 = 2^t$, then it is of type $(\alpha+1, \beta)$, where either $\alpha+1 = 0$ and it is a Z_4-linear code or $\alpha = 2^r - 1$, $2 \leq r \leq t \leq 2r$.*

In the next two subsections we give a characterization of extended 1-perfect additive codes and we give the rank and the kernel of such codes. The first subsection is about codes of type (α, β) with $\alpha > 0$ and the second one is when $\alpha = 0$ and the code is $\mathbb{Z}_4$-linear. Theorems in these two sections can be found in [BPR03] unless it is said otherwise.

4.5.1 Extended 1-perfect additive non $\mathbb{Z}_4$-linear codes

Theorem 4.22. *For any r and $t \geq 4$ such that $2 \leq r \leq t \leq 2r$ there is exactly one extended 1-perfect additive code C^* of type $(2^r, 2^{t-1} - 2^{r-1})$, up to coordinate permutation.*

Proof: The statement follows directly from Proposition 4.15 and Theorem 4.21. ∎

The following theorem gives the rank and the dimension of the kernel of such a 1-perfect additive code.

Theorem 4.23. *Let $C^\star$ be an extended 1-perfect additive code of type $(2^r, 2^{t-1}-2^{r-1})$ where $t > 3$, then*

(i) $dim(ker(C^\star)) = 2^{r-1} + 2^{t-1} - r$ if $t \neq r$ and $dim(ker(C^\star)) = 2^r - r - 1$ if $t = r$.

(ii) $rank(C^*) = 2^t - r - 1$.

In Theorem 4.14 it is shown that an additive code can be constructed as the kernel of a map $\vartheta : \mathbb{F}^n \longrightarrow \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. For any allowable parameter r and t, code $C^\star$ could be seen as the kernel of a group homomorphism:

$$\mathbb{F}^{n+1} = \mathbb{Z}_2^{\alpha+1} \times \mathbb{Z}_4^\beta \xrightarrow{\theta} \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$$

where $\alpha + 1 = 2^r$, $\beta = 2^{t-1} - 2^{r-1}$, $\gamma = 2r - t + 1$ and $\delta = t - r$. This homomorphism could be represented by a matrix like

$$H = \left(\begin{array}{c|c} (B_1)_{\gamma\times\alpha+1} & (B_2)_{\gamma\times\beta} \\ \hline (Q_1)_{\delta\times\alpha+1} & (Q_2)_{\delta\times\beta} \end{array}\right)$$

The columns of this matrix are all the possible independent vectors in $\{1 \in \mathbb{Z}_2\} \times \mathbb{Z}_2^{\gamma-1} \times \mathbb{Z}_4^\delta$. B_i are binary matrices, Q_1 is a quaternary matrix with elements of order 2 and Q_2 is a quaternary matrix with elements of order 4. H can be considered as a parity check matrix of the code $C^\star$.

Example 4.5.1. *Let C be a 1-perfect extended code of an additive code of length 31. From Theorem 4.22 there are three different pairs of allowable parametres of such a code: $(3,5)$, $(4,5)$ and $(5,5)$. Let C be of type $(3,5)$, then, C is the kernel of the homomorphism $\mathbb{F}^{32} = \mathbb{Z}_2^8 \times \mathbb{Z}_4^{12} \longrightarrow \mathbb{Z}_2^2 \times \mathbb{Z}_4^2$. A parity check matrix of the code given by the homomorphism is*

$$H = \left(\begin{array}{cccccccc|cccccccccc} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&0&0&1&1&1&1&1&1 \\ \hline 0&0&2&2&0&0&2&2&1&1&1&1&0&2&1&1&1&1&0&2 \\ 0&2&0&2&0&2&0&2&0&1&2&3&1&1&0&1&2&3&1&1 \end{array}\right)$$

The rank of C *is* $2^t-r-1=28$ *and the dimension of the kernel is* $2^{r-1}+2^{t-1}-r=17$.

In [BPR03] it is also constructed the parity check matrix when the code is of type $(4,5)$ *and* $(5,5)$.

The following tables show the different values of γ and δ and the values of $R = rank(C^\star)$ and $K = dim(ker(C^\star))$ in each case for t equal to 4, 5 and the general case.

$t=4$	R	K	R	K	R	K
	11	11	12	9	13	8
γ	4		3		1	
δ	0		1		2	

$t=5$	R	K	R	K	R	K	R	K
	26	26	27	20	28	17	$*$	$*$
γ	6		4		2		0	
δ	0		1		2		3	

t	R	K	R	K
	$2^t-t-1+\delta$	2^t-t-1	$2^t-t-1+\delta$	$2^{t-\delta-1}+2^{t-1}-t+\delta$
δ	0		≥ 3	

4.5.2 Extended 1-perfect additive $\mathbb{Z}_4$-linear codes

Let $C^\star$ be an extended 1-perfect additive code of length $n+1=2^t\geq 16$ of type $(0,\beta)$, where $2\beta=n+1$; that is, $C^\star$ is a $\mathbb{Z}_4$-linear code of length $n+1$.

Theorem 4.24. *Let* $C^\star$ *be an extended* 1*-perfect* $\mathbb{Z}_4$*-linear code of length* $n+1=2^t\geq 16$*, such that* $\mathbb{F}^{n+1}/C^\star$ *is isomorphic to* $\mathbb{Z}_2^\gamma\times\mathbb{Z}_4^\delta$ *for a fixed* $\delta\in\{1,\cdots,\lfloor(t+1)/2\rfloor\}$ *and* $\gamma=t+1-2\delta$*. Then,* $C^\star$ *is unique, up to coordinate permutation.*

Theorem 4.25. *For every* $t\geq 4$*, there are exactly* $\lfloor(t+1)/2\rfloor$ *extended* 1*-perfect* $\mathbb{Z}_4$*-linear codes of length* $n+1=2^t$.

This theorem, that is a corollary of Theorem 4.24, was previously proved by Krotov in [Kro01] using Hadamard codes. Each one of the nonequivalent codes of length $n+1=2^t$ correspond to the $\lfloor (t+1)/2 \rfloor$ different quotient groups $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ such that $\gamma + 2\delta = t+1$.

As in Section 4.5.1, for any allowable parameters r, t we can construct an extended 1-perfect additive $\mathbb{Z}_4$-linear code $C^\star$ as the kernel of the group homomorphism:

$$\mathbb{F}^{n+1} = \mathbb{Z}_4^\beta \xrightarrow{\theta} \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$$

where $\beta = 2^{t-1}$ and $t+1 = \gamma + 2\delta$. This homomorphism could be represented by a matrix like

$$H = \left(\frac{(B)_{\gamma \times \beta}}{(Q)_{\delta \times \beta}} \right)$$

The columns of this matrix are all the possible independent vectors in $\mathbb{Z}_2^\gamma \times \{1 \in \mathbb{Z}_4\} \times \mathbb{Z}_4^{\delta-1}$. B is a binary matrix and Q is a quaternary matrix. H can be considered as a parity check matrix of the code $C^\star$.

Now we will see some theorems about the rank and the kernel of extended 1-perfect additive $\mathbb{Z}_4$-linear codes.

Theorem 4.26. *Let $C^\star$ be an extended 1-perfect $\mathbb{Z}_4$-linear code of length $n+1=2^t > 16$ and assume the quotient set is isomorphic to $G = \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Then, $rank(C^\star) = 2^t - t - 1 + \delta$. For the case $t=4$, either $G = \mathbb{Z}_2^{t-1} \times \mathbb{Z}_4$ and $rank(C^\star) = 2^t - t - 1$; i.e. $C^\star$ is linear, or $G = \mathbb{Z}_2 \times \mathbb{Z}_4^2$ and $rank(C^\star) = 2^t - t - 1 + 2$.*

Theorem 4.27. *Let $C^\star$ be an extended 1-perfect $\mathbb{Z}_4$-linear code of binary length $n+1=2^t$.*

For $\delta = 1$ the dimension of the kernel is $dim(ker(C^\star)) = 2^{t-1} + t - 1$.

For $\delta = 2$ the dimension of the kernel is $dim(ker(C^\star)) = 2^{t-1} - \delta + 2 = 2^{t-1}$.

For $\delta \geq 3$ the dimension of the kernel is $dim(ker(C^\star)) = 2^{t-1} - \delta + 1$.

Example 4.5.2. *Let $C^\star$ be an extended 1-perfect additive $\mathbb{Z}_4$-linear code of length 32. $C^\star$ is of type $(0, 16)$. There are three possible pairs of values to the parameters*

(δ,γ): $(0,3)$, $(2,2)$ and $(4,1)$. Assume the case $\delta = \gamma = 2$. $C^\star$ is the kernel of the homomorphism $\mathbb{F}^{32} = \mathbb{Z}_4^{16} \longrightarrow \mathbb{Z}_2^2 \times \mathbb{Z}_4^2$. Then, a parity check matrix of the code given by the homomorphism is

$$H = \left(\begin{array}{cccccccccccccccc} 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ \hline 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1&2&2&2&2&3&3&3&3 \end{array}\right)$$

The rank of C is $2^t - t - 1 + \gamma = 26$ and the dimension of the kernel is $2^{t-1} = 16$.

Parity check matrices of codes with the other parameters are constructed in [BPR03].

The following tables show the different values of γ and δ and the values of $R = rank(C^\star)$ and $K = dim(ker(C^\star))$ in each case, for t equals to 4, 5 and the general case.

$t=4$	R	K	R	K	R	K
	$*$	$*$	11	11	13	8
γ	4		3		1	
δ	0		1		2	

$t=5$	R	K	R	K	R	K	R	K
	$*$	$*$	27	20	28	16	29	14
γ	6		4		2		0	
δ	0		1		2		3	

t	R	K	R	K	R	K	R	K
	$*$	$*$	$2^t - t +$ $\delta - 1$	$2^{t-1} +$ $t - 1$	$2^t - t$ $\delta - 1$	2^{t-1}	$2^t - t + \delta - 1$ $((t,\delta) \neq (4,1))$	$2^{t-1} - \delta + 1$
δ	0		1		2		≥ 3	

4.6 Punctured extended 1-perfect $\mathbb{Z}_4$-linear codes

Let C be a 1-perfect additive code. By Theorem 4.24 the extended code $C^\star$ is an extended 1-perfect $\mathbb{Z}_4$-linear or additive non $\mathbb{Z}_4$-linear code. If $C^\star$ is the extended 1-perfect additive non $\mathbb{Z}_4$-linear code of C and we puncture a binary coordinate, then $(C^\star)'$ is isomorphic to C. It is not true if we puncture a quaternary coordinate.

The aim of this section is to prove that a punctured extended $\mathbb{Z}_4$-linear code is not a 1-perfect additive code up to the extended Hamming code of length 16. All the results in this section can be found in [BF02] that contains the source code of the implementations used in the proof of the results.

Lemma 4.28. *Let C be a 1-perfect code and $C^\star$ the extended code. Then, the rank and the dimension of the kernel of C and $C^\star$ coincide.*

Lemma 4.29. *Let $C^\star$ be an extended 1-perfect $\mathbb{Z}_4$-linear code of length $n+1 = 2^t \geq 16$ such that $\mathbb{F}^{n+1}/C^\star \cong \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$, $\gamma + 2\delta = t + 1$, and assume $C = (C^\star)'$ is a 1-perfect additive code. Then, the allowable parameters of t and δ are:*

(i) $t = 4,\ \delta = 1,$

(ii) $t = 4,\ \delta = 2,$

(iii) $t = 5,\ \delta = 1.$

Proof: From Theorems 4.20 and 4.26 we obtain:

$$rank(C) = n - r = 2^t - r - 1$$

$$rank(C^\star) = \begin{cases} 2^t - t - 1 \text{ or } 2^t - t + 1 & \text{if } t = 4, \\ 2^t - t - 1 + \delta & \text{if } t > 4. \end{cases}$$

By Lemma 4.28 $rank(C^\star) = rank(C)$ then,

- if $t = 4$, either $r = t$ or $r = t - 2$,
- if $t > 4$, $\delta = t - r$.

Now, from Theorems 4.19 and 4.27 we obtain:

$$dim(ker(C)) = \begin{cases} 2^r - r - 1, & \text{if } t = r, \\ 2^{r-1} + 2^{t-1} - r, & \text{if } t \neq r. \end{cases}$$

$$dim(ker(C^\star)) = \begin{cases} 2^{t-1} + t - 1 & \text{if } \delta = 1, \\ 2^{t-1} & \text{if } \delta = 2, \\ 2^{t-1} - \delta + 1 & \text{if } \delta \geq 3. \end{cases}$$

By Lemma 4.28 $dim(ker(C)) = dim(ker(C^\star))$, and hence,

- if $t = 4$ and $r = t = 4$, then $2^r - r - 1 = 2^{t-1} + t - 1$ and $\delta = 1$, that corresponds to the case (i),
- if $t = 4$ and $r \neq t$, then $r = t - 2 = 2$, $2^{r-1} + 2^{t-1} - r = 2^{t-1}$ and $\delta = 2$, that corresponds to the case (ii),
- if $t > 4$, then $\delta = t - r$ and there are three cases:

  (1) $2^{r-1} + 2^{t-1} - r = 2^{t-1} + t - 1$ and $\delta = 1$.
  We obtain the equations $2^{r-1} - r = t - 1$ and $1 = t - r$, and hence, $2^{t-2} = 2t - 2$ that has solution if and only if $t = 5$, that corresponds to the case (iii).

  (2) $2^{r-1} + 2^{t-1} - r = 2^{t-1}$ and $\delta = 2$.
  $2^{r-1} = r$ if and only if $r = 1, 2$, but for these values of r it is not possible $\delta = t - r$, $t > 4$ and $\delta = 2$.

  (3) $2^{r-1} + 2^{t-1} - r = 2^{t-1} - \delta + 1$ and $\delta \geq 3$.
  $2^{r-1} - r = -\delta + 1 \leq -2$. But $2^{r-1} \leq r - 2$ has no solution.

∎

Proposition 4.30. *If $C^\star$ is an extended 1-perfect $\mathbb{Z}_4$-linear code with parameters $t = 4$ and $\delta = 2$, then the punctured code $(C^\star)'$ is not a 1-perfect additive code.*

Proof: Assume $C^\star$ is an extended 1-perfect $\mathbb{Z}_4$-linear code with parameters $t = 4$ and $\delta = 2$. The rank of $C^\star$ is 13 and the dimension of the kernel is 8. If $C = (C^\star)'$ is a 1-perfect additive code then, its rank and dimension of the kernel have the same values than $C^\star$, and hence, C is necessarily of type $(3, 6)$ (see Table (4.2)).

Constructing the $STS(15)$ associated to $(C^\star)'$ and computing the pattern array of fragments (see [LeV95]) we obtain that the pattern array of fragments from $(C^\star)'$ corresponds to the $STS(15)$ number 3 whereas the pattern array of fragments from the 1-perfect additive code of type $(3, 6)$ corresponds to the $STS(15)$ number 7. As the $STS(15)'s$ obtained from these two codes are not isomorphic, the codes are not isomorphic, and hence, $(C^\star)'$ is not a 1-perfect additive code. ∎

Proposition 4.31. *If $C^\star$ is an extended 1-perfect $\mathbb{Z}_4$-linear code with parameters $t = 5$ and $\delta = 1$, then the punctured code $(C^\star)'$ is not a 1-perfect additive code.*

Proof: Assume $C^\star$ is an extended 1-perfect $\mathbb{Z}_4$-linear code with parameters $t = 5$ and $\delta = 1$. The rank of $C^\star$ is 27 and the dimension of the kernel 20. If $C = (C^\star)'$ is a 1-perfect additive code then, its rank and dimension of the kernel have the same values than $C^\star$ and C is necessarily of type $(15, 8)$ (see Table (4.2)).

Let S_1 be the set of weight 3 codewords of the punctured extended 1-perfect $\mathbb{Z}_4$-linear code, $(C^\star)'$ and S_2 the set of weight 3 codewords of the extended 1-perfect non $\mathbb{Z}_4$-linear code with parameters $t = 5$ and $\delta = 1$ puncturing a binary coordinate. Note that, as it is punctured a binary coordinate, this code coincides to the 1-perfect additive code of type $(15, 8)$.

Both, S_1 and S_2, contain 155 codewords of length 31 and weight 3 (results obtained by computer test). Using GAP we compute the dimensions of these sets and we obtain $dim(S_1) = 26$ and $dim(S_2) = 27$. As their dimensions are different, S_1 and S_2 are not isomorphic, and hence, the punctured code $(C^\star)'$ is not a 1-perfect additive code. ∎

Proposition 4.32. *Let C be a 1-perfect code of length $n = 2^t - 1$. Let $S_n(C)$ be the $STS(n)$ associated to C. Let $\mathcal{H}_n$ be the Hamming code of length n. Hence, we obtain*

the following inequation:

$$rank(\mathcal{H}_n) \leq dim(S_n(C)) \leq rank(C).$$

and $r(\mathcal{H}_n) = dim(S_n(C))$ *if and only if* $S_n(C)$ *is isomorphic to* $S_n(\mathcal{H}_n)$.

Proof: Clearly, $dim(S_n) \leq rank(C)$. The other inequation and the condition to the equality can be found in ([AJK92, Theorem 8.2.1]) ∎

By the last proposition, if C is a code of lenght 31, then the dimension of the set of its weight 3 codewords is equals to $r(\mathcal{H}_{31}) = 26$ if and only if this set is isomorphic to the set of weight 3 codewords in $\mathcal{H}_{31}$. In the proof of Proposition 4.31, we have obtained a code of rank 27; that is, a nonlinear code, but the set of its weight 3 codewords is isomorphic to the set of weight 3 codewords in a linear code.

Theorem 4.33. *If* $C^\star$ *is a binary extended* 1*-perfect* $\mathbb{Z}_4$*-linear code of length* $n+1 \geq 16$ *then, the punctured code* $(C^\star)'$ 1*-perfect is not a* 1*-perfect additive code up to the case that* $C^\star$ *equals to the extended of the Hamming code of length* 15.

Proof: Let $C^\star$ be a binary extended 1-perfect $\mathbb{Z}_4$-linear code of length $n+1 \geq 16$. If $C = (C^\star)'$ is a 1-perfect additive code then, by Lemma 4.29 the allowable parameteres of t and δ are:

(i) $t = 4,\ \delta = 1,$

(ii) $t = 4,\ \delta = 2,$

(iii) $t = 5,\ \delta = 1.$

By Proposition 4.30, if $C^\star$ is a binary extended 1-perfect $\mathbb{Z}_4$-linear code with the parameters given in (ii), then the punctured code $(C^\star)'$ is not a 1-perfect additive code. We obtain the same conclusion with Proposition 4.31 and the parameters given in (iii). Finally, the parameters given in (i) correspond to the extended of the Hamming code of length 15. ∎

Chapter 5

Reed-Muller codes

The family of Reed-Muller codes was introduced by Muller in 1954 in [Mul54]. Muller presented a mathematical method to simplify switching circuit. This method can be applied in those circuits that may be represented by using Boolean algebra. As a result, a relationship between Boolean expressions and error-detecting codes of length a power of two was given. The same year, Reed, in [Ree54], analyzed in depth these codes and described a decoding algorithm. One of the most important properties of this family of codes is the ease with which they can be implemented and decoded by using majority-logic circuit. This fact makes these codes very useful even though their minimum distance is relatively small (lower than BCH codes). Finally, we emphasize the mathematical interest of Reed-Muller codes. They are the simplest example of geometrical codes and they are related to affine and projective geometries.

Section 5.1 presents Boolean functions and analyze the connections between them and Reed-Muller codes. In Section 5.2, definitions, constructions and properties of Reed-Muller codes are given. Next, we will establish the relationship between such codes and geometries in Section 5.3 and, finally, we will study the $\mathbb{Z}_4$-linearity of Reed-Muller codes in Section 5.4.

5.1 Boolean functions

As mentioned above, the first definition of Reed-Muller codes was given in terms of Boolean functions. Thus, it is the purpose of this section to introduce Boolean functions to conclude, in the next section, with the first definition of Reed-Muller codes. The definitions of Boolean functions in this section are obtained from [MS77] and [PHB98].

Let m be a positive integer and $n = 2^m$. Any function $f : \mathbb{F}^m \to \mathbb{F}$; that is, a function in m variables that takes on the values 0 and 1 is called a Boolean function. Let $\mathcal{B}$ be the set of all Boolean functions.

Any function $f \in \mathcal{B}$ can be identified with a vector $\mathfrak{f} \in \mathbb{F}^n$ with coordinates the value of f in all 2^m possible arguments. The m-tuples are lexicographically ordered; that is, $(a_1, \ldots, a_m) \leq (b_1, \ldots, b_m)$ if and only if there is an integer k such that $a_k = 0$, $b_k = 1$ and $a_i = b_i$ for $k < i \leq m$.

The usual logical operations, $\cup$ (or), $\cap$ (and), $\neg$ (not) and $\uplus$ (exclusive or), may be applied to Boolean functions. These operations can also be defined in terms of binary functions in the following way:

$$\begin{array}{rcl} f \cap g & \equiv & fg \\ f \cup g & \equiv & f + g + fg \\ \neg f & \equiv & \mathbf{1} + f \\ f \uplus g & \equiv & f + g \end{array} \tag{5.1}$$

Example 5.1.1. *Let $f : \mathbb{F}^2 \to \mathbb{F}$ defined by $f(x_1, x_2) = x_1 \uplus x_2 = x_1 + x_2$. The ordered 2-tuples are $(0,0)$, $(0,1)$, $(1,0)$ and $(1,1)$, and the corresponding vector of length 4 to the function f is $\mathfrak{f} = (0,1,1,0)$.*

Using equivalences given in (5.1) between logical and binary operations and due to the fact that $x_i^2 = x_i$, any Boolean function can be expressed as a linear combination of

$$1, x_1, \ldots, x_m, x_1x_2, \ldots, x_{m-1}x_m, \ldots, x_1x_2 \cdots x_m. \tag{5.2}$$

Therefore, (5.2) is a basis of the set of Boolean functions and if $f \in \mathcal{B}$, we can write

$$f(x_1, \ldots, x_m) = \sum_{(a_1,\ldots,a_m)\in\mathbb{F}^m} c_{(a_1,\ldots,a_m)} x_1^{a_1} \cdots x_m^{a_m},$$

where $c_{(a_1,\ldots,a_m)} \in \mathbb{F}$. The degree of f is defined as

$$max\Big\{ \sum_{i=0}^{m} a_i | c_{(a_1,\ldots,a_m)} \neq 0 \Big\}.$$

Define the i-th coordinate function as $f(x_1, \ldots, x_m) = x_i$ which takes the value 1 on all m-tuples $(x_1, \ldots, x_m)$ with $x_i = 1$. Its corresponding vector in $\mathbb{F}^n$ will be denoted v_i and has weight 2^{m-1}.

Let us order lexicographically all vectors u_j in $\mathbb{F}^m$. If we construct a matrix with columns vectors u_j then, row i is the vector v_i corresponding to the i-th coordinate function.

Example 5.1.2. *m=3, n=8*

	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8
v_1	0	0	0	0	1	1	1	1
v_2	0	0	1	1	0	0	1	1
v_3	0	1	0	1	0	1	0	1

It is easy to check that the j-th coordinate, $j = 1, \ldots, n$, of v_i is 1 if and only if 2^{i-1} occurs in the binary expansion of $j - 1$.

Let $f, g \in \mathcal{B}$ with associated binary vectors $\mathfrak{f}, \mathfrak{g}$ respectively. Then, $f + g, fg \in \mathcal{B}$ and the corresponding binary vectors are, respectively, $\mathfrak{f} + \mathfrak{g}$ and $\mathfrak{fg}$. As the vector associated to the i-th coordiantes function is v_{m-i+1}, the binary vectors corresponding to the basis given in (5.2) is

$$1, v_1, \ldots, v_m, v_1v_2, \ldots, v_{m-1}v_m, \ldots, v_1v_2 \cdots v_m. \tag{5.3}$$

5.2 Definitions and properties

Reed-Muller codes can be defined in a simple way in terms of Boolean functions.

Definition 5.2.1. *The r-th order binary Reed-Muller code $RM(r, m)$ of length $n = 2^m$, for $0 \leq r \leq m$ is the set of all vectors $\mathfrak{f}$ where $f(x_1, \ldots, x_m) \in \mathcal{B}$ has degree at most r.*

A basis of $\mathcal{B}$ is given in (5.2), and therefore, the set of vectors corresponding to this basis, (5.3), is a basis of the code. That way, $RM(r, m)$ consits of all linear combinations of the vectors corresponding to the products

$$\mathbf{1}, v_1, \ldots, v_m, v_1v_2, v_1v_3, \ldots, v_{m-1}v_m, \ldots \text{(up to degree } r\text{)}.$$

The number of different vectors in the basis is

$$k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}.$$

Define

$$P_I(v_1, \ldots, v_m) = \prod_{i \in I} v_i, \tag{5.4}$$

where $I = \{i_1, \ldots, i_s\} \subseteq \{1, \ldots, m\}$, $i_1 < i_2 < \cdots < i_s$, and $P_I = \mathbf{1}$ if $|I| = 0$. Therefore, the r-th order Reed-Muller code of length 2^m can be defined as

$$RM(r, m) = \left\langle \{P_I(v_1 \ldots, v_m)\}_{|I| \leq r} \right\rangle. \tag{5.5}$$

Table 5.1 shows the basis vectors of a $RM(r, 5)$. Vectors $\mathbf{1}$, $v_1, \ldots, v_5$ correspond to the basis vectors of $RM(1, 5)$; $\mathbf{1}$, $v_1, \ldots, v_5$,$v_1v_2, \ldots, v_4v_5$ correspond to the basis vectors of $RM(2, 5)$; $\mathbf{1}$, $\ldots, v_1v_2v_3, \ldots, v_3v_4v_5$ to $RM(3, 5)$, etc. In this example, $RM(0, 5)$ is the code generated by vector $\mathbf{1}$; that is, the repetition code. It is easy to check that $RM(1, 5)$ is the dual of the extended Hamming code and $RM(5, 5)$ is the whole space $\mathbb{F}^{2^5}$. We will see that these properties are, in fact, general properties for any $m \geq 1$.

The following theorem gives us a recursive definition of Reed-Muller codes, using vectors or in terms of generator matrices.

$r = 0$	1	1111	1111	1111	1111	1111	1111	1111	1111
$r = 1$	v_1	0000	0000	0000	0000	1111	1111	1111	1111
	v_2	0000	0000	1111	1111	0000	0000	1111	1111
	v_3	0000	1111	0000	1111	0000	1111	0000	1111
	v_4	0011	0011	0011	0011	0011	0011	0011	0011
	v_5	0101	0101	0101	0101	0101	0101	0101	0101
$r = 2$	v_1v_2	0000	0000	0000	0000	0000	0000	1111	1111
	v_1v_3	0000	0000	0000	0000	0000	1111	0000	1111
	v_1v_4	0000	0000	0000	0000	0011	0011	0011	0011
	v_1v_5	0000	0000	0000	0000	0101	0101	0101	0101
	v_2v_3	0000	0000	0000	1111	0000	0000	0000	1111
	v_2v_4	0000	0000	0011	0011	0000	0000	0011	0011
	v_2v_5	0000	0000	0101	0101	0000	0000	0101	0101
	v_3v_4	0000	0011	0000	0011	0000	0011	0000	0011
	v_3v_5	0000	0101	0000	0101	0000	0101	0000	0101
	v_4v_5	0001	0001	0001	0001	0001	0001	0001	0001
$r = 3$	$v_1v_2v_3$	0000	0000	0000	0000	0000	0000	0000	1111
	$v_1v_2v_4$	0000	0000	0000	0000	0000	0000	0011	0011
	$v_1v_2v_5$	0000	0000	0000	0000	0000	0000	0101	0101
	$v_1v_3v_4$	0000	0000	0000	0000	0000	0011	0000	0011
	$v_1v_3v_5$	0000	0000	0000	0000	0000	0101	0000	0101
	$v_1v_4v_5$	0000	0000	0000	0000	0001	0001	0001	0001
	$v_2v_3v_4$	0000	0000	0000	0011	0000	0000	0000	0011
	$v_2v_3v_5$	0000	0000	0000	0101	0000	0000	0000	0101
	$v_2v_4v_5$	0000	0000	0001	0001	0000	0000	0001	0001
	$v_3v_4v_5$	0000	0001	0000	0001	0000	0001	0000	0001
$r = 4$	$v_1v_2v_3v_4$	0000	0000	0000	0000	0000	0000	0000	0011
	$v_1v_2v_3v_5$	0000	0000	0000	0000	0000	0000	0000	0101
	$v_1v_2v_4v_5$	0000	0000	0000	0000	0000	0000	0001	0001
	$v_1v_3v_4v_5$	0000	0000	0000	0000	0000	0001	0000	0001
	$v_2v_3v_4v_5$	0000	0000	0000	0001	0000	0000	0000	0001
$r = 5$	$v_1v_2v_3v_4v_5$	0000	0000	0000	0000	0000	0000	0000	0001

Table 5.1: Generators of the code $RM(r, 5)$

Theorem 5.1 ([MS77]). *Let r, m be integers such that $0 \leq r \leq m$. The Reed-Muller code $RM(0, m)$ is the repetition code $\{\mathbf{0}, \mathbf{1}\}$ and*

$$RM(r+1, m+1) = \{(u, u+v) | u \in RM(r+1, m), v \in RM(r, m)\}. \tag{5.6}$$

If $G(r, m)$ is the generator matrix of the Reed-Muller code $RM(r, m)$ then, $G(0, m) = (\mathbf{1})$ and

$$G(r+1, m+1) = \begin{pmatrix} G(r+1, m) & G(r+1, m) \\ 0 & G(r, m) \end{pmatrix} \tag{5.7}$$

Note that $G(r, m)$ can be defined as the all columns vectors of $\mathbb{Z}_2^m$.

Example 5.2.1.

$$GM(1,4) = \begin{pmatrix} \mathbf{1} \\ v_4 \\ v_3 \\ v_2 \\ v_1 \end{pmatrix} = \begin{pmatrix} 1111 & 1111 & 1111 & 1111 \\ 0101 & 0101 & 0101 & 0101 \\ 0011 & 0011 & 0011 & 0011 \\ 0000 & 1111 & 0000 & 1111 \\ 0000 & 0000 & 1111 & 1111 \end{pmatrix},$$

$$GM(0,4) = \big(1111111111111111\big).$$

Using (5.7) we obtain the generator matrix of the code $RM(1, 5)$

$$GM(1,5) = \left(\begin{array}{cccc|cccc} 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 \\ 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 \\ 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 \\ 0000 & 1111 & 0000 & 1111 & 0000 & 1111 & 0000 & 1111 \\ 0000 & 0000 & 1111 & 1111 & 0000 & 0000 & 1111 & 1111 \\ \hline 0000 & 0000 & 0000 & 0000 & 1111 & 1111 & 1111 & 1111 \end{array}\right) = \begin{pmatrix} \mathbf{1} \\ v_5 \\ v_4 \\ v_3 \\ v_2 \\ v_1 \end{pmatrix}$$

As a corollary of Theorem 5.1, and considering codes $RM(r+1, m)$ and $RM(r, m)$ as subsets of $\mathbb{Z}_4^{2^m}$, we obtain the following construction of $RM(r+1, m+1)$, where ϕ is the extended Gray map defined in (3.4).

Corollary 5.2. *Let r, m be integers such that $0 \leq r \leq m$.*

$$RM(r+1, m+1) = \phi(2RM(r+1, m)) + \phi(RM(r, m)).$$

The following Lemma gives a property of the generator vectors of $RM(r, m)$ codes. It will allow us to build up a different recursive construction of $RM(r, m)$, for $r \geq 2$.

Lemma 5.3. *Let $I_1, I_2 \subseteq \{1, 2, \ldots, m\}$. Then,*

$$P_{I_1}(v_1, \ldots, v_m) P_{I_2}(v_1, \ldots, v_m) = P_{(I_1 \cup I_2)}(v_1, \ldots, v_m)$$

Proof: By definition, $P_{I_1}(v_1, \ldots, v_m) = \prod_{i \in I_1} v_i$, $P_{I_2}(v_1, \ldots, v_m) = \prod_{i \in I_2} v_i$. Due to the fact that $v_i v_i = v_i$ for $i \in \{1, \ldots, m\}$, $P_{I_1}(v_1, \ldots, v_m) P_{I_2}(v_1, \ldots, v_m) = \prod_{i \in (I_1 \cup I_2)} v_i = P_{(I_1 \cup I_2)}(v_1, \ldots, v_m)$. ∎

Proposition 5.4. *Let r, s, m be integers such that $0 \leq r, s \leq m$. Define*

$$C_{r+s} = \{xy \mid x \in RM(r, m), y \in RM(s, m)\}.$$

Then, $\langle C_{r+s} \rangle = RM(t, m)$, where $t = min\{r + s, m\}$.

Proof: Let $t = min\{r + s, m\}$. Let $x = \sum_{i=0}^{k} P_{I_i}(v_1, \ldots, v_m) \in RM(r, m)$, $y = \sum_{j=0}^{k'} P_{J_j}(v_1, \ldots, v_m) \in RM(s, m)$. By definition, $|I_i| \leq r$ and $|J_j| \leq s$. Thus, $xy = \sum_{i=0}^{k} \sum_{j=0}^{k'} P_{I_i}(v_1, \ldots, v_m) P_{J_j}(v_1, \ldots, v_m)$ that is equals to $\sum_{i=0}^{k} \sum_{j=0}^{k'} P_{(I_i \cup J_j)}(v_1, \ldots, v_m)$ due to Lemma 5.3. As $|I_i \cup J_j| = t$, we obtain that, effectively, $xy \in RM(t, m)$ and $\langle C_{r+s} \rangle \subseteq RM(t, m)$.

Let $P_I(v_1, \ldots, v_m)$ be a generator vector of $RM(t, m)$. $|I| \leq t$, and therefore, there exist I_{i_r}, I_{i_s} such that $|I_{i_r}| \leq r, |I_{i_s}| \leq s$ and $(I_{i_r} \cup I_{i_s}) = I_i$. That way $P_I(v_1, \ldots, v_m) = P_{(I_{i_r} \cup I_{i_s})}(v_1, \ldots, v_m) = P_{I_r}(v_1, \ldots, v_m) P_{I_s}(v_1, \ldots, v_m) \in C_{r+s}$. Hence, $RM(t, m) \subseteq \langle C_{r+s} \rangle$. ∎

The next lemma summarizes the basic properties of Reed-Muller codes. The proof of such properties can be found, for example, in [MS77] and [PHB98]. Nevertheless, most of them are easily derived from the different definitions of the codes.

Lemma 5.5. *Let r, m be integers such that $0 \leq r \leq m$. Let $RM(r,m)$ be the r-th order Reed-Muller code.*

(i) The dimension of the code is $k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$.

(ii) The minimum distance is $d = 2^{m-r}$.

(iii) The weight of $P_I(v_1, \ldots, v_m)$ is 2^{m-i}, where $i = |I|$.

(iv) $RM(r,m) \subset RM(r+1,m)$, $\forall r < m$.

(v) $RM(r,m)^{\perp} = RM(m-r-1,m)$ $\forall r < m$.

As we have seen in the case of the Reed-Muller code of length 2^5, with some specific values of r we obtain well-known codes. We present a list of such different codes (the proof can also be found in [MS77] and [PHB98]):

- $RM(0,m)$ is a repetition code.
- $RM(1,m)$ is the dual of the extended Hamming code, $(H')^{\perp}$.
- $RM(1,m) \subset K_m \subset RM(2,m)$, where K_m is the Kerdock code if $m \geq 4$, m even.
- $RM(m-3,m) \subset P_m \subset RM(m-2,m)$, where P_m is the Preparata code if $m \geq 4$, m even.
- $RM(m-2,m)$ is the extended Hamming code H'.
- $RM(m-1,m)$ is the even code (all vectors in $\mathbb{Z}_2^{2^m}$ of even weight).
- $RM(m,m) = \mathbb{Z}_2^{2^m}$.

Figure 5.1 shows the sequence of Reed-Muller codes.

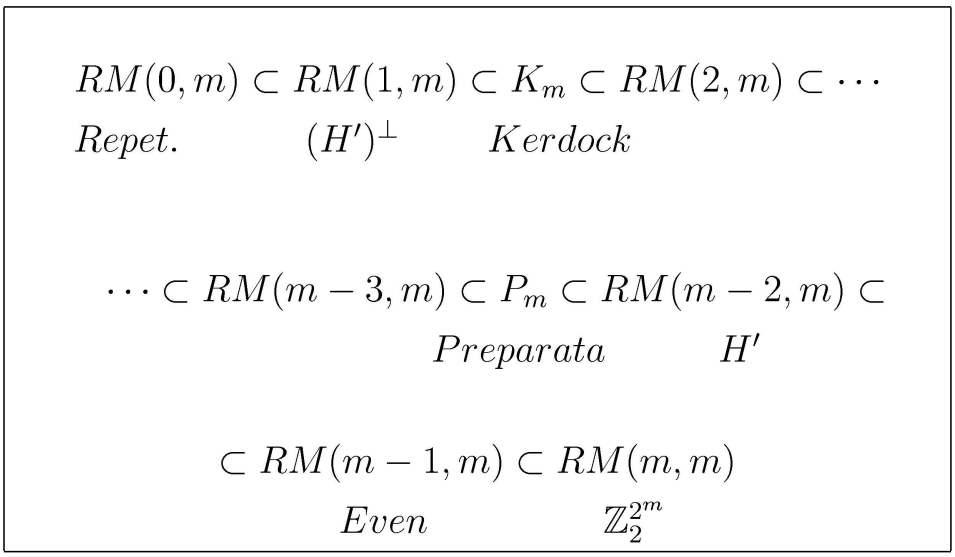

Figure 5.1: Sequence of Reed-Muller codes

5.3 Reed-Muller codes and geometries

In this section we briefly outline an introduction to projective geometries and the connection of such geometries with $RM(r,m)$ codes. All the information in this section can be found in [MS77].

Definition 5.3.1. *A finite projective geometry consist of a finite set V of points $p, q, \ldots$ together with a collection of subsets $L, M, \ldots$ of V called lines, which satisfies axioms (i)-(iv).*

(i) There is a unique line pq passing through any two distinct points p and q.

(ii) Every line contains at least 3 points.

(ii) If distinct lines L, M have a common point p, and if q, r are points of L not equal to p, and s, t are points of M not equal to p, then the lines (qt) and (rs) also have a common point.

(iv) For any point p there are at least two lines not containing p, and for any line L there are at least two points not on L.

A subspace of the projective geometry is a subset S of V such that

(v) If p, q are distinct points of S then S contains all points of the line (pq)

Let $GF(q)$ be a finite field and suppose $m \geq 2$. The points of V are taken to be the nonzero $(m+1)$-tuple

$$(a_0, a_1, \ldots, a_m),\ a_i \in GF(q),$$

with the rule that

$$(a_0, a_1, \ldots, a_m) \text{ and } (\lambda a_0, \lambda a_1, \ldots, \lambda a_m)$$

are the same point, where λ is any nonzero element of $GF(q)$. These are called homogeneous coordinates for the points. There are $q^{m+1} - 1$ nonzero $(m+1)$-tuples, and each point appears $q-1$ times, so the number of points in V is $(q^{m+1}-1)/(q-1)$.

The lines through the points $(a_0, \ldots, a_m)$ and $(b_0, \ldots, b_m)$ consist of the points

$$(\lambda a_0 + \mu b_0, \ldots, \lambda a_m + \mu b_m),$$

where $\lambda, \mu \in GF(q)$ are not both zero. The projective geometry defined in this way is denoted by $PG(m, q)$.

A hyperplane or subspace of dimension $m-1$ in $PG(m, q)$ consist of those points $(a_0, \ldots, a_m)$ which satisties a homogeneous linear equation

$$\lambda_0 a_0 + \lambda_1 a_1 + \cdots + \lambda_m a_m = 0,\ \lambda_i \in GF(q).$$

It is denoted $[\lambda_0, \ldots, \lambda_m]$ or $\lambda_0 X_0 + \lambda_1 X_1 + \cdots + \lambda_m X_m = 0$. The affine geometry $EG(m, q)$ is obtained from $PG(m, q)$ by deleting the points of a hyperplane H. A subspace S of $EG(m, q)$ is called a flat. A flat of dimension r in $EG(m, q)$ is a coset of an $EG(r, q)$, and will be referred as an $EG(r, q)$ or an r-flat. A subspace $PG(r, q)$ of $PG(m, q)$ is also called an r-flat.

Any subset S of the points of $EG(m, 2)$ has associated with it a binary incidence vector $\chi(S)$ of length 2^m, containing a 1 in those components $s \in S$ and zeroes elsewhere.

Similarly, any vector $x = (x_0, \ldots, x_{2^m-1})$ of length 2^m describes a subset S_x of $EG(m, 2)$ consisting of those points P_i for which x_i has value 1.

Therefore, we obtain a one-to-one correspondence between points of $EG(m, 2)$ and coordinate positions of binary vectors of length 2^m.

For example, let us consider $EG(3, 2)$. Such affine geometry contains 2^3 vectors of length 3, said, $P_0, P_1, \ldots, P_7$

P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7
1	1	1	1	0	0	0	0
1	1	0	0	1	1	0	0
1	0	1	0	1	0	1	0

$$\chi(S) = (1, 1, 0, 0, 0, 0, 1, 1) \longleftarrow S = \{P_0, P_1, P_6, P_7\},$$

$$x = (1, 0, 0, 0, 1, 1, 1, 0) \longrightarrow S_x = \{P_0, P_4, P_5, P_6\}.$$

Consider $v_1, \ldots, v_m$ the generating vectors of $RM(1, m)$ and $\bar{v}_1, \ldots, \bar{v}_m$ its complements, $\bar{v}_i = \mathbf{1} + v_i$. Points of $EG(m, 2)$, $P_0, P_1, \ldots, P_{2^m-1}$, are columns of

$$\begin{pmatrix} \bar{v}_1 \\ \bar{v}_2 \\ \vdots \\ \bar{v}_{m-1} \\ \bar{v}_m \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 & 0 & \cdots & 0 & 0 \\ 1 & 1 & \cdots & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 1 & 1 & \cdots & 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 1 & \cdots & 1 & 0 \end{pmatrix}$$

Hyperplanes $X_i = 0$; that is, $[\lambda_0, \ldots, \lambda_{m-1}]$, with $\lambda_i = 1$ and $\lambda_j = 0$, for $j \neq i$, are hyperplanes that pass through the origin. Points in hyperplane $X_i = 0$ are those $(x_0 \ldots, x_{m-1})$ such that $x_i = 0$.

With $m = 3$, we obtain three hyperplanes: $X_0 = 0, X_1 = 0$ and $X_2 = 0$. Note that the incidence vectors of such hyperplanes corresponds to the generator vectors of $RM(1, m)$:

hyperplane H	Set of points	$\chi(H)$
$X_2 = 0$	$\{P_4, P_5, P_6, P_7\}$	$00001111 = v_1$
$X_1 = 0$	$\{P_2, P_3, P_6, P_7\}$	$00110011 = v_2$
$X_0 = 0$	$\{P_1, P_3, P_5, P_7\}$	$01010101 = v_3$

Note that $RM(1, m)$ is spanned by the incidence vectors of hyperplanes, or $(m-1)$-flats, with equation $X_i = 0$.

Vectors v_i themselves are called the characteristic vectors of such $(m-1)$-flats, $v_i v_j$ with $i \neq j$ describes $(m-2)$-flats and so on. That way, $P_I(v_1, \ldots, v_m)$, are characteristic vectors of $(m - |I|)$-flats. $RM(r, m)$ is spanned by the incidence vector of these $(m-s)$-flats, for $0 \leq s \leq r$. We will see more general results with any $(m-r)$-flats, not only the ones defined before.

Let H be any hyperplane in $EG(m, 2)$, $h = \chi(H)$. Note that if $v \in RM(r, m)$ is an incidence vector of S_v, then $hv \in RM(r+1, m)$ and is incidence vector of $S_v \cap H$.

Theorem 5.6 ([MS77]). *Let v be a minimum weight codeword of $RM(r, m)$. Then, S_v is an $(m-r)$-dimensional flat in $EG(m, 2)$that need not pass through the origin.*

The converse of the last theorem is the following theorem.

Theorem 5.7 ([MS77]). *The incidence vector of any $(m-r)$-flat in $EG(m, 2)$ is in $RM(r, m)$. Moreover, they generate $RM(r, m)$.*

Finally, we obtain the following corollary.

Corollary 5.8 ([MS77]). *The minimum weight codewords in $RM(r, m)$ generate $RM(r, m)$.*

5.4 Relationship with quaternary codes

In section 5.2, Reed-Muller codes were presented and their different definitions and their basic properties were given. In this section, the relationship between Reed-Muller codes and quaternary codes will be established. The first question one can

formulate about this topic is when a Reed-Muller code is $\mathbb{Z}_4$-linear code. The answer was partially given in 1994 in [HKC$^+$94] with the following theorem.

Theorem 5.9. *The r-th order binary Reed-Muller code $RM(r,m)$ of length $n = 2^m$, $m \geq 1$, is $\mathbb{Z}_4$-linear for $r = 0, 1, 2, m-1$ and m.*

This theorem was proved in terms of some quaternary codes denoted $ZRM(r,m)$ (further information of these codes in Chapter 7). In the same paper, the authors also conjectured that these were the only values of r such that $RM(r,m)$ was a $\mathbb{Z}_4$-linear code. This fact was proved lately in [HLK98].

Recall the connection between $RM(r,m)$ codes and k-flats in binary m-space. Each coordinate in $RM(r,m)$ corresponds to a binary m-tuple in m-space.

Theorem 5.10. *[MS77, Theorem 24] The automorphism group of the Reed-Muller codes is the general affine group $GA(m)$ acting on the m-space,*

$$\begin{array}{ccc} \mathbb{Z}_2^m & \longrightarrow & \mathbb{Z}_2^m \\ x & \longrightarrow & Ax + b \end{array}$$

for $1 \leq r \leq m-2$. When $r = 0, m-1$ and m, the automorphism group is S_{2^m}.

Lemma 5.11. *Let $\pi \in GA(m)$, $\pi \neq Id, \sigma$. Then, π has $2^k < 2^m$ fixed points.*

Proof: Let $\pi(x) = Ax + b \in GA(m)$, $(A \neq (0))$. Assume $b = 0$. $S = \{x \in \mathbb{Z}_2^m | Ax = x\}$ is a subspace of $\mathbb{Z}_2^m$, and hence, $|S| = 2^k$ for some $k \leq m$.

If $b \neq 0$ then, if there exist an m-tuple a such that $Aa + b = a$, the set $S' = \{x \in \mathbb{Z}_2^m | Ax + b = x\}$ is exactly $S + a$, *an affine subspace or a flat.* Therefore, $|S'| = |S| = 2^k$, for some $k \leq m$. ∎

Corollary 5.12. *Let $1 \leq r \leq m-2$. The number of fixed coordinates in $RM(r,m)$ of any automorphism $\pi \neq Id, \sigma$ is $2^k < 2^m$.*

Lemma 5.13. *Let ϕ be a general Gray map, $1 \leq r \leq m-2$. The number of odd coordinates of $\phi^{-1}(x)$, $x \in RM(r,m)$ is $0, 2^{m-2}$ or 2^{m-1}.*

Proof: Let $x \in RM(r,m)$. π_x is an automorphism and σ is a fixed point free involution on $RM(r,m)$.

The number of odd coordinates of $\phi^{-1}(\mathbf{0})$ and $\phi^{-1}(\mathbf{u})$ are 0 and 2^{m-1} respectively, where $u \in RM(r,m)$ is such that $\pi_{\mathbf{u}} = \sigma$.

Assume $x \in RM(r,m)$ different to $\mathbf{0}$ and $\mathbf{u}$, $1 \leq\ r \leq m-2$.

Since π_x is an automorphism, it fixes 2^k coordinates (Corollary 5.12), and therefore, $\phi^{-1}(x)$ has 2^{k-1} even coordinates. Moreover, $\sigma \circ \pi_x$ is also an automorphism on $RM(r,m)$ and fixes $2^{k'}$. Then, $\phi^{-1}(x)$ has $2^{k'-1}$ odd coordinates. As $2^k, 2^{k'} < 2^m$ and $2^k + 2^{k'} = 2^m$, necessarily, $2^k = 2^{k'} = 2^{m-1}$. That way, $\phi^{-1}(x)$ has 2^{m-2} odd coordinates. ∎

Theorem 5.14. *The r-th order binary Reed-Muller code $RM(r,m)$ of length $n = 2^m$, $m \geq 1$, is $\mathbb{Z}_4$-linear if and only if $r = 0, 1, 2, m-1$ and m.*

Proof: Clearly, for $r = 0, 1, 2, m-1$ and m, $RM(r,m)$ is $\mathbb{Z}_4$-linear due to Theorem 5.9.

To prove the inverse, first note that $RM(r,m)$ is generated by minimum weight codewords (Corollary 5.8); that is, is generated by the codewords of weight 2^{m-r}. Let $1 \leq\ r \leq m-2$, it follows from Lemma 5.13 that the number of odd coordinates of $\phi^{-1}(x)$, $x \in RM(r,m)$ is $0, 2^{m-2}$ or 2^{m-1}. Thus, if $r > 2$ then, all minimum weight codeword x in $RM(r,m)$ is such that $\phi^{-1}(x)$ is an order 2 codeword, and therefore, the code generated has all codewords with $\phi^{-1}(y)$ of order 2, $y \in RM(r,m)$ which is impossible. ∎

Recall that we say a binary code C is $\mathbb{Z}_4$-linear if it is equivalent under coordinate permutation to a general Gray map image $\phi(\mathcal{C})$ of some quaternary code $\mathcal{C} \subseteq \mathbb{Z}_4^n$.

Lemma 5.15. *For $r = 0, m-1$ and m, there exist an unique $\mathbb{Z}_4$-code $\mathcal{C}$ up to isomorphism such that $\phi(\mathcal{C})$ is permutation-equivalent to $RM(r,m)$. Moreover, $\phi^{-1}(RM(r,m))$ is of type $4^0 2^1$, $4^{2^{m-1}-1}2^1$ and $4^{2^{m-1}}$, for $r = 0, m-1$ and m respectively.*

Proof: By definition, $RM(0,m) = \langle \mathbf{1} \rangle$, $RM(m-1,m)$ is the even code and $RM(m,m) = \mathbb{Z}_2^{2^m}$. Therefore, if $r = 0, m-1$ or m, for any coordinate permutation $\pi \in \mathcal{S}_{2^m}$, $\pi(RM(r,m)) = RM(r,m)$. That way, for these values of r, if $\mathcal{C}$ is a quaternary code such that $\phi(\mathcal{C})$ is permutation-equivalent to $RM(r,m)$, then, necessarily, $\mathcal{C} = \phi^{-1}(RM(r,m))$.

Note that $\phi^{-1}(RM(0,m)) = \langle \mathbf{2} \rangle_4$ and $\phi^{-1}(RM(m,m)) = \mathbb{Z}_4^{2^{m-1}}$. Clearly, $\langle \mathbf{2} \rangle_4$ and $\mathbb{Z}_4^{2^{m-1}}$ are $\mathbb{Z}_4$-codes of type $4^0 2^1$ and $4^{2^{m-1}}$ respectively.

Finally, as $RM(m-1,m)$ is the even code and the Gray map is weight-preserving then, $\mathcal{C} = \phi^{-1}(RM(m-1,m))$ is the even code in $\mathbb{Z}_4^{2^{m-1}}$. The dimension of $RM(m-1,m)$ is $2^m - 1$, and therefore, $|\mathcal{C}| = 2^{2^m-1}$. Moreover, the number of order 2 codewords in $\mathcal{C}$ is the number of order 2 codewords in $\mathbb{Z}_4^{2^{m-1}}$; that is, 2^{m-1}. Hence, if $\mathcal{C}$ is of type $4^{k_1}2^{k_2}$ then,

$$\begin{aligned} 2k_1 + k_2 &= 2^m - 1 \\ k_1 + k_2 &= 2^{m-1} \end{aligned}$$

That way, $k_1 = 2^m - 1 - 2^{m-1} = 2^{m-1} - 1$, $k_2 = 1$ and $\mathcal{C}$ is of type $4^{2^{m-1}-1}2^1$. ∎

Let us consider $RM(1,m)$. As mentioned in Section 5.2, it is the dual of the extended Hamming code, and therefore, it is a Hadamard code. $\mathbb{Z}_4$-linear Hadamard codes are characterized in [Kro01], [PRV04] and [PRV05] and we can obtain a characterization of $\mathbb{Z}_4$-linear $RM(1,m)$ codes.

Proposition 5.16. *[PRV04, PRV05] Let δ, γ be positive integers such that $m+1 = \gamma + 2\delta$. For each possible value δ, there exits a unique $\mathbb{Z}_4$-dual code H of the extended 1-perfect $\mathbb{Z}_4$-linear code and all these codes H are pairwise non-equivalent, except for $\delta = 1$ and $\delta = 2$, where the codes H coincides with the binary dual of the extended Hamming code. The generator matrix for the corresponding $\mathbb{Z}_4$-linear code of H consist of all columns vectors of the form $\{\mathbf{1} \in \mathbb{Z}_4\} \times \mathbb{Z}_4^{\delta-1} \times 2\mathbb{Z}_2^{\gamma}$.*

Corollary 5.17. *Let $\mathcal{C}$ be a $\mathbb{Z}_4$-linear code such that $\phi(\mathcal{C})$ is equivalent to $RM(1,m)$, $m \geq 3$. Then, up to isomorphism, $\mathcal{C}$ is of type $4^1 2^{m-1}$ and its generator matrix is*

the all columns vectors of the form $2\mathbb{Z}_2^{m-1} \times \{\mathbf{1} \in \mathbb{Z}_4\}$ *or* $\mathcal{C}$ *is of type* $4^2 2^{m-3}$ *and its generator matrix is the all columns vectors of the form* $2\mathbb{Z}_2^{m-3} \times \{\mathbf{1} \in \mathbb{Z}_4\} \times \mathbb{Z}_4$.

From last corollary, we obtain that there are only two non-isomorphic quaternary codes, one of type $4^1 2^{m-1}$ and the other of type $4^2 2^{m-3}$, such that their image under the Gray map is permutation-equivalent to $RM(1, m)$. Let us consider ϕ the extended Gray map defined in (3.4). In Lemma 5.19 it will be proved that $\phi^{-1}(RM(1, m))$ is, in fact, the quaternary code of type $4^1 2^{m-1}$. First, the next lemma will give the image of the generator vectors of $RM(1, m)$ under the Gray map defined in (3.4).

Lemma 5.18. *Let* v_i *(*$i \in \{1, 2, \ldots, m\}$*) be the generating vectors in* $RM(1, m)$ *and* v'_i *(*$i \in \{1, 2, \ldots, m+1\}$*) be the generating vectors in* $RM(1, m+1)$*. Let* ϕ *be the extended Gray map defined in (3.4). Then,* $\phi(v_i) = v'_1 v'_{i+1}$ *and* $\phi(2v_i) = v'_{i+1}$.

Proof: Notice that, by construction, vectors v'_i can be expressed as $v'_1 = (\mathbf{0}, \mathbf{1})$ and $v'_{i+1} = (v_i, v_i)$ for $i \in \{1, 2, \ldots, m\}$, where $\mathbf{0}$ and $\mathbf{1}$ are the all zeroes and all ones vectors of length 2^m respectively. Therefore, $\phi(2v_i) = (v_i, v_i) = v'_{i+1}$ and $\phi(v_i) = (\mathbf{0}, v_i) = v'_1 v'_{i+1}$ for $i \in \{1, 2, \ldots, m\}$. ∎

Lemma 5.19. *Let* $m \geq 3$*. Let the matrix* G_1 *be the all columns vectors of the form* $2\mathbb{Z}_2^{m-1} \times \{\mathbf{1} \in \mathbb{Z}_4\}$ *and the matrix* G_2*, the all columns vectors of the form* $2\mathbb{Z}_2^{m-3} \times \{\mathbf{1} \in \mathbb{Z}_4\} \times \mathbb{Z}_4$*. Let* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *be the* $\mathbb{Z}_4$*-code generated by* G_1 *and* G_2 *respectively. Then,* $\phi(\mathcal{C}_1) = RM(1, m)$ *and there exist* $\pi \in \mathcal{S}_{2^m}$ *such that* $\pi \circ \phi(\mathcal{C}_2) = RM(1, m)$*, where* ϕ *is the Gray map defined in (3.4).*

Proof: By last corollary, $\phi(\mathcal{C}_1)$ and $\phi(\mathcal{C}_2)$ are equivalent to $RM(1, m)$. Hence, we only have to check that $\phi(\mathcal{C}_1) = RM(1, m)$ or, equivalently, the generator vectors $v_1, \ldots, v_m$ of $RM(1, m)$ are in $\phi(\mathcal{C}_1)$.

Note that, by definition, G_1 can be expressed as

$$G_1 = \begin{pmatrix} 2v'_1 \\ 2v'_2 \\ \cdots \\ 2v'_{m-1} \\ \mathbf{1} \end{pmatrix},$$

where $v'_1, \ldots, v'_{m-1}$ are the generator vectors of $RM(1, m-1)$. Thus, for $i = 1, \ldots, m-1$, we obtain $\phi(2v'_i) = (v'_i, v'_i) = v_{i+1}$ (see Lemma 5.18). Finally, $\phi(\mathbf{1}) = v_1$, and therefore, $v_1, \ldots, v_m \in \phi(\mathcal{C}_1)$. ∎

Example 5.4.1. *Let $\mathcal{C}_1$, $\mathcal{C}_2$ be the two non-isomorphic codes (obtained from the different values of δ) such that $\phi(C_1)$ and $\phi(C_2)$ are codes equivalent to $RM(1,4)$, ϕ defined in (3.4). If $\delta = 1$, then $\mathcal{C}_1$ is of type $4^1 2^3$. If G_1 is the generator matrix of $\mathcal{C}_1$, then*

$$G_1 = \begin{pmatrix} 0202 & 0202 \\ 0022 & 0022 \\ 0000 & 2222 \\ 1111 & 1111 \end{pmatrix}$$

For $\delta = 2$, $\mathcal{C}_2$ is of type $4^2 2^1$ and the generator matrix, G_2 is

$$G_2 = \begin{pmatrix} 0000 & 2222 \\ 1111 & 1111 \\ 0123 & 0123 \end{pmatrix}.$$

Note that

$$\begin{pmatrix} \phi(22222222) \\ \phi(G_1) \end{pmatrix} = \begin{pmatrix} 1111 & 1111 & 1111 & 1111 \\ 0101 & 0101 & 0101 & 0101 \\ 0011 & 0011 & 0011 & 0011 \\ 0000 & 1111 & 0000 & 1111 \\ 0000 & 0000 & 1111 & 1111 \end{pmatrix},$$

that is the generator matrix of $RM(1,4)$. Therefore, $\phi(\mathcal{C}_1) = RM(1,4)$.

As we have seen, $RM(r,m)$ codes are $\mathbb{Z}_4$-linear if and only if $r = 0, 1, 2, m-1$ and m. Let ϕ be the extended Gray map defined in (3.4). In [HKC+94] it was proved that $\phi^{-1}(RM(r,m))$ is a $\mathbb{Z}_4$-code for $r = 0, 1, 2, m-1$ and m. When $3 \leq r \leq m-2$, $\phi^{-1}(RM(r,m))$ is not a quaternary code for any extended Gray map. Up to the end of this chapter, the Gray map ϕ will be the specific extended Gray map defined in (3.4). Using this Gray map we will study which are the codewords missing in $\phi^{-1}(RM(r,m))$ to be a quaternary code. In that case, we can construct the minimum quaternary code $\mathcal{C}$ such that $\phi(\mathcal{C})$ contains the code $RM(r,m)$.

First, we will study some properties of Reed-Muller codes related to its generator basis and the Gray map ϕ.

Let x be a codeword in $RM(r,m)$. The order of x in $(\mathbb{Z}_2^{2^m}, \star)$, $\star$ defined in (2.5), is the order of $\phi^{-1}(x)$ in $(\mathbb{Z}_4^{2^{m-1}}, +)$ (due to (3.5)). The following lemma will show that all vectors $P_I(v_1, \ldots, v_m)$ are order 2 codewords if and only if $1 \notin I$.

Lemma 5.20. *If $1 \notin I$ then $\phi^{-1}(P_I(v_1, \ldots, v_m))$ is an order 2 codeword; otherwise, all nonzero coordinates in $\phi^{-1}(P_I(v_1, \ldots, v_m))$ are of order 4.*

Proof: By construction, $\phi^{-1}(v_1) = \mathbf{1}$; that is, an order 4 codeword, and v_j, for all $j \neq 1$, is an order 2 codeword.

If $1 \notin I$, $P_I(v_1, \ldots, v_m)$ is a componentwise product of vectors of order 2, and therefore, an order 2 codeword. Assume $1 \in I$, $P_I(v_1, \ldots, v_m) = v_1 P_{I\setminus\{1\}}(v_1, \ldots, v_m)$ where $P_{I\setminus\{1\}}(v_1, \ldots, v_m)$ is an order 2 codewords and all coordinates in $\phi^{-1}(v_1)$ are of order 4. Thus, all nonzero coordinates in such a product are of order 4. ∎

Corollary 5.21. *Let $I \subseteq \{2, \ldots, m\}$. Then,*

$$P_I(v_1, \ldots, v_m) = \phi(2\phi^{-1}(v_1 P_I(v_1, \ldots, v_m))).$$

Example 5.4.2. *From Table 5.1, let us consider vector $v_1v_3v_5$:*

$$\begin{array}{c} 0000\ 0000\ 0000\ 0000\ 0000\ 0101\ 0000\ 0101 \\ \downarrow{\scriptstyle \phi^{-1}} \\ 00\ 00\ 01\ 01\ 00\ 00\ 01\ 01 \\ \downarrow \\ 00\ 00\ 02\ 02\ 00\ 00\ 02\ 02 \\ \downarrow{\scriptstyle \phi} \\ 0000\ 0101\ 0000\ 0101\ 0000\ 0101\ 0000\ 0101 \end{array}$$

that is exactly vector v_3v_5.

Corollary 5.22. *Let $I, J \subseteq \{1, 2, \ldots, m\}$. Then,*

$$\phi\big(2\phi^{-1}(P_I(v_1,\ldots,v_m)P_J(v_1,\ldots,v_m))\big) = \begin{cases} 0, & 1 \notin I \cup J, \\ P_{(I\cup J)\setminus\{1\}}(v_1,\ldots,v_m), & 1 \in I \cup J. \end{cases}$$

Proof: Clearly, if $1 \notin I \cup J$, $x = \phi^{-1}(P_I(v_1,\ldots,v_m)P_J(v_1,\ldots,v_m))$ is an order 2 codeword and $\phi(2x) = \mathbf{0}$. Assume $1 \in I \cup J$. Then, $\phi^{-1}(P_I(v_1,\ldots,v_m)P_J(v_1,\ldots,v_m)) = \phi^{-1}(P_{I\cup J}(v_1,\ldots,v_m)) = \phi^{-1}(v_1P_{(I\cup J)\setminus\{1\}}(v_1,\ldots,v_m))$ and the Corollary holds by Corollary 5.21. ∎

Lemma 5.23. *Let σ be defined in (3.6).*

$$\sigma(P_I(v_1,\ldots,v_m)) = \begin{cases} P_I(v_1,\ldots,v_m), & 1 \notin I, \\ P_I(v_1,\ldots,v_m) + P_{I\setminus\{1\}}(v_1,\ldots,v_m), & 1 \in I. \end{cases}$$

Proof: If $1 \notin I$, then $P_I(v_1,\ldots,v_m)$ is an order 2 codeword and $\sigma(P_I(v_1,\ldots,v_m)) = P_I(v_1,\ldots,v_m)$. If $1 \in I$, then $P_I(v_1,\ldots,v_m) = v_1P_{I\setminus\{1\}}(v_1,\ldots,v_m)$ and, all nonzero coordinates in $\phi^{-1}(P_I(v_1,\ldots,v_m))$ are of order 4. That case, $\sigma(P_I(v_1,\ldots,v_m)) = P_I(v_1,\ldots,v_m) + \phi(2\phi^{-1}(P_I(v_1,\ldots,v_m)))$, and the lemma holds by Corollary 5.21. ∎

Corollary 5.24. $\sigma(RM(r,m)) = RM(r,m)$.

Proof: By Lemma 5.23, $\sigma(RM(r,m)) \subset RM(r,m)$. As $RM(r,m)$ and $\sigma(RM(r,m))$ has the same dimension, then $\sigma(RM(r,m)) = RM(r,m)$. ∎

Given two generator vectors $P_{I_1}(v_1,\ldots,v_m)$ and $P_{I_2}(v_1,\ldots,v_m)$, we can consider the two different binary operations $+$ and $\star$ (propelinear operation defined in (2.5)). Any $RM(r,m)$ code is a linear code and, therefore, closed with respect to the operation $+$. To prove that a Reed-Muller code is a $\mathbb{Z}_4$-linear code, we would have to show that the code is closed with respect to the operation $\star$.

Proposition 5.25. *Let $I_1, I_2 \subseteq \{1,2,\ldots,m\}$ such that $|I_1|, |I_2| \leq r$ and $1 \in (I_1 \cap I_2)$. Then,*

$$P_{I_1}(v_1,\ldots,v_m) \star P_{I_2}(v_1,\ldots,v_m) = P_{I_1}(v_1,\ldots,v_m) + P_{I_2}(v_1,\ldots,v_m) + P_{(I_1\cup I_2)\setminus\{1\}}(v_1,\ldots,v_m).$$

Proof: Let $I_1, I_2 \subseteq \{1,2,\ldots,m\}$ such that $|I_1|, |I_2| \leq r$ and $1 \in I_1 \cap I_2$. By equation (2.5)

$$P_{I_1}(v_1,\ldots,v_m) \star P_{I_2}(v_1,\ldots,v_m) = \phi\big(\phi^{-1}(P_{I_1}(v_1,\ldots,v_m)) + \phi^{-1}(P_{I_2}(v_1,\ldots,v_m))\big),$$

that can be written, by (3.8), as

$$\phi\big(\phi^{-1}(P_{I_1}(v_1,\ldots,v_m))\big) + \phi\big(\phi^{-1}(P_{I_2}(v_1,\ldots,v_m))\big) + \phi\big(2\phi^{-1}(P_{I_1}(v_1,\ldots,v_m))\phi^{-1}(P_{I_2}(v_1,\ldots,v_m))\big).$$

Thus, the equality is given if and only if

$$\phi\big(2\phi^{-1}(P_{I_1}(v_1,\ldots,v_m)\big)\phi^{-1}\big(P_{I_2}(v_1,\ldots,v_m)\big) = P_{(I_1\cup I_2)\setminus\{1\}}(v_1,\ldots,v_m),$$

that is true by Corollary 5.21.

∎

Lemma 5.26. *Let C be a binary linear code, $a, b \in C$. Therefore $a \star b \in C$ if and only if $\phi(2\phi^{-1}(a)\phi^{-1}(b)) \in C$.*

Proof: By (3.8) $a+b = \phi(\phi^{-1}(a)+\phi^{-1}(b)+2\phi^{-1}(a)\phi^{-1}(b)) = \phi(\phi^{-1}(a)+\phi^{-1}(b)) + \phi(2\phi^{-1}(a)\phi^{-1}(b)) = a \star b + \phi(2\phi^{-1}(a)\phi^{-1}(b))$. Therefore, $a \star b \in C$ if and only if $\phi(2\phi^{-1}(a)\phi^{-1}(b)) \in C$. ∎

Proposition 5.27. *Let $a, b \in RM(a, b)$. There exist indexes $I_1, \ldots, I_s$ and $J_1, \ldots, J_{s'}$, $|I_i| \leq r$ and $|J_k| \leq r$, such that $a = \sum_{i=1}^{s} P_{I_i}(v_1, \ldots, v_m)$ and $b = \sum_{j=1}^{s'} P_{J_j}(v_1, \ldots, v_m)$. Hence, $a \star b \in RM(r, m)$ if and only if for all pair i,j, where $i \in \{1, \ldots, s\}$ and $j \in \{1, \ldots, s'\}$, $P_{I_i}(v_1, \ldots, v_m) \star P_{J_j}(v_1, \ldots, v_m) \in RM(r, m)$.*

Proof: In all of the proof, we will omit variables v_i writing P_I instead of $P_I(v_1, \ldots, v_m)$.

If $a \star b \in RM(r, m)$ for all $a, b \in RM(r, m)$ then, in particular, $P_I \star P_J \in RM(r, m)$ for all $I, J \subseteq \{1, \ldots, m\}$.

To prove the converse assume that for all pairs $I, J \subseteq \{1, \ldots, m\}$ with $|I| \leq r, |J| \leq r$, $P_I \star P_J \in RM(r, m)$. First of all, since $P_I \star P_J = P_I + \pi_{P_I}(P_J) \in RM(r, m)$, see (2.5) and $P_I \in RM(r, m)$ then, $\pi_{P_I}(P_J) \in RM(r, m)$. Hence, $P_I \star b = P_I + (\sum_{i=1}^{s} \pi_{P_I}(P_{J_i})) \in RM(r, m)$ for any $b = \sum_{i=1}^{s} P_{J_i} \in RM(r, m)$. Since $P_I \star b = b \star P_I = b + \pi_b(P_I) \in RM(r, m)$, it follows by a similar argument that $\pi_b(P_I) \in RM(r, m)$ and thus $b \star a = a \star b \in RM(r, m)$ ∎

From the last proposition, to prove that $\star$ is closed it is enough to check the operation $\star$ on the generator vectors. From Proposition 5.25, if there exist two subsets $I_1, I_2 \subseteq \{1, \ldots, m\}$ such that $1 \in (I_1 \cap I_2)$, $|I_1|, |I_2| \leq r$ and $|(I_1 \cup I_2) \setminus \{1\}| > r$, then $RM(r, m)$ is not a $\mathbb{Z}_4$-linear code. The following lemma shows for which values of r this property is achieved.

Lemma 5.28. *There exist two subsets I_1, I_2 of $\{1, 2, \ldots, m\}$ such that $|I_1|, |I_2| \leq r$, $|I_1 \cap I_2| \geq 1$ and $|I_1 \cup I_2| > r + 1$ if and only if $3 \leq r \leq m - 2$.*

Proof: In cases $r \leq 2$ and $r = m - 1$, it is clear that $|I_1 \cup I_2| - 1 \leq r$.

Let us consider $I_1 = \{1, 2, \ldots, r\}$, $I_2 = \{1, m, \ldots, m-r+1\}$. $|I_1 \cup I_2| = r + |\{i \mid i \leq m, i > max(r, m-r+1)\}|$.

If $m - r + 1 > r$, $|I_1 \cup I_2| = r + (m - (m - r + 1)) = 2r - 1 > r + 1$ if and only if $r \geq 3$. In the case $r \geq m - r + 1$ then, $|I_1 \cup I_2| = r + (m - r - 1) = m - 1 > r + 1$ if and only if $r < m - 2$. Finally, when $r = m - 2$ and $r \geq 3$ then, $|I_1 \cup I_2| = r + 2$.

∎

Proposition 5.29. *$\phi^{-1}(RM(r, m))$ is not a quaternary code if and only if $3 \leq r \leq m - 2$.*

Proof: For $I_1 \subseteq \{2, 3, \ldots, m\}$, $|I_1| \leq r$, $P_{I_1}(v_1, \ldots, v_m)$ is an order 2 codeword. Then, for any $I_2 \subseteq \{1, 2, \ldots, m\}$, $P_{I_1}(v_1, \ldots, v_m) \star P_{I_2}(v_1, \ldots, v_m) = P_{I_1}(v_1, \ldots, v_m) + P_{I_2}(v_1, \ldots, v_m) \in RM(r, m)$.

For all $I_1, I_2 \subseteq \{1, 2, \ldots, m\}$, with $1 \in (I_1 \cap I_2)$, by Proposition 5.25, $P_{I_1}(v_1, \ldots, v_m) \star P_{I_2}(v_1, \ldots, v_m) \in RM(r, m)$ if and only if $P_{(I_1 \cup I_2) \setminus \{1\}}(v_1, \ldots, v_m) \in RM(r, m)$; that is, $|(I_1 \cup I_2) \setminus \{1\}| \leq r$, but by Lemma 5.28, it is not true in general when $3 \leq r \leq m-2$.

∎

For the cases $r \leq 2$ and $r \geq m - 1$, $RM(r, m)$ it was known to be a $\mathbb{Z}_4$-linear code. We have seen that, in the rest of the cases, there are several vectors missing; the ones given by $P_{(I_1 \cup I_2) \setminus \{1\}}(v_1, \ldots, v_m)$ in Proposition 5.29. Such vectors, indeed, should belong to any $\mathbb{Z}_4$-linear code containing $RM(r, m)$.

Theorem 5.30. *Let $\mathcal{C}$ be the minimum quaternary code such that $RM(r, m) \subseteq \phi(\mathcal{C})$. Then, for $3 \leq r \leq m - 2$, $C = \phi(\mathcal{C}) = \{RM(r, m) \cup (\bigcup_{r < |I| \leq t, 1 \notin I} P_I(v_1, \ldots, v_m))\}$, and $|C| = 2^k$, where*

$$k = \sum_{i=0}^{r-1} \binom{m-1}{i} + \sum_{i=0}^{t} \binom{m-1}{i},$$

for $t = min\{m - 1, 2r - 2\}$.

Proof: Let r, m be integers such that $3 \leq r \leq m - 2$. By Proposition 5.25 and, as a corollary of Proposition 5.29, C is a $\mathbb{Z}_4$-linear code containing $RM(r, m)$ if and only

if for all $P_{I_1}(v_1,\ldots,v_m), P_{I_2}(v_1,\ldots,v_m) \in RM(r,m)$, $P_{(I_1\cup I_2)\setminus\{1\}}(v_1,\ldots,v_m) \in C$, where $|(I_1 \cup I_2) \setminus \{1\}| \leq min\{m-1, 2r-2\}$. Therefore, the minimum $\mathbb{Z}_4$-linear code is the one containing $RM(r,m)$ and all vectors $P_{(I_1\cup I_2)\setminus\{1\}}(v_1,\ldots,v_m) \in C$, where $|(I_1 \cup I_2) \setminus \{1\}| \leq t$, where $t = min\{m-1, 2r-2\}$; that is, $C = \{RM(r,m) \cup (\bigcup_{r\leq|I|\leq t, 1\notin I} P_I(v_1,\ldots,v_m))\}$. Finally, $|C| = 2^k$, where $k = dim(RM(r,m))+|\{I \mid r < |I| \leq t\}| = \sum_{i=0}^{r}\binom{m}{i} + \sum_{i=r+1}^{t}\binom{m-1}{i}$ As $\sum_{i=0}^{r}\binom{m}{i} = \sum i=0^{r-1}\binom{m-1}{i} + \sum_{i=0}^{r}\binom{m-1}{i}$ then, $k = \sum i=0^{r-1}\binom{m-1}{i} + \sum i=0^{t}\binom{m-1}{i}$. ∎

Note that last theorem gives the minimum quaternary code such that $\phi(\mathcal{C})$ contains $RM(r,m)$, where ϕ is the Gray map defined in (3.4), that is not the minimum $\mathbb{Z}_4$-linear code containing $RM(r,m)$. There may exist a quaternary code $\mathcal{C}'$ with dimension less than $\mathcal{C}$ and a coordinate permutation π such that $\pi \circ \phi(\mathcal{C}')$ contains $RM(r,m)$ (or, equivalently, a different extended Gray map $\phi' = \pi \circ \phi$). Nevertheless, with the last proposition we can assure the following statement.

Corollary 5.31. *Let C be the minimum $\mathbb{Z}_4$-linear code containing $RM(r,m)$. Then,*

$$dim(C) \leq \sum_{i=0}^{r-1}\binom{m-1}{i} + \sum_{i=0}^{t}\binom{m-1}{i},$$

where $t = min\{m-1, 2r-2\}$.

Proof: The minimum $\mathbb{Z}_4$-linear code containing a linear code is both, $\mathbb{Z}_4$-linear and linear (see Lemma 7.11). Then, if C be the minimum $\mathbb{Z}_4$-linear code containing $RM(r,m)$, C is a linear code and the upper bound of its dimension is obtained from Theorem 5.30. ∎

Chapter 6

QRM codes

In this chapter, we will study a special case of quaternary codes related with Reed-Muller codes; $\mathcal{QRM}$ codes. In this case, however, the map relating both classes of codes is not the Gray map but α (modulo 2) map. The original construction of such codes ([HKC$^+$94]) is given in Section 6.1. After that, in Section 6.2 we will generalize these codes; we will construct the class of $\mathcal{QRM}$ codes ($\overline{\mathcal{QRM}}$). We will calculate the dimension of the kernel and rank of this class in Subsections 6.2.1 and 6.2.2 respectively. Finally, chains of codes in $\overline{\mathcal{QRM}}$ will be studied in Subsection 6.2.3.

6.1 Definitions and properties

$\mathcal{QRM}(r,m)$ codes were defined in [HKC$^+$94] to be quaternary Reed-Muller codes of length 2^m, $\mathcal{QRM}(r,m) \subseteq \mathbb{Z}_4^{2^m}$. The main property of these codes is the fact that their image, under the α map is $RM(r,m)$.

Let $R = \mathbb{Z}_4[\xi]$ be the Galois ring $GR(4^m)$ where ξ is a basic primitive root of unity, so that $\xi^n = 1$, $n = 2^m - 1$. Let us consider T the relative trace defined in (3.10).

Definition 6.1.1. *Let $\mathcal{QRM}(0,m)$ be the quaternary repetition code of length $n = 2^m$*

and for $1 \leq r \leq m$ *let* $\mathcal{QRM}(r,m)$ *be generated by* $\mathcal{QRM}(0,m)$ *together with all vectors of the form*

$$(0, T(\lambda_j), T(\lambda_j\xi^j), T(\lambda_j\xi^{2j}), \ldots, T(\lambda_j\xi^{(n-1)j}))$$

where j *ranges over all representatives of cyclotomic cosets mod* 2^m-1 *for which* $wt(j) \leq r$*, and* λ_j *ranges over* $GR(4)$*. Then,* $\mathcal{QRM}(r,m)$ *is a quaternary code of length* $n = 2^m$ *and type* 4^k*, where*

$$k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}.$$

If $m \geq 3$, m odd $\mathcal{QRM}(1,m)$ is a quaternary Kerdock code ([HKC$^+$94]). In (3.11) we obtain a generator matrix of a such code and, therefore, a generator matrix of $\mathcal{QRM}(1,m)$. We can obtain a construction of a general $\mathcal{QRM}(r,m)$ starting from a similar matrix (see [Wan97]). Let us consider the $((m+1)\times 2^m)$ matrix:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \cdots & \xi^{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ b_{1\infty} & b_{11} & b_{12} & \cdots & b_{1n-1} \\ b_{2\infty} & b_{21} & b_{22} & \cdots & b_{2n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ b_{m\infty} & b_{m1} & b_{m2} & \cdots & b_{mn-1} \end{pmatrix} = \begin{pmatrix} \mathbf{1} \\ u_1 \\ u_2 \\ \vdots \\ u_m \end{pmatrix},$$

where ξ^j is replaced in the second matrix by the m-tuple $(b_{1j}, \ldots, b_{mj}) \in \mathbb{Z}_4^m$ given by $\xi^j = b_{1j} + b_{2j}\xi + \cdots + b_{mj}\xi^{m-1}$. Then, the quaternary r-th order Reed-Muller $\mathcal{QRM}(r,m)$, $0 \leq r \leq m$, of length 2^m is the code generated by the 2^m-tuples of the form

$$\mathbf{1}, u_1, \ldots, u_m, u_1u_2, u_1u_3, \ldots, u_{m-1}v_m, \ldots \text{(up to degree } r).$$

Example 6.1.1. *Let* ξ *be a root of* $h(X) = X^3+2X^2+X+1$*. The generator matrix of* $\mathcal{QRM}(r,m)$*, obtained from* ξ *as in Section 3.5, is*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 0 & 3 & 3 & 3 & 2 \\ 0 & 0 & 0 & 1 & 2 & 3 & 1 & 1 \end{pmatrix}$$

Let us define $P_I(u_1, \ldots, u_m) = \prod_{i \in I} u_i$, where $\prod$ is the componentwise product, $I \subseteq \{1, \ldots, m\}$ and $P_I = \mathbf{1}$ if $|I| = 0$. Then,

$$\mathcal{QRM}(r, m) = \left\langle \{P_I(u_1, \ldots, u_m)\}_{|I| \leq r} \right\rangle_4$$

Both definitions of $\mathcal{QRM}(r, m)$ (Definition 6.1.1 and the last one) are equivalent (see [Wan97]).

Basic properties of $\mathcal{QRM}$ codes are grouped together in the next lemma.

Lemma 6.1 ([HKC$^+$94]). *Let r, m be integers such that $0 \leq r \leq m$. Let $\mathcal{QRM}(r, m)$ be a quaternary Reed-Muller code of length 2^m.*

(i) $\mathcal{QRM}(r, m)$ *is of type* 4^k*, where* $k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$.

(ii) $\mathcal{QRM}(r, m) \subset \mathcal{QRM}(r + 1, m)$, $\forall r < m$.

(iii) $\mathcal{QRM}(r, m)^\perp = \mathcal{QRM}(m - r - 1, m)$, $\forall r < m$.

(iv) $\alpha(\mathcal{QRM}(r, m)) = RM(r, m)$.

As in the case of Reed-Muller codes, we can construct a chain or sequence of $\mathcal{QRM}$ codes that includes some well-known codes. Such codes are listed below and the proof can be found in [HKC$^+$94] and [Wan97]. Figure 6.1 shows the sequence of $\mathcal{QRM}$ codes.

- $\mathcal{QRM}(0, m)$ is a repetition code.
- $\mathcal{QRM}(1, m)$ is the code $\mathcal{K}$ defined in Theorem 3.5.
- $\mathcal{QRM}(m - 2, m)$ is the code $\mathcal{P}$ defined in Theorem 3.6.
- $\mathcal{QRM}(m, m) = \mathbb{Z}_4^{2^m}$.

Corollary 6.2. *Let $m \geq 3$ odd. Then,*

(i) $\phi(\mathcal{QRM}(1, m)) = K_{m+1}$,

$$\mathcal{QRM}(0,m) \subset \mathcal{QRM}(1,m) = \mathcal{K} \subset \mathcal{QRM}(2,m) \subset \cdots$$

Repet.

$$\cdots \subset \mathcal{QRM}(m-3,m) \subset \mathcal{QRM}(m-2,m) = \mathcal{P} \subset$$

$$\subset \mathcal{QRM}(m-1,m) \subset \mathcal{QRM}(m,m)$$

$$\mathbb{Z}_4^{2^m}$$

Figure 6.1: Sequence of $\mathcal{QRM}$ codes

(ii) $\phi(\mathcal{QRM}(m-2,m)) = P_{m+1}$.

Let $\phi : \mathbb{Z}_4^{2^m} \longrightarrow \mathbb{Z}_2^{2^{m+1}}$ be a general Gray map. We define $QRM(r,m) = \phi(\mathcal{QRM}(r,m))$ a binary $\mathbb{Z}_4$-linear code of length 2^{m+1}, and the application:

$$\Psi : \mathbb{Z}_2^{2^{m+1}} \longrightarrow \mathbb{Z}_2^{2^m}$$

grouped by $\Psi(x) = \alpha \circ \phi^{-1}(x)$ (Image 6.2). That way $\Psi(QRM(r,m)) = RM(r,m)$.

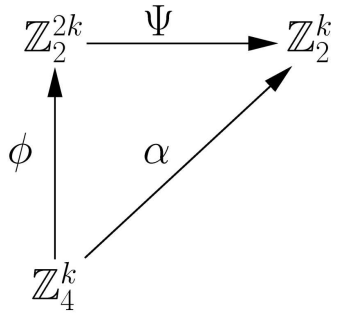

Figure 6.2: Psi map

Lemma 6.3. *$\Psi = \alpha \circ \phi^{-1}$ is a homomorphism between $\mathbb{Z}_2^{2k}$ and $\mathbb{Z}_2^k$.*

Proof: Let us consider $\phi(x), \phi(y) \in \mathbb{Z}_2^{2k}$. By [BPR03], $\phi(x)+\phi(y) = \phi(x+y+2xy)$. Therefore, $\Psi(\phi(x)+\phi(y)) = \Psi(\phi(x+y+2xy)) = \alpha(x+y+2xy) = \alpha(x)+\alpha(y) = \Psi(\phi(x))+\Psi(\phi(y))$. ∎

6.2 Class $\overline{\mathcal{QRM}}(r, m)$ of codes

Even though the best-known $\mathbb{Z}_4$-linear Kerdock and Preparata codes are the ones given in [HKC+94], there are many other nonequivalent $\mathbb{Z}_4$-linear Kerdock and Preparata codes, called Kerdock-like and Preparata-like, all of which seem to have a common set of basic properties ([SZZ71],[SZZ72], [SZZ73], [CCS97],[Kan83]). Hence, it is reasonable to define a class of quaternary Reed-Muller codes which includes all these nonequivalent codes as well as others.

Definition 6.2.1. *Let r, m be integers such that $0 \leq r \leq m$. Let us define $\overline{\mathcal{QRM}}(r, m)$ a class of quaternary Reed-Muller codes where $\mathcal{C} \in \overline{\mathcal{QRM}}(r, m)$ if and only if:*

(i) The quaternary length of the code $\mathcal{C}$ is 2^m.

(ii) $\mathcal{C}$ is of type 4^k, where
$k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$.

(iii) $\alpha(\mathcal{C}) = RM(r, m)$.

We also define the related binary class

$$\overline{QRM}(r, m) = \{C = \phi(\mathcal{C}) \mid \mathcal{C} \in \overline{\mathcal{QRM}}(r, m)\}.$$

Properties *(i)-(iii)* in the definition of the quaternary Reed-Muller codes class, were given in Lemma 6.1 to the particular quaternary code $\mathcal{QRM}(r, m)$. Thus, the quaternary code defined in [HKC+94] belongs to the $\overline{\mathcal{QRM}}(r, m)$ class but other codes belong to this class as well.

Let $\{P_I(v_1,\ldots,v_m)\,|\,|I|\leq r\}$ be the generator vectors of $RM(r,m)$ defined in (5.4). Define the $\mathbb{Z}_4$-code

$$\mathcal{SRM}(r,m)=\left\langle\{P_I(v_1,\ldots,v_m)\,|\,|I|\leq r\}\right\rangle_4. \tag{6.1}$$

By construction, length $\mathcal{SRM}(r,m)$ is 2^m and $\mathcal{SRM}(r,m)$ is of type 4^k, where $k=|\{P_I(v_1,\ldots,v_m)\,|\,|I|\leq r\}|=\sum_{i=0}^{r}\binom{m}{i}$, by Lemma 3.1. Moreover, $\alpha(\mathcal{SRM}(r,m))=RM(r,m)$ and, therefore, $\mathcal{SRM}(r,m)\in\overline{\mathcal{QRM}}(r,m)$.

The minimum distance of $\mathcal{SRM}(r,m)$ code coincides with the minimum distance of $RM(r,m)$; that is, has value 2^{m-r}. Thus, $\mathcal{SRM}(m-2,m)$ has minimum distance 4 whereas $\mathcal{QRM}(m-2,m)$ has minimum distance 6 and, hence, they are different codes in $\overline{\mathcal{QRM}}(r,m)$. Note that if $\mathcal{C}\in\overline{\mathcal{QRM}}(r,m)$, then the minimum distance of $\mathcal{C}$ is greater or equal to 2^{m-r} due to the fact that $\alpha(\mathcal{C})=RM(r,m)$. As a result, $\mathcal{SRM}(r,m)$ codes has the lowest minimum distance of codes in $\overline{\mathcal{QRM}}(r,m)$.

In order to give more examples of codes in $\overline{\mathcal{QRM}}(r,m)$ apart from $\mathcal{QRM}(r,m)$ codes, the Doubling construction will be used. As with Reed-Muller codes, the Doubling construction applied to these codes gives another code in this class; something which is not generally true of the particular codes $\mathcal{QRM}(r,m)$.

Proposition 6.4. *Let $\mathcal{C}\in\overline{\mathcal{QRM}}(r+1,m)$ and $\mathcal{D}\in\overline{\mathcal{QRM}}(r,m)$. Then, the code $\mathcal{C}^*$ defined as $\{(u,u+v)\mid u\in\mathcal{C},v\in\mathcal{D}\}$ belongs to the class $\overline{\mathcal{QRM}}(r+1,m+1)$.*

Proof: By construction, the length of $\mathcal{C}^*$ is 2^{m+1}. Let $(u,u+v)$ be a codeword in $\mathcal{C}^*$, where $u\in\mathcal{C}$ and $v\in\mathcal{D}$. $\alpha(u,u+v)=(\alpha(u),\alpha(u+v))=(\alpha(u),\alpha(u)+\alpha(v))\in RM(r+1,m+1)$. Therefore, $\alpha(\mathcal{C}^*)=RM(r+1,m+1)$. We only have to check that $\mathcal{C}^*$ is of type 4^k, where $k=\sum_{i=0}^{r+1}\binom{m+1}{i}$. Recall that $\mathcal{C}^*$ is of type 4^k if and only if $|\mathcal{C}^*|=4^k$ and the number of order 2 codewords in $\mathcal{C}^*$ is 2^k. As $\mathcal{C}\in\overline{\mathcal{QRM}}(r+1,m)$ and $\mathcal{D}\in\overline{\mathcal{QRM}}(r,m)$, $\mathcal{C}$ is of type 4^{k_1}, where $k_1=\sum_{i=0}^{r+1}\binom{m}{i}$, and $\mathcal{D}$ is of type 4^{k_2}, where $k_2=\sum_{i=0}^{r}\binom{m}{i}$. Moreover, the number of order 2 codewords is 2^{k_1} in $\mathcal{C}$ and 2^{k_2} in $\mathcal{D}$. Note that $|\mathcal{C}^*|=|\mathcal{C}||\mathcal{D}|=4^k$, where $k=k_1+k_2=\sum_{i=0}^{r+1}\binom{m}{i}+\sum_{i=0}^{r}\binom{m}{i}=\sum_{i=0}^{r+1}\binom{m}{i}+\sum_{i=1}^{r+1}\binom{m}{i-1}=\binom{m}{0}+\sum_{i=1}^{r+1}\left[\binom{m}{i}+\binom{m}{i-1}\right]=\binom{m+1}{0}+\sum_{i=1}^{r+1}\binom{m+1}{i}=\sum_{i=0}^{r+1}\binom{m+1}{i}$. Finally,

order 2 codewords in $\mathcal{C}^*$ are those $(u, u+v)$ where both, u and v, are order 2 codewords in $\mathcal{C}$ and $\mathcal{D}$ respectively. Therefore, the number of order 2 codewords in $\mathcal{C}^*$ is $2^{k_1+k_2} = 2^k$.

∎

Finally, we can define codes in $\overline{\mathcal{QRM}}(r, m)$ class in terms of generator matrices.

If G is a quaternary matrix, with row vectors $x_1, x_2, \ldots, x_k$ then, $\alpha(G)$, is defined as

$$\alpha(G) = \begin{pmatrix} \alpha(x_1) \\ \alpha(x_2) \\ \vdots \\ \alpha(x_k) \end{pmatrix}$$

Lemma 6.5. *Let $\mathcal{C} \in \overline{\mathcal{QRM}}(r, m)$ and let G be its generator matrix. Then, $\alpha(G)$ is a generator matrix of $RM(r, m)$.*

Proof: Let $k = \sum_{i=0}^{r} \binom{m}{i}$ and $x_1, x_2, \ldots, x_k$ be the row vectors of G. For any $y \in RM(r, m)$, there exist $x \in \overline{\mathcal{QRM}}(r, m)$ such that $\alpha(x) = y$. x can be expressed as $x = a_1x_1 + a_2x_2 + \cdots + a_kx_k$, where $a_1, \ldots, a_k \in \mathbb{Z}_4$. Hence, $y = \alpha(x) = \alpha(a_1x_1 + a_2x_2 + \cdots + a_kx_k) = \alpha(a_1)\alpha(x_1) + \alpha(a_2)\alpha(x_2) + \cdots + \alpha(a_k)\alpha(x_k)$, where $\alpha(a_1), \ldots, \alpha(a_k) \in \mathbb{Z}_2$ and $\alpha(x_1), \ldots, \alpha(x_k)$ are row vectors of $\alpha(G)$. ∎

Proposition 6.6. *Let $\mathcal{C}$ be a quaternary code of length 2^m. $\mathcal{C}$ belongs to the class $\overline{\mathcal{QRM}}(r, m)$ if and only if there exist a binary $(\sum_{i=0}^{r} \binom{m}{i} \times 2^m)$ matrix, N, such that the generator matrix of $\mathcal{C}$ is*

$$G = G(r, m) + 2N,$$

where $G(r, m)$ is the generator matrix of $RM(r, m)$ defined in (5.7).

Proof: Let N be a binary $(\sum_{i=0}^{r} \binom{m}{i} \times 2^m)$ matrix, $G(r, m)$ the generator matrix of $RM(r, m)$, and $\mathcal{C}$ the quaternary code generated by the matrix $G = G(r, m) + 2N$. By construction, length $\mathcal{C} = 2^m$ and $\alpha(\mathcal{C}) = RM(r, m)$. Moreover any row vectors in

G is an order 4 vector. Then, $\mathcal{C}$ is a quaternary code of type 4^k, where $k = \sum_{i=0}^{r} \binom{m}{i}$, and hence, $\mathcal{C} \in \overline{\mathcal{QRM}}(r, m)$.

Let $\mathcal{C} \in \overline{\mathcal{QRM}}(r, m)$ and G a generator matrix of $\mathcal{C}$ with row vectors $x_1, \ldots, x_k$, where $k = \sum_{i=0}^{r} \binom{m}{i}$. G can by written as $\alpha(G) + 2N$, where

$$2N = \begin{pmatrix} x_1 - \alpha(x_1) \\ x_2 - \alpha(x_2) \\ \vdots \\ x_k - \alpha(x_k) \end{pmatrix}.$$

Let $G(r, m)$ be the generator matrix of $RM(r, m)$ defined in (5.7). As $\alpha(G)$ is a generator matrix of $RM(r, m)$ by Lemma 6.5 then, after a linear row combination of $\alpha(G) + 2N$, we obtain $G(r, m) + 2N'$ that is a generator matrix of $\mathcal{C}$.

∎

Define the set of matrices that are generator matrices of codes in $\overline{\mathcal{QRM}}(r, m)$

$$GQ(r, m) = \{G(r, m) + 2N | N \text{ is a binary } (\sum_{i=0}^{r} \binom{m}{i} \times 2^m) \text{ matrix } \}. \tag{6.2}$$

Note that, if $N = (\mathbf{0})$, the code generated by $G(r, m) \in GQ(r, m)$ is the code $\mathcal{SRM}(r, m)$ defined in (6.1).

Proposition 6.4 can be established in terms of generator matrices as it was done in (5.7) of Theorem 5.1.

Proposition 6.7. *Let $M_1, M_2 \in GQ(r + 1, m)$ and $M_4 \in GQ(r, m)$. The matrix*

$$M = \begin{pmatrix} M_1 & M_2 \\ 2N_3 & M_4 \end{pmatrix}, \tag{6.3}$$

where N_3 is a binary $(\sum_{i=0}^{r} \binom{m}{i} \times 2^m)$ matrix, belongs to $GQ(r + 1, m + 1)$.

Proof: If $M_1, M_2 \in GQ(r+1, m)$ and $M_4 \in GQ(r, m)$ and N_3 is a binary $(\sum_{i=0}^{r} \binom{m}{i} \times 2^m)$, then by (6.3)

$$M = \begin{pmatrix} M_1 & M_2 \\ 2N_3 & M_4 \end{pmatrix} = \begin{pmatrix} G(r+1, m) & G(r+1, m) \\ \mathbf{0} & G(r, m) \end{pmatrix} + \begin{pmatrix} 2N_1 & 2N_2 \\ 2N_3 & 2N_4 \end{pmatrix},$$

where N_1, N_2 and N_4 are binary matrices. Dimension of N_1 and N_2 is $(\sum_{i=0}^{r+1} \binom{m}{i} \times 2^m)$ and dimension of N_4 is $(\sum_{i=0}^{r} \binom{m}{i} \times 2^m)$. Note that if N is defined as

$$N = \begin{pmatrix} N_1 & N_2 \\ N_3 & N_4 \end{pmatrix},$$

then, the dimension of N is $((\sum_{i=0}^{r+1} \binom{m}{i} + \sum_{i=0}^{r} \binom{m}{i}) \times (2^m + 2^m))$ that is, $(\sum_{i=0}^{r+1} \binom{m+1}{i} \times 2^{m+1})$ and $M = G(r+1, m+1) + 2N \in GQ(r+1, m+1)$. ∎

When $N_3 = (\mathbf{0})$, the construction is exactly the Doubling construction of Proposition 6.4.

We will study some general properties of the class $\overline{\mathcal{QRM}}(r, m)$. In particular, is it possible to generalize the rest of the properties of Lemma 6.1 to this class of codes? When the parameters of codes $RM, \mathcal{QRM}, \overline{\mathcal{QRM}}, \ldots$ are omitted, they are exactly r and m.

Lemma 6.8. *Let us consider RM as a subset in $\mathbb{Z}_4^{2^m}$ and $\mathcal{C} \in \overline{\mathcal{QRM}}$. Then, $2\mathcal{C} = 2RM$.*

Proof: Let $\mathcal{C} \in \overline{\mathcal{QRM}}$ and $x \in \mathcal{C}$. By the properties of $\overline{\mathcal{QRM}}$ class, $\alpha(x) \in RM$ and $2x = 2\alpha(x)$. Hence, $2\mathcal{C} = 2\alpha(\mathcal{C}) = 2RM$. ∎

Corollary 6.9. *Let $\mathcal{C}, \mathcal{D} \in \overline{\mathcal{QRM}}$. Then, $2\mathcal{C} = 2\mathcal{D}$.*

In particular, $\mathcal{QRM} \in \overline{\mathcal{QRM}}$ and, therefore, for any code $\mathcal{C} \in \overline{\mathcal{QRM}}$, we obtain $2\mathcal{C} = 2\mathcal{QRM}$. That way, we will denote $2\mathcal{QRM}$ to refer any $2\mathcal{C}$ such that $\mathcal{C} \in \overline{\mathcal{QRM}}$.

Lemma 6.10. *Let $C \in \overline{QRM}$. Then, $C_{Id} = \phi(2\mathcal{QRM})$.*

Proof: Let $\mathcal{C} = \phi^{-1}(C) \in \overline{\mathcal{QRM}}$. Clearly, $\phi(2\mathcal{QRM}) = \phi(2\mathcal{C}) \subseteq C_{Id}$. Now, we will prove that if $x \in C$ such that $\pi_x = Id$, then $x \in \phi(2\mathcal{C})$.

Codes in $\overline{\mathcal{QRM}}$ are quaternary codes of type 4^k; that is, are permutation-equivalents to a code with generator matrix of the form

$$G = \begin{pmatrix} Id_k & A \end{pmatrix},$$

where A is a $\mathbb{Z}_4$-matrix (Chapter 3). Notice that all codewords in the generator matrix have order 4 and, hence, if $x \in \mathcal{C}$ of order 2 then, there exist $y \in \mathcal{C}$ such that $2y = x$. Therefore, all codewords of order 2 in $\mathcal{C}$, that is $\phi^{-1}(C_{Id})$, are in $2\mathcal{C} = 2\mathcal{QRM}$. ∎

We will write QRM_{Id} instead of C_{Id} for any code $C \in \overline{QRM}$, ($C_{Id} = QRM_{Id},\ QRM \in \overline{QRM}$). In fact, $QRM_{Id} = \phi(2\mathcal{QRM})$.

Lemma 6.11. *Let $C \in QRM$ and let $x, y \in C$. Then, $\Psi(x) = \Psi(y)$ if and only if $\pi_x = \pi_y$.*

Proof: If $\Psi(x) = \Psi(y)$, then there exist $z \in \mathcal{C}$ of order 2, such that $\phi^{-1}(x) = z + \phi^{-1}(y)$. Therefore, $\pi_{\phi(z)} = Id$ and $x = \phi(z) \star y$. As $(C, \star)$ is a propelinear code ([PR97b]), then $\pi_x = \pi_{\phi(z)} \circ \pi_y = Id \circ \pi_y = \pi_y$.

Conversely, if $\pi_x = \pi_y$ then, $x = y + z$, where $\phi^{-1}(z)$ is an order 2 codeword and $\Psi(x) = \Psi(y) + \Psi(z) = \Psi(y)$. ∎

Lemma 6.12. *Let $\mathcal{C} \in \overline{\mathcal{QRM}}$. Then, $\mathcal{C}/2\mathcal{QRM} \cong RM$.*

Proof: Let us consider the map

$$\alpha : (\mathcal{C}, +) \longrightarrow (RM, +).$$

Clearly, α is a homomorphism. By the first isomorphism theorem, $\mathcal{C}/ker(\alpha) \cong Im(\alpha)$. Now, $ker(\alpha) = \{x \in \mathcal{C} \mid 2x = \mathbf{0}\} = 2\mathcal{QRM}$ and, by definition of $\overline{\mathcal{QRM}}$, $Im(\alpha) = RM$. ∎

Lemma 6.13. *Let $C \in \overline{QRM}$. Then, $C/QRM_{Id} \cong RM$.*

Proof: Let us consider the map

$$\Psi : (C, \star) \longrightarrow (RM, +).$$

Let $x, y \in C$. $\Psi(x \star y) = \alpha \circ \phi^{-1}(x \star y) = \alpha \circ \phi^{-1}(\phi(\phi^{-1}(x) + \phi^{-1}(y))) = \alpha(\phi^{-1}(x)) + \alpha(\phi^{-1}(y)) = \Psi(x) + \Psi(y)$ and Ψ is a homomorphism. $ker(\Psi) = \{x \in C \mid 2(\phi^{-1}(x)) = \mathbf{0}\} = \phi(\{x \in \mathcal{C} \mid 2x = \mathbf{0}\}) = \phi(2\mathcal{QRM}) = QRM_{Id}$ and the lemma holds using the same argument as in Lemma 6.12. ∎

As a corollary of the last lemma, for any code $C \in \overline{QRM}$, we obtain $|C|/|QRM_{Id}| = |RM|$ and, consequently, $|QRM_{Id}| = 4^k/2^k = 2^k$, where $k = \sum_{i=0}^{r} \binom{m}{i}$. Therefore,

$$dim(QRM_{Id}) = \sum_{i=0}^{r} \binom{m}{i}. \tag{6.4}$$

Moreover, QRM_{Id} not only has the same dimension that RM but also there exist an isomorphism between them.

Lemma 6.14. $(QRM_{Id}, \star) \cong (RM, +)$.

Proof: From Corollary 6.8, $2\mathcal{QRM} = 2RM$ and, by Lemma 6.10, $QRM_{Id} = \phi(2\mathcal{QRM})$. Let define the map $\varphi : RM \to 2QRM_{Id}$ by $\varphi(x) = \phi(2x)$. φ is a homomorphism due to the fact that $\phi(2x)$ and $\phi(2y)$ are order 2 codewords and then, $\varphi(x + y) = \phi(2x + 2y) = \phi(2x) + \phi(2y) = \phi(2x) \star \phi(2y) = \varphi(x) \star \varphi(y)$. As QRM_{Id} and RM have the same dimension, φ is an isomorphism. ∎

Image 6.3 shows the relationship between cosets obtained from Lemmas 6.12 and 6.13 and codewords in a Reed-Muller code.

The following propositions give a generalization of properties (ii) and (iii) of Lemma 6.1. That way, starting from the properties given in the definition of $\overline{\mathcal{QRM}}$, we will prove that codes in such a class fulfill all properties of the initial $\mathcal{QRM}$ code.

Lemma 6.15. *Let $x, y \in \mathbb{Z}_4^n$. Then, $\alpha(x \cdot y) = \alpha(x) \cdot \alpha(y)$.*

Proof: $\alpha(x \cdot y) = \alpha\big(\sum_{i=0}^{n} x_i y_i \pmod 4\big) = \sum_{i=0}^{n} \big(\alpha(x_i y_i)\big) \pmod 2 = \sum_{i=0}^{n} \big(\alpha(x_i)\alpha(y_i)\big) \pmod 2 = \alpha(x) \cdot \alpha(y)$. ∎

Proposition 6.16. *Let $\mathcal{C} \in \overline{\mathcal{QRM}}(r, m)$, $r < m$. Then, $\mathcal{C}^{\perp} \in \overline{\mathcal{QRM}}(m - r - 1, m)$.*

Proof: Let $\mathcal{C} \in \overline{\mathcal{QRM}}(r, m)$. It is clear that the length of $\mathcal{C}^{\perp}$ is 2^m. The number of codewords is $4^{k'} = 4^{2^m - k}$, where $k = \sum_{i=0}^{r} \binom{m}{i}$. Then, $k' = 2^m - \sum_{i=0}^{r} \binom{m}{i} = \sum_{i=r+1}^{m} \binom{m}{i} = \sum_{i=0}^{m-r-1} \binom{m}{i}$. We have to check that $\alpha(\mathcal{C}^{\perp}) = RM(m - r - 1, m) = RM(r, m)^{\perp}$. By definition of $\mathcal{C}$, $RM(r, m)^{\perp} = \alpha(\mathcal{C})^{\perp}$ and, for all x in $RM(r, m)$,

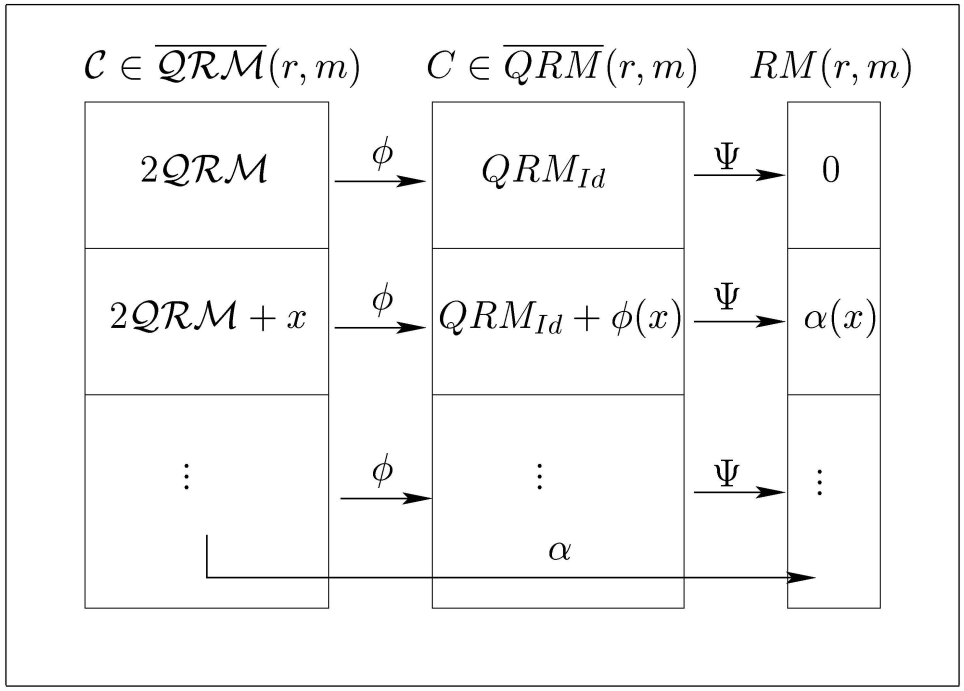

Figure 6.3: Cosets of Reed-Muller and quaternary Reed-Muller codes

there exist $x' \in \mathcal{C}$ such that $\alpha(x') = x$. Let $y \in \mathcal{C}^\perp$, then, using Lemma 6.15, $\alpha(y) \cdot x = \alpha(y) \cdot \alpha(x') = \alpha(y \cdot x') = \alpha(0) = 0$. ∎

Image 6.4 shows the applications involved in the relationship of codes in classes $\overline{QRM}$ and $\overline{\mathcal{QRM}}$, Reed-Muller codes and their duals.

Code $\mathcal{QRM}(r,m) \in \overline{\mathcal{QRM}}(r,m)$ not only has the property that $\mathcal{QRM}^\perp(r,m) \in \overline{\mathcal{QRM}}(m-r-1,m)$, but also $\mathcal{QRM}^\perp(r,m) = \mathcal{QRM}(m-r-1,m)$. That is, the chain of codes $\mathcal{QRM}(r,m)$ in $\overline{\mathcal{QRM}}(r,m)$, $r = 0,\ldots,m$, contains both $\mathcal{QRM}(r,m)$ and $\mathcal{QRM}^\perp(r,m)$ codes.

This fact is not true in general. Let us consider codes $\mathcal{SRM}(r,m) \in \overline{\mathcal{QRM}}(r,m)$ defined in (6.1). By construction, $\mathcal{SRM}(r,m) \subset \mathcal{SRM}(r+1,m)$ for $0 \leq r \leq m-1$, forming a chain of codes in $\overline{\mathcal{QRM}}(r,m)$. However, for a given code $\mathcal{SRM}(r,m)$, its dual code does not belong to the chain. As $\mathcal{SRM}^\perp(r,m) \in \overline{\mathcal{QRM}}(m-r-1,m)$ (by Proposition 6.16) and $\mathcal{SRM}(m-r-1,m) \in \overline{\mathcal{QRM}}(m-r-1,m)$ we only have to check that $\mathcal{SRM}^\perp(r,m) \neq \mathcal{SRM}(m-r-1,m)$.

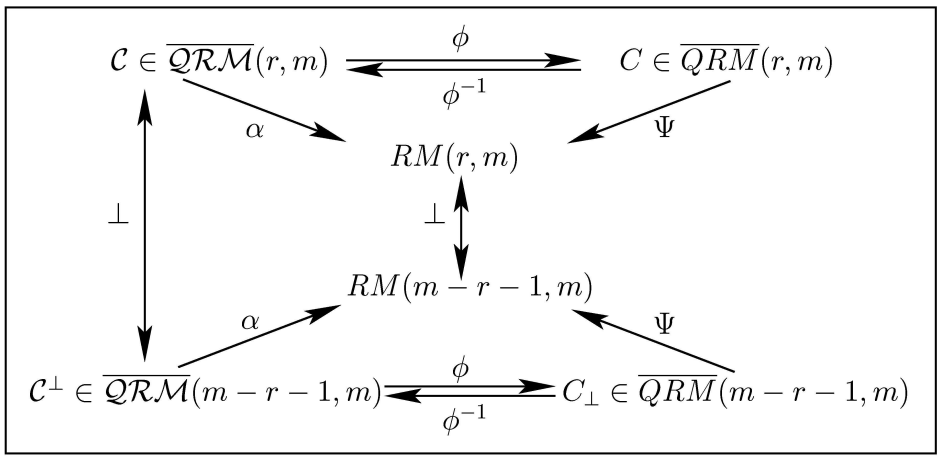

Figure 6.4: Applications between Reed-Muller codes and related codes.

Lemma 6.17. $\mathcal{SRM}(r,m)^{\perp} \neq \mathcal{SRM}(m-r-1,m)$.

Proof: Let $P_I(v_1,\ldots,v_m) \in \mathcal{SRM}(r,m)$ and $P_J(v_1,\ldots,v_m) \in \mathcal{SRM}(m-r-1,m)$ (see (6.1)).

Note that

$$\begin{aligned} &< P_I(v_1,\ldots,v_m), P_J(v_1,\ldots,v_m) >_4 = \\ &w_L(P_I(v_1,\ldots,v_m) \cdot P_J(v_1,\ldots,v_m)) = \\ &\mathrm{wt}(P_{(I \cup J)}(v_1,\ldots,v_m)) = \\ &2^{m-|I \cup J|}. \end{aligned}$$

If $I = \{m, m-1, \ldots, m-r+1\}$ and $J = \{1, 2, \ldots, m-r-1\}$ then, $|I \cup J| = m-1$ and $< P_I(v_1,\ldots,v_m), P_J(v_1,\ldots,v_m) >_4 = 2 \neq 0$. Thus, $\mathcal{SRM}(r,m)^{\perp} \neq \mathcal{SRM}(m-r-1,m)$. ∎

Nevertheless, for all $P_I(v_1,\ldots,v_m) \in \mathcal{SRM}(r,m)$ and $P_J(v_1,\ldots,v_m)$ with $|J| \leq m-r-2$ we can assure that $|I \cup J| \leq m-2$ and their inner product, $2^{m-|I \cup J|}$ is 0 modulo 4. Hence, even though $\mathcal{SRM}(m-r-1,m) \neq \mathcal{SRM}^{\perp}(r,m)$, the code $\mathcal{SRM}(m-r-2,m) \subset \mathcal{SRM}^{\perp}(r,m)$.

Proposition 6.18. *Let $\mathcal{C} \in \overline{\mathcal{QRM}}(r,m)$, with $1 \leq r \leq m$. There exist $\mathcal{D} \in \overline{\mathcal{QRM}}(r-1,m)$ such that $\mathcal{D} \subset \mathcal{C}$.*

Proof: Let $\mathcal{C} \in \overline{\mathcal{QRM}}(r,m)$. By Lemma 6.12 we can write $\mathcal{C}$ as the union of cosets, $\mathcal{C} = 2\mathcal{QRM}(r,m) \cup (2\mathcal{QRM}(r,m) + x_1) \cup (2\mathcal{QRM}(r,m) + x_2) \cup \cdots$, where $y \in 2\mathcal{QRM}(r,m) + x_i$ if and only if $\alpha(y) = \alpha(x_i)$.

We define $2\mathcal{D}$ as $2\mathcal{QRM}(r-1,m) = 2RM(r-1,m)$ (Corollary 6.8). Clearly, $2\mathcal{D} \subset 2\mathcal{C}$. For every coset $2\mathcal{QRM}(r,m) + x_i$ such that $\alpha(x_i) \in RM(r-1,m) \subset RM(r,m)$ we get the coset $2\mathcal{QRM}(r-1,m) + x_i$ of $\mathcal{D}$.

By construction, $\mathcal{D} \subset \mathcal{C}$, the length of $\mathcal{D}$ is 2^m and $\alpha(\mathcal{D}) = RM(r-1,m)$. The number of codewords is $|2\mathcal{QRM}(r-1,m)| \cdot |\{x_i \text{ such that } \alpha(x_i) \in RM(r-1,m)\}|$; that is, $2^{k'} \cdot 2^{k'} = 4^{k'}$, where $k' = \sum_{i=0}^{r-1} \binom{m}{i}$. Therefore, $\mathcal{D} \in \overline{\mathcal{QRM}}(r-1,m)$. ∎

As we have seen in the last proposition, we can construct a chain of codes in $\overline{\mathcal{QRM}}$ codes. Nevertheless, this chain is not unique; given a code $\mathcal{C} \in \overline{\mathcal{QRM}}(r,m)$, there may exist $\mathcal{D}_1, \mathcal{D}_2 \in \overline{\mathcal{QRM}}(r-1,m)$, such that $\mathcal{D}_1 \neq \mathcal{D}_2$ and $\mathcal{D}_1, \mathcal{D}_2 \subset \mathcal{C}$. This is due to the fact that, for a given coset $2\mathcal{QRM}(r,m) + x_i$ and taking y_i in this coset, we obtain $2\mathcal{QRM}(r,m) + x_i = 2\mathcal{QRM}(r,m) + y_i$ but not necessarily $2\mathcal{QRM}(r-1,m) + x_i = 2\mathcal{QRM}(r-1,m) + y_i$. We also can construct a chain of $\overline{\mathcal{QRM}}$ codes in terms of their generator matrices.

Let $\mathcal{C} \subset \overline{\mathcal{QRM}}(r,m)$, and $M \in GQ(r,m)$ its generator matrix. By definition (see (6.2)), $M = G(r,m) + 2N$ for some binary $(\sum_{i=0}^{r} \binom{m}{i} \times 2m)$ matrix, N. If $r \geq 1$, consider the matrix N_{-1} formed by the first $\sum_{i=0}^{r-1} \binom{m}{i}$ row vectors of N. Hence,

$$M_{-1} = G(r-1,m) + 2N_{-1} \in GQ(r-1,m). \tag{6.5}$$

Moreover, if $r < m$, for any binary $(\binom{m}{r+1} \times 2m)$ matrix, N_{+1}, we obtain

$$M_{+1} = G(r+1,m) + \begin{pmatrix} N \\ N_{+1} \end{pmatrix} \in GQ(r+1,m). \tag{6.6}$$

Let $\mathcal{C}_{-1} \in \overline{\mathcal{QRM}}(r-1,m)$ and $\mathcal{C}_{+1} \in \overline{\mathcal{QRM}}(r+1,m)$ be the codes generated by

M_{-1} and M_{+1} respectively. Then,

$$\mathcal{C}_{-1} \subset \mathcal{C} \subset \mathcal{C}_{+1}.$$

Note that, with this construction, code $\mathcal{C}_{+1}$ may not be unique, it depends on the choice of matrix N_{+1}

6.2.1 Kernel of codes in $\overline{\mathcal{QRM}}(r, m)$

Lemma 6.19. *Let $C \in \overline{QRM}$, and let $x \in ker(C)$, $y \in C$ such that $\Psi(x) = \Psi(y)$. Then, $y \in ker(C)$.*

Proof: There exist $\sigma_1, \cdots, \sigma_j \in S_{2^m}$ such that $ker(C) = C_{Id} \cup C_{\sigma_1} \cup \cdots \cup C_{\sigma_j}$. If $x \in ker(C)$, then $C_{\pi_x} \subseteq ker(C)$. Hence, by Lemma 6.11, if $\Psi(x) = \Psi(y)$, $y \in C_{\pi_x} \subseteq ker(C)$. ∎

Let $\mathcal{C} \in \overline{\mathcal{QRM}}$. We define the coset $\mathbf{u} = x + 2\mathcal{QRM} \in \mathcal{C}$, where $\alpha(x) = \mathbf{1} \in RM$. Notice that for all $u \in \mathbf{u}$, $\alpha(u) = \mathbf{1} \in RM$, $2u$ is the all two's vector and $\pi_u = \sigma$.

Lemma 6.20. *Let $C \in \overline{QRM}$. Then, $C_\sigma \subset ker(C)$.*

Proof: Let $C \in \overline{QRM}$ and $u \in \mathbf{u}$. For any $y \in C$, where $y = \phi(x)$, $x \in \mathcal{C}$, $\phi(u) + y = \phi(u) + \phi(x) = \phi(u + x + 2ux) \in C$ by (3.8) and, hence, $\phi(u) \in ker(C)$. Finally, using Lemmas 6.11 and 6.19, $C_\sigma = C_{\pi_{\phi(u)}} \subset ker(C)$. ∎

Lemma 6.21. *Let $\mathcal{C} \in \overline{\mathcal{QRM}}$, where $1 \leq r \leq m-1$, then for all pair of coordinate positions $i, j \in \{1, \ldots, 2^m\}$, there exists $x \in \mathcal{C}$ with exactly 2^{m-r} odd coordinates and such that x has odd coordinates in positions i and j.*

Proof: For $1 \leq r \leq m-2$, $RM(r, m)$ is invariant under the group of all affine transformation of the 2^m-dimensional binary space which is triply transitive (see [MS77]). As a consequence, the nonzero codewords of any weight in RM form a 3-design, and hence a 2-design as well. For $r = m-1$, RM contains all weight two vectors. Then the claim follows taking into account that $\alpha(\mathcal{C}) = RM$. ∎

Proposition 6.22. *Let $C \in \overline{QRM}$. For $0 \leq r \leq m-1$, $ker(C) = QRM_{Id} \cup C_\sigma$.*

Proof: Clearly, $C_{Id} \subset ker(C)$ and therefore, by Lemma 6.20, $C_{Id} \cup C_\sigma \subseteq ker(C)$.

If $r = 0$, then $C = \{\mathbf{0}, \mathbf{1}, \phi(\mathbf{u}), \phi(-\mathbf{u})\}$, where $\phi(\mathbf{u}) \in C_\sigma$, therefore $ker(C) = C = C_{Id} \cup C_\sigma$.

If $1 \leq r \leq m-1$, assume that there is some other codeword $v \in ker(C)$, such that $v \notin C_{Id} \cup C_\sigma$. Note that $v \in ker(C)$ if and only if $\pi_v \in Aut(C)$ [BPRZ03].

For any $x \in \mathcal{C} = \phi^{-1}(C)$, note that $\phi^{-1}\pi_v\phi(x) \in \mathcal{C}$ would be a codeword like x with some coordinates, but not all, with a sign change. Let i be one of these coordinate positions and let j be a coordinate position without sign change. By Lemma 6.21 we can assume that x has exactly 2^{m-r} odd coordinates and x has odd coordinates in positions i and j. Now, let $z = x + \phi^{-1}\pi_v\phi(x) \in \mathcal{C}$. If $\phi(z)$ has weight w, it is clear that $0 < w < 2^{m-r+1}$. But z is an order two codeword, thus $\phi(z) \in C_{Id} = \phi(2\mathcal{QRM})$. But also $C_{Id} = \phi(2RM)$, hence C_{Id} has minimum weight 2^{m-r+1} and we get a contradiction. ∎

Corollary 6.23. *For $0 \leq r \leq m-1$, if $C \in \overline{QRM}$, then*

$$dim(ker(C)) = \sum_{i=0}^{r} \binom{m}{i} + 1,$$

and $dim(ker(C)) = 2^{m+1}$, for $r = m$.

Proof: For $r \leq m-1$, we obtain the result from Proposition 6.22 and (6.4), using $C_\sigma = \{C_{Id} + \phi(u)\}$, for all $C \in \overline{QRM}$, $u \in \mathbf{u}$. And for $r = m$ we have that $C = \mathbb{Z}_2^{m+1}$.
∎

Let $\mathcal{P}$ and $\mathcal{K}$ be the quaternary Preparata-like and Kerdock codes defined in [HKC+94]. In that article, it is proved that $\mathcal{P} = \mathcal{QRM}(2m-3, 2m-1)$ and $\mathcal{K} = \mathcal{QRM}(1, 2m-1)$ and, therefore $\mathcal{P} \in \overline{\mathcal{QRM}}(2m-3, 2m-1)$ and $\mathcal{K} \in \overline{\mathcal{QRM}}(1, 2m-1)$. Moreover, we obtain $\phi(\mathcal{P}) \in \overline{QRM}(2m-3, 2m-1)$ and $\phi(\mathcal{K}) \in \overline{QRM}(1, 2m-1)$. Next Lemma shows that this result is true for any Preparata-like and Kerdock-like code.

Lemma 6.24. *Let P_{2m} be a $\mathbb{Z}_4$-linear Preparata-like code and K_{2m} a $\mathbb{Z}_4$-linear Kerdock-like code of length $n+1 = 2^{2m}$. $P_{2m} \in \overline{QRM}(2m-3, 2m-1)$ and $K_{2m} \in \overline{QRM}(1, 2m-1)$.*

Proof: K_{2m} has the same parameters as the $\mathbb{Z}_4$-linear Kerdock code defined in [HKC+94] and, therefore, $K_{2m} \in \overline{QRM}(1, 2m-1)$ if and only if $\Psi(K_{2m}) = RM(1, 2m-1)$. By [BPRZ03],

$$ker(K_{2m}) = RM(1, 2m) = \langle \phi(RM(0, 2m-1)), \phi(2RM(1, 2m-1)) \rangle.$$

As $\phi(2RM(1, 2m-1)) \subset K_{2m}$ and $\phi^{-1}(K_{2m})$ is a quaternary code of type 4^{2m-1} then, $RM(1, 2m-1) \subset \phi^{-1}(K_{2m})$. Hence, $RM(1, 2m-1) = \alpha(RM(1, 2m-1) \subset \Psi(K_{2m})$. Finally, as $|RM(1, 2m-1)| = 2^{2m+1}$ and $|\phi^{-1}(K_{2m})| = 4^{2m+1}$ it follows that $RM(1, 2m-1) = \Psi(K_{2m})$. If P_{2m} is a $\mathbb{Z}_4$-linear Preparata-like, then $P_{2m} = (K_{2m})_\perp$ where $K_{2m} \in \overline{QRM}(1, 2m-1)$. Then, by Proposition 6.16 $P_{2m} \in \overline{QRM}(2m-3, 2m-1)$. ∎

As a corollary, $\phi^{-1}(P_{2m}) \in \overline{\mathcal{QRM}}(2m-3, 2m-1)$ and $\phi^{-1}(K_{2m}) \in \overline{\mathcal{QRM}}(1, 2m-1)$.

From [BPRZ03], $ker(K_{2m}) = RM(1, 2m)$ and, therefore, $dim(ker(K_{2m})) = 2m + 1$. Moreover, $dim(ker(P_{2m}))$, $dim(P_{Id}(2m))$ and $dim((K_{2m})_{Id})$ can also be found in such article. Nevertheless, the following proposition will present all these results considering such codes as particular cases of codes in the QRM class.

Proposition 6.25. *Let P_{2m} be a $\mathbb{Z}_4$-linear Preparata-like code and K_{2m} a $\mathbb{Z}_4$-linear Kerdock-like code of length $n + 1 = 2^{2m}$. Then*

(i) $dim((P_{2m})_{Id}) = 2^{2m-1} - 2m$, and $dim(ker(P_{2m})) = 2^{2m-1} - 2m + 1$,

(ii) $dim((K_{2m})_{Id}) = 2m$, and $dim(ker(K_{2m})) = 2m + 1$.

Proof: $P_{2m} \in QRM(2m-3, 2m-1)$ and $K_{2m} \in QRM(1, 2m-1)$. Using (6.4) $dim((P_{2m})_{Id}) = \sum_{i=0}^{2m-3} \binom{2m-1}{i} = 2^{2m-1} - 2m$ and $dim((K_{2m})_{Id}) = \sum_{i=0}^{1} \binom{2m-1}{i} = 2m$. In both cases, the dimension of the kernel follows directly from Proposition 6.22. ∎

6.2.2 Rank of codes in $\overline{\mathcal{QRM}}(r,m)$

Let $\mathcal{C}$ be a quaternary code. Let $\bar{\mathcal{C}}$ be defined as the span of the subset containing $2xy$ for all $x, y \in \mathcal{C}$;

$$\bar{\mathcal{C}} = \langle 2xy \mid x, y \in \mathcal{C} \rangle_4. \tag{6.7}$$

Proposition 6.26. *Let $\mathcal{C}$ be a quaternary code, $C = \phi(\mathcal{C})$ and $\bar{\mathcal{C}}$ defined in (6.7). Then, $\langle C \rangle = \phi\big(\mathcal{C} + \bar{\mathcal{C}}\big)$.*

Proof: $\phi\big(\mathcal{C} + \bar{\mathcal{C}}\big)$ is a $\mathbb{Z}_4$-linear code, and, moreover, for all pair of elements $x, y \in \mathcal{C} + \bar{\mathcal{C}}$, $2xy \in \mathcal{C} + \bar{\mathcal{C}}$. Hence, by Theorem 3.4, $\phi\big(\mathcal{C} + \bar{\mathcal{C}}\big)$ is a linear code. Clearly, $C \subseteq \phi\big(\mathcal{C} + \bar{\mathcal{C}}\big)$ and, then, we obtain $\langle C \rangle \subseteq \phi\big(\mathcal{C} + \bar{\mathcal{C}}\big)$.

Let $x, y \in \mathcal{C}$. Using (3.8) we obtain $\phi(2xy) = \phi(x) + \phi(y) + \phi(x+y) \in \langle C \rangle$. For any $z \in \bar{\mathcal{C}}$, z can be expressed as $z = 2x_1y_1 + 2x_2y_2 + \cdots + 2x_ky_k$, where $k \geq 0$ and $x_i, y_i \in \mathcal{C}$, $i \in \{1, \ldots, k\}$. Image under the Gray map of z is $\phi(z) = \phi(2x_1y_1) + \cdots + \phi(2x_ky_k) \in \langle C \rangle$ and, then, $\phi(\bar{\mathcal{C}}) \subseteq \langle C \rangle$. Finally, if $x \in \mathcal{C} + \bar{\mathcal{C}}$ then, $x = c + z$ where $c \in \mathcal{C}$ and $z \in \bar{\mathcal{C}}$ and $\phi(x) = \phi(c) + \phi(z) \in \langle C \rangle$. ∎

Lemma 6.27. *Let $\mathcal{C} \in \overline{\mathcal{QRM}}$, $\bar{\mathcal{C}}$ defined in (6.7). Then, $|\bar{\mathcal{C}}| = 2^k$, where $k = \sum_{i=0}^{t} \binom{m}{i}$, $t = min\{2r, m\}$.*

Proof: $\bar{\mathcal{C}}$ can be defined as $\langle 2\alpha(x)\alpha(y) \mid x, y \in \mathcal{C} \rangle_4$ that is isomorphic to $\langle \alpha(x)\alpha(y) \mid x, y \in \mathcal{C} \rangle$ where $\alpha(x)$, $\alpha(y) \in RM$. Considering the basis of RM and being k such that $|\bar{\mathcal{C}}| = 2^k$, we obtain

$k = |\{P_I(v_1, \ldots, v_m)P_J(v_1, \ldots, v_m) | I, J \subseteq \{1, \ldots, m\}, |I|, |J| \leq r\}| =$

$= |\{P_{(I \cup J)}(v_1, \ldots, v_m) \mid I, J \subseteq \{1, \ldots, m\}, |I|, |J| \leq r\}|$ by Lemma 5.3. Hence, $k = |\{I \cup J \mid I, J \subseteq \{1, \ldots, m\}, |I|, |J| \leq r\}| = |\{I \mid I \subseteq \{1, \ldots, m\}, |I| \leq t\}|$ where $t = min\{2r, m\}$ and this value is exactly $\sum_{i=0}^{t} \binom{m}{i}$.

∎

Lemma 6.28. *Let $\mathcal{C}$ be a quaternary code and $\bar{\mathcal{C}}$ defined in (6.7). Then,*

$$|\mathcal{C} + \bar{\mathcal{C}}| = \frac{|\mathcal{C}||\bar{\mathcal{C}}|}{|\mathcal{C} \cap \bar{\mathcal{C}}|}.$$

Proof: By the second isomorphism theorem, $\mathcal{C}/(\mathcal{C} \cap \bar{\mathcal{C}}) \cong (\mathcal{C} + \bar{\mathcal{C}})/\bar{\mathcal{C}}$ and, therefore, $\frac{|\mathcal{C}|}{|\mathcal{C} \cap \bar{\mathcal{C}}|} = \frac{|\mathcal{C}+\bar{\mathcal{C}}|}{|\bar{\mathcal{C}}|}$.

∎

Proposition 6.29. *Let $C \in \overline{QRM}$. Then,*

$$rank(C) = \sum_{i=0}^{r} \binom{m}{i} + \sum_{i=0}^{t} \binom{m}{i},$$

where $t = min\{2r, m\}$.

Proof: Let $\mathcal{C} \in \overline{\mathcal{QRM}}$, $C = \phi(\mathcal{C})$ and $\bar{\mathcal{C}}$ defined in (6.7). By Proposition 6.26, $\langle C \rangle = \phi(\mathcal{C} + \bar{\mathcal{C}})$. Clearly, $rank(C) = dim\langle C \rangle$ and $|\langle C \rangle| = |\phi(\mathcal{C} + \bar{\mathcal{C}})| = |\mathcal{C} + \bar{\mathcal{C}}|$.

It is easy to check that $\mathcal{C} \cap \bar{\mathcal{C}} = 2\mathcal{QRM}$ and then, $|\mathcal{C}|/|\mathcal{C}+\bar{\mathcal{C}}| = |\mathcal{C}/2\mathcal{QRM}| = |RM|$ using Lemma 6.12. That way, $|\mathcal{C} + \bar{\mathcal{C}}| = |RM||\bar{\mathcal{C}}|$ applying Lemma 6.28 that is equal to $2^{k_1}2^{k_2} = 2^{k_1+k_2}$ where $k_1 = dim(RM) = \sum_{i=0}^{r} \binom{m}{i}$ and $k_2 = \sum_{i=0}^{t} \binom{m}{i}$, where $t = min\{2r, m\}$ by Lemma 6.27. Finally, $rank(C) = dim\langle C \rangle = k_1 + k_2 = \sum_{i=0}^{r} \binom{m}{i} + \sum_{i=0}^{t} \binom{m}{i}$.

∎

As in the case of the kernel of quaternary Kerdock-like and Preparata-like codes, the results of their ranks can be found in [BPRZ03]. These results are obtained as a corollary of the last theorem.

Corollary 6.30. *Let P_{2m} be a $\mathbb{Z}_4$-linear Preparata-like code and K_{2m} a $\mathbb{Z}_4$-linear Kerdock-like code of length $n + 1 = 2^{2m}$. Then*

(i) $rank(P_{2m}) = 2^{2m} - 2m$,

(ii) $rank(K_{2m}) = 2m^2 + m + 1$.

Proof: $P_{2m} \in QRM(2m - 3, 2m - 1)$, therefore $rank(P_{2m}) = \sum_{i=0}^{2m-3} \binom{2m-1}{i} + \sum_{i=0}^{2m-1} \binom{2m-1}{i} = 2^{2m-1} - \binom{2m-1}{2m-2} - \binom{2m-1}{2m-1} + 2^{2m-1} = 2^{2m} - 2m$.

Similarly, $K_{2m} \in QRM(1, 2m - 1)$ and $rank(K_{2m}) = \sum_{i=0}^{1} \binom{2m-1}{i} + \sum_{i=0}^{2} \binom{2m-1}{i} = 2\binom{2m-1}{0} + 2\binom{2m-1}{1} + \binom{2m-1}{2} = 2m^2 + m + 1$. ∎

We present a table with all properties of the Preparata-like, P_m, and Kerdock-like, K_m, codes:

C	K_m	P_m
length	2^m	2^m
d	$2^{m-1} - 2^{(m-2)/2}$	6
$\|C\|$	2^{2m}	2^{2^m-2m}
$dim(C_{Id})$	m	$2^{m-1} - m$
$dim(ker(C))$	$m+1$	$2^{m-1} - m + 1$
$rank(C)$	$(m^2+m)/2 + 1$	$2^m - m$
$\phi^{-1}(C)$ in	$\overline{\mathcal{QRM}}(1, m-1)$	$\overline{\mathcal{QRM}}(m-3, m-1)$

6.2.3 Chain of codes in $\overline{\mathcal{QRM}}(r, m)$

A chain of codes $\mathcal{C}_0 \subseteq \mathcal{C}_1 \subseteq \cdots \subseteq \mathcal{C}_{m-1}$ is denoted $(\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{m-1})$.

We define the set of chain of codes where all codes in the chain belongs to the $\overline{\mathcal{QRM}}(r, m)$ class.

$$\bar{\Gamma} = \{(\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{m-1}) \mid \mathcal{C}_r \in \overline{\mathcal{QRM}}(r, m), r = 0, \ldots, m-1\} \tag{6.8}$$

Due to the fact that if $\mathcal{C} \subset \mathcal{D}$, then $\mathcal{D}^\perp \subset \mathcal{C}^\perp$, we can consider the dual of a chain.

Definition 6.2.2. *The dual of a chain of codes* $(\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{m-1})$ *is*

$$(\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{m-1})^\perp = (\mathcal{C}_{m-1}^\perp, \mathcal{C}_{m-2}^\perp, \ldots, \mathcal{C}_0^\perp). \tag{6.9}$$

If $(\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{m-1})^\perp = (\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{m-1})$*, then it is called a self-dual chain of codes.*

Lemma 6.31. *If* $\Gamma \in \bar{\Gamma}$ *then,* $\Gamma^\perp \in \bar{\Gamma}$.

Proof: Let $\Gamma \in \bar{\Gamma}$; that is, $\Gamma = (\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{m-1})$, where $\mathcal{C}_i \in \overline{\mathcal{QRM}}(i, m)$. As $\Gamma^\perp = (\mathcal{C}_{m-1}^\perp, \mathcal{C}_{m-2}^\perp, \ldots, \mathcal{C}_0^\perp)$, we only have to check that $\mathcal{C}_i^\perp \in \overline{\mathcal{QRM}}(m-i-1, m)$ for all $0 \leq i \leq m-1$, but this is true due to Proposition 6.16. ∎

Two different chains of codes can be found in last section. The class $\overline{\mathcal{QRM}}(r, m)$ was introduced in order to generalize the well-known $QRM(r, m)$ codes. From Lemma 6.1, such codes can be arranged to form a chain of codes (see Image 6.1). Denote

$$\Gamma_{\mathcal{QRM}} = (\mathcal{QRM}(0, m), \mathcal{QRM}(1, m), \ldots, \mathcal{QRM}(m-1, m)). \tag{6.10}$$

Therefore, $\Gamma_{\mathcal{QRM}} \in \bar{\Gamma}$.

A chain of codes can also be constructed with $\mathcal{SRM}(r, m)$ codes defined in (6.1). It will be denote

$$\Gamma_{\mathcal{SRM}} = (\mathcal{SRM}(0, m), \mathcal{SRM}(1, m), \ldots \mathcal{SRM}(m-1, m)). \tag{6.11}$$

Again, note that $\Gamma_{\mathcal{SRM}} \in \bar{\Gamma}$.

By Lemma 6.1, the dual code of $\mathcal{QRM}(r, m)$ is $\mathcal{QRM}(r, m)^{\perp} = \mathcal{QRM}(m - r - 1, m)$ that also belongs to the chain. Therefore, $\Gamma^{\perp}_{\mathcal{QRM}} = \Gamma_{\mathcal{QRM}}$ and $\Gamma_{\mathcal{QRM}}$ is a self-dual chain.

This property of $\Gamma_{\mathcal{QRM}}$ is not a general property. Even though given a code $\mathcal{C} \in \overline{\mathcal{QRM}}(r, m)$, its dual code belongs to $\overline{\mathcal{QRM}}(m - r - 1, m)$, there may exist a chain $\Gamma \in \bar{\Gamma}$ containing $\mathcal{C}$ that do not contains $\mathcal{C}^{\perp}$. This is the case, for example of $\Gamma_{\mathcal{SRM}}$.

Lemma 6.32. $\Gamma_{\mathcal{SRM}} \neq \Gamma^{\perp}_{\mathcal{SRM}}$.

Proof: By Proposition 6.16, $\mathcal{SRM}(r, m)^{\perp}$ belongs to the chain of $\mathcal{SRM}(r, m)$ codes if and only if $\mathcal{SRM}(r, m)^{\perp} = \mathcal{SRM}(m - r - 1, m)$, that is not true by Lemma 6.17.

∎

Construction of chains

Let $1 \leq r \leq m$, $\mathcal{C}_r \in \overline{\mathcal{QRM}}(r, m)$. We have presented different methods to obtain codes $\mathcal{C}_{r-1} \in \overline{\mathcal{QRM}}(r-1, m)$ and $\mathcal{C}_{r+1} \in \overline{\mathcal{QRM}}(r+1, m)$ such that $\mathcal{C}_{r-1} \subset \mathcal{C}_r \subset \mathcal{C}_{r+1}$.

First, in Proposition 6.18, a code $\mathcal{C}_{r-1} \in \overline{\mathcal{QRM}}(r-1, m)$ is given. However, this construction of codes is not unique. We can obtain $\mathcal{C}'_{r-1} \in \overline{\mathcal{QRM}}(r-1, m)$ such that $\mathcal{C}'_{r-1} \neq \mathcal{C}_{r-1}$ and $\mathcal{C}'_{r-1} \subset C$.

The second construction is given in terms of generator matrix. From $M_r \in GQ(r,m)$ the generator matrix of $\mathcal{C}_r$, we obtain $M_{r-1} \in GQ(r-1,m)$ and $M_{r+1} \in GQ(r+1,m)$ ((6.5) and (6.6)) that are generator matrices of some codes $\mathcal{C}_{r-1}$ and $\mathcal{C}_{r+1}$ respectively. In that case, the construction of $\mathcal{C}_{r-1}$ is unique but not the contruction of $\mathcal{C}_{r+1}$.

As a conclusion, we obtain the following lemma.

Lemma 6.33. *Given a code $\mathcal{C} \in \overline{\mathcal{QRM}}(r,m)$, we can construct different $\Gamma \in \bar{\Gamma}$ such that $\mathcal{C}$ is in Γ.*

Minimum distance of chains

Definition 6.2.3. *Let $\Gamma = (\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{m-1}) \in \bar{\Gamma}$. Define the minimum distance of Γ as*

$$d(\Gamma) = (d_0, d_1, \ldots, d_{m-1}), \tag{6.12}$$

where d_i is the minimum distance of $\mathcal{C}_i$.

Lemma 6.34. *Let $\Gamma \in \bar{\Gamma}$, $d(\Gamma) = (d_0, d_1, \ldots, d_{m-1})$. Then,*

(i) $2^{m-r} \leq d_r \leq 2^{m-r+1}$, $0 \leq r \leq m$,

(ii) if $m \geq 3$ odd, $d_1 \leq 2^m - 2^{(m-1)/2}$,

(iii) if $m \geq 3$ odd, $d_{m-2} \leq 6$.

Proof: Let $\mathcal{C} \in \overline{\mathcal{QRM}}(r,m)$, with $0 \leq r \leq m$, and d_r be the minimum distance of $\mathcal{C}$.

In order to establish bounds to d_r, notice that, as $\alpha(\mathcal{C}) = RM(r,m)$, d_r is, at least, the minimum distance of $RM(r,m)$. By Lemma 5.5 and due to the fact that $\mathbf{0} \in RM(r,m)$, the minimum distance of $RM(r,m)$ is 2^{m-r} and, therefore, $d_r \geq 2^{m-r}$.

Let $v \in \mathcal{C}$ such that $\alpha(v)$ is a minimum weight codeword, 2^{m-r}, in $RM(r,m)$. Codeword $2v$ also belongs to $\mathcal{C}$ and $w_L(2v) = 2\mathrm{wt}(\alpha(v)) = 2^{m-r+1}$. Hence $d \leq 2^{m-r+1}$ yielding (i).

To prove (ii) and (iii), we first note that if $m \geq 3$ odd, then $\phi(QRM(1, m)) = K_{m+1}$ and $\phi(QRM(m-2, m)) = P_{m+1}$ (Corollary 6.2). Any code with the same number of codewords than K_{m+1} and P_{m+1} has minimum distance lower than $2^m - 2^{(m-1)/2}$ and 6 respectively ([MS77]). Then, $d_1 \leq 2^m - 2^{(m-1)/2}$ and $d_{m-2} \leq 6$. ∎

Lemma 6.35. $d(\Gamma_{\mathcal{SRM}}) = (2^m, 2^{m-1}, \ldots, 2^{m-r}, \ldots, 2)$.

Note that the minimum distance of any code in $\Gamma_{\mathcal{SRM}}$ is the least possible for codes in $\overline{\mathcal{QRM}}(r, m)$ with the same parameters r and s.

Chapter 7

ZRM codes

In the literature, there are two different definitions of ZRM codes. The first definition was given in [HKC$^+$94] in 1994 and these codes will be denoted $\mathcal{ZRM}(r,m)$. The second one can be found in [Wan97] (1997) and codes in this case are denoted $\mathcal{ZRM}^*(r,m)$. Even though they are not equivalent definitions, in both cases they are used to prove the $\mathbb{Z}_4$-linearity of $RM(r,m)$ (whenever it is a $\mathbb{Z}_4$-linear code). For $r = 0, 1, 2, m-1$ and m, the image of both families of codes under ϕ are Reed-Muller code, where ϕ is the extended Gray map defined in (3.4).

Definitions and constructions of both families of codes are in Section 7.1. The linearity of $\phi(\mathcal{ZRM}(r,m))$ is given in Section 7.2 whereas the computation of the rank and the dimension of the kernel of $\phi(\mathcal{ZRM}^*(r,m))$ is in Section 7.3. Finally, Sections 7.4 and 7.5 relate $ZRM(r,m)$ codes with the family of Reed-Muller codes and codes in the class $\overline{\mathcal{QRM}}(r,m)$, respectively.

Note that if C is a binary code, then $rank(C) = rank(\pi(C))$ and $dim(ker(C)) = dim(ker(\pi(C)))$ for any coordinate permutation π. Moreover, if $\mathcal{C}$ is a linear code then, $\pi(C)$ is also a linear code. That way, in order to obtain the rank and the dimension of the kernel and study the linearity of $\phi(\mathcal{ZRM}(r,m))$ codes, we can apply a specific extended Gray map (a general Gray map is the composition of a coordinate permutation and an extended Gray map). For this reason, in all this

chapter, unless it is said otherwise, ϕ is the extended Gray map defined in (3.4).

7.1 Definitions of $\mathcal{ZRM}(r,m)$ and $\mathcal{ZRM}^*(r,m)$ codes

Let m, r be integers such that $-1 \leq r \leq m+1$. Let $RM(r,m)$ be a r-th order binary Reed-Muller code, $G(r,m)$ its generator matrix and $P_I(v_1 \ldots, v_m)$ its generator vectors for $|I| \leq r$ (Theorem 5.1), where $RM(-1,m) = RM(m+1,m) = \{\mathbf{0}\}$ and $G(-1,m) = G(m+1,m) = (\mathbf{0})$.

Let $\mathcal{ZRM}(r,m)$ be the quaternary code of length 2^m generated by $RM(r-1,m)$ and $2RM(r,m)$;

$$\mathcal{ZRM}(r,m) = \big\langle RM(r-1,m), 2RM(r,m) \big\rangle_4. \tag{7.1}$$

Denote by $ZRM(r,m) = \phi(\mathcal{ZRM}(r,m))$ the $\mathbb{Z}_4$-linear code of length 2^{m+1}.

Let $\mathcal{ZRM}^*(r,m)$ be the $\mathbb{Z}_4$-code of length 2^m generated by the matrix

$$\begin{pmatrix} G(r-1,m) \\ 2G(r,m) \end{pmatrix}.$$

Note that $\mathcal{ZRM}^*(r,m)$ can be defined as

$$\mathcal{ZRM}^*(r,m) = \big\langle \{P_I(v_1,\ldots,v_m) \mid |I| \leq r-1\} \big\rangle_4 + \big\langle \{2P_I(v_1,\ldots,v_m) \mid |I| \leq r\} \big\rangle_4. \tag{7.2}$$

Denote by $ZRM^*(r,m) = \phi(\mathcal{ZRM}^*(r,m))$ the $\mathbb{Z}_4$-linear code of length 2^{m+1}.

In [HKC+94] and [Wan97] can be found the proof of the following Proposition.

Proposition 7.1. *Let $r = 0, 1, 2, m-1$ and m.*

(i) $ZRM(r,m-1) = RM(r,m)$,

(ii) $ZRM^*(r,m-1) = RM(r,m)$.

As a corollary, for the values of r, m such that $RM(r,m)$ is a $\mathbb{Z}_4$-linear code, both definitions, $\mathcal{ZRM}(r,m-1)$ and $\mathcal{ZRM}^*(r,m-1)$, coincide and the binary image of such codes under the Gray map is, exactly, $RM(r,m)$.

Example 7.1.1. *$\mathcal{ZRM}(2,3)$ and $\mathcal{ZRM}^*(2,3)$ are generated by the matrix*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \end{pmatrix} = \begin{pmatrix} v_0 \\ v_3 \\ v_2 \\ v_1 \\ 2v_3v_2 \\ 2v_3v_1 \\ 2v_2v_1 \end{pmatrix}.$$

So we have seen that for some values of r, m, $\mathcal{ZRM}(r,m)$ and $\mathcal{ZRM}^*(r,m)$ codes coincide. What is the difference between such codes? Let u_1, u_2 be codewords in $RM(r-1,m)$. Since u_1 and u_2 belong to both codes, so does their quaternary sum. Now consider their binary sum u_3. By definition, u_3 belongs to $RM(r-1,m) \subseteq \mathcal{ZRM}(r,m)$ but it may not belong to $\mathcal{ZRM}^*(r,m)$. Thus, some of the codewords in $\mathcal{ZRM}(r,m)$ (obtained from the binary sum of codewords) may not be generated in $\mathbb{Z}_4$ by the generator vectors of $\mathcal{ZRM}^*(r,m)$ (Equation (7.2)). We will give a set of generator vectors of $\mathcal{ZRM}(r,m)$ and will see that these codes are equivalent only for the values of r, m of the Proposition 7.1.

Note that, given codewords with all nonzero coordinates equal to one, we may be interested in both, their binary and their quaternary sum. In order to avoid confusion, any binary sum of such codewords x and y will be denoted $x +_b y$ and the quaternary sum is denoted simply $x + y$.

Lemma 7.2. *Let $x_1, x_2, \ldots, x_s$ vectors in $\mathbb{Z}_4^n$ with all nonzero coordinates equal to 1. Then,*

$$x_1 +_b x_2 +_b \cdots +_b x_s = (x_1 + x_2 + \cdots + x_s) + 2\Big(\sum_{1 \le i < j \le s} x_i x_j\Big).$$

Proof: Let a_i be the ℓ-th coordinate of x_i, $i = 1, \ldots, s$. Let $i_1, \ldots i_k \subset \{1, 2, \ldots, s\}$ be indexes of vectors with nonzero ℓ-th coordinate. The ℓ-th coordinate of $x_1 +_b x_2 +_b \cdots +_b x_s$ is $k = a_1 + a_2 + \cdots + a_s \bmod 2$. Moreover, the product $a_i a_j$ is nonzero if and

only if both a_i and a_j are nonzero coordinates; that is, $i, j \in \{i_1, \ldots, i_k\}$. That way, $\sum_{1 \le i < j \le s} 2x_i x_j$ is exactly $2\binom{k}{2} = k(k-1)$ and we only have to check that

$$k \bmod 2 = \big(k + k(k-1)\big) \bmod 4 = k^2 \bmod 4.$$

If $k = 2m$, $m \ge 0$ we obtain $k^2 = 4m^2 = 0 \bmod 4$ whereas if $k = 2m+1$, $k^2 = 4m^2 + 4m + 1 = 1 \bmod 4$; so that, $k \bmod 2$ is, effectively, $k^2 \bmod 4$. ∎

Let us consider $P_I(v_1, \ldots, v_m), P_J(v_1, \ldots, v_m)$ generator vectors in $RM(r, m)$. Clearly, their binary sum belongs to $RM(r, m)$ and, therefore, to $\big\langle RM(r, m)\big\rangle_4$. As these generator vectors also belongs to $\big\langle RM(r, m)\big\rangle_4$ so do their (quaternary) sum.

Thus, both the binary and quaternary sum are codewords in the $\mathbb{Z}_4$-spanned code of $RM(r, m)$ and they are related by the last lemma as follows:

$$P_I(v_1, \ldots, v_m) +_b P_J(v_1, \ldots, v_m)\big) =$$
$$P_I(v_1, \ldots, v_m) + P_J(v_1, \ldots, v_m) + 2P_I(v_1, \ldots, v_m)P_J(v_1, \ldots, v_m)$$

Corollary 7.3. *Let $x_1, x_2, \ldots, x_s$ be vectors in $\mathbb{Z}_4^n$ and let ϕ be a general Gray map. Then,*

$$\phi(x_1 + x_2 + \cdots + x_s) = \phi(x_1) +_b \phi(x_2) +_b \cdots +_b \phi(x_s) +_b 2\Big(\sum_{1 \le i < j \le s} \phi(x_i x_j)\Big).$$

Lemma 7.4. *Let r, m, t be integers such that $0 \le r \le m$ and $t = min\{2r, m\}$. Then, $2P_I(v_1, \ldots, v_m) \in \big\langle RM(r, m)\big\rangle_4$ for all $I \subseteq \{1, 2, \ldots, m\}$ where $|I| \le t$.*

Proof: Let $I \subseteq \{1, 2 \ldots, m\}$ such that $|I| \le t$. There exist $I_1, I_2 \subseteq \{1, 2 \ldots, m\}$, with $|I_1|, |I_2| \le r$ such that $I_1 \cup I_2 = I$. As $P_{I_1}(v_1, \ldots, v_m), P_{I_2}(v_1, \ldots, v_m)$ are codewords in $RM(r, m)$ their binary sum, called s, also belongs to $RM(r, m)$. Therefore, $s - P_{I_1}(v_1, \ldots, v_m) - P_{I_2}(v_1, \ldots, v_m) \in \big\langle RM(r, m)\big\rangle_4$ that is, by Lemma 7.2 $2P_{I_1}(v_1, \ldots, v_m)P_{I_2}(v_1, \ldots, v_m) \in \big\langle RM(r, m)\big\rangle_4$. Using Lemma 5.3,
$2P_{I_1}(v_1, \ldots, v_m)P_{I_2}(v_1, \ldots, v_m) = 2P_{I_1 \cup I_2}(v_1, \ldots, v_m) = 2P_I(v_1, \ldots, v_m) \in \big\langle RM(r, m)\big\rangle_4$.
∎

As $\big\langle RM(r-1, m)\big\rangle_4 \subseteq \mathcal{ZRM}(r, m)$ by definition, we obtain directly the following corollary.

Corollary 7.5. *Let r, m, t be integers such that $0 \leq r \leq m$ and $t = min\{2r-2, m\}$. Then, $2P_I(v_1, \ldots, v_m) \in \mathcal{ZRM}(r,m)$ for all $I \subseteq \{1, 2, \ldots, m\}$ where $|I| \leq t$.*

Proposition 7.6. *Let r, m be integers such that $0 \leq r \leq m$. Then,*

$$\langle RM(r,m)\rangle_4 = \langle \{P_I(v_1, \ldots, v_m) \,|\, |I| \leq r\}\rangle_4 + \langle \{2P_I(v_1, \ldots, v_m) \,|\, r+1 \leq |I| \leq t\}\rangle_4,$$

where $t = min\{2r, m\}$.

Proof: Let $x \in RM(r,m)$. x can be expressed as the binary sum of some generator vectors $P_{I_1}(v_1, \ldots, v_m), \ldots, P_{I_s}(v_1, \ldots, v_m)$ and, by Lemma 7.2, $x = P_{I_1}(v_1, \ldots, v_m) + \cdots + P_{I_s}(v_1, \ldots, v_m) + 2\big(\sum_{1 \leq i < j \leq s} P_{I_i}(v_1, \ldots, v_m) P_{I_j}(v_1, \ldots, v_m)\big) \in \langle RM(r,m)\rangle_4$. As $|I_i| \leq r$, $P_{I_i}(v_1, \ldots, v_m) P_{I_j}(v_1, \ldots, v_m) = P_{I_i \cup I_j}(v_1, \ldots, v_m)$ with $0 \leq |I_i \cup I_j| \leq min\{2r, m\}$. Thus, if $t = min\{2r, m\}$,
$x \in \langle \{P_I(v_1, \ldots, v_m) \,|\, |I| \leq r\}\rangle_4 + \langle \{2P_I(v_1, \ldots, v_m) \,|\, |I| \leq t\}\rangle_4 =$
$\langle \{P_I(v_1, \ldots, v_m) \,|\, |I| \leq r\}\rangle_4 + \langle \{2P_I(v_1, \ldots, v_m) \,|\, r+1 \leq |I| \leq t\}\rangle_4$.

That way, if $x \in RM(r,m)$ there exist $a \in \langle \{P_I(v_1, \ldots, v_m) \,|\, |I| \leq r\}\rangle_4$ and $b \in \langle \{2P_I(v_1, \ldots, v_m) \,|\, r+1 \leq |I| \leq t\}\rangle_4$ such that $x = a + b$.

Let us consider $\lambda_1 x_1 + \cdots + \lambda_k x_k \in \langle RM(r,m)\rangle_4$ where $x_i \in RM(r,m)$ and $\lambda_i \in \mathbb{Z}_4$. Then, $\lambda_1 x_1 + \cdots + \lambda_k x_k = (\lambda_1 a_1 + \cdots + \lambda_k a_k) + (\lambda_1 b_1 + \cdots + \lambda_k b_k)$, where $\lambda_1 a_1 + \cdots + \lambda_k a_k \in \langle \{P_I(v_1, \ldots, v_m) \,|\, |I| \leq r\}\rangle_4$ and $\lambda_1 b_1 + \cdots + \lambda_k b_k \in \langle \{2P_I(v_1, \ldots, v_m) \,|\, r+1 \leq |I| \leq t\}\rangle_4$. As a result,

$$\langle RM(r,m)\rangle_4 \subseteq \langle \{P_I(v_1, \ldots, v_m) \,|\, |I| \leq r\}\rangle_4 + \langle \{2P_I(v_1, \ldots, v_m) \,|\, r+1 \leq |I| \leq t\}\rangle_4.$$

Clearly, $\langle \{P_I(v_1, \ldots, v_m) \,|\, |I| \leq r\}\rangle_4 \subseteq \langle RM(r,m)\rangle_4$, therefore, to prove the converse we only have to check that $\langle \{2P_I(v_1, \ldots, v_m) \,|\, r+1 \leq |I| \leq t\}\rangle_4 \subseteq \langle RM(r,m)\rangle_4$ but this is true due to Lemma 7.4. ∎

Proposition 7.7. *Let r, m be integers such that $2 \leq r \leq m+1$. Then,*

$$\mathcal{ZRM}(r,m) = \langle RM(r-1,m)\rangle_4.$$

Proof:

By definition, $\mathcal{ZRM}(r,m) = \big\langle RM(r-1,m), 2RM(r,m)\big\rangle_4 = \big\langle RM(r-1,m)\big\rangle_4 + \big\langle 2RM(r,m)\big\rangle_4$.

Clearly, $\big\langle RM(r-1,m)\big\rangle_4 \subseteq \mathcal{ZRM}(r,m)$. Hence, we only have to check that $\big\langle 2RM(r,m)\big\rangle_4 \subseteq \big\langle RM(r-1,m)\big\rangle_4$.

Now, let $P_{I_1}(v_1,\cdots,v_m),\ldots,P_{I_s}(v_1,\cdots,v_m) \in RM(r,m)$. Note that $2P_{I_1}(v_1,\cdots,v_m)+\cdots+2P_{I_s}(v_1,\cdots,v_m) = 2\big(P_{I_1}(v_1,\cdots,v_m)+_b\cdots+_b P_{I_s}(v_1,\cdots,v_m)\big)$. Therefore, by Proposition 7.6, $\big\langle 2RM(r,m)\big\rangle_4 = \big\langle\{2P_I(v_1,\ldots,v_m)\,|\,|I|\le r\}\big\rangle_4 \subseteq \big\langle RM(r-1,m)\big\rangle_4$ if and only if $r \le min\{2r-2,m\}$; that is, $r \le m$ and $r \le 2r-2$ or, equivalently, $2 \le r \le m$. Thus, for $r \le 2r-2$, $\mathcal{ZRM}(r,m) = \big\langle RM(r-1,m)\big\rangle_4$.

Finally, if $r = m+1$, $\mathcal{ZRM}(m+1,m) = \big\langle RM(m,m), 2RM(m+1,m)\big\rangle_4 = \big\langle RM(m,m)\big\rangle_4$ by definition of $RM(m+1,m)$. ∎

Corollary 7.8. *Let r,m be integers such that $2 \le r \le m+1$. Then,*

$$\mathcal{ZRM}(r,m) = \big\langle\{P_I(v_1,\ldots,v_m)\,|\,|I|\le r-1\}\big\rangle_4 + \big\langle\{2P_I(v_1,\ldots,v_m)\,|\,r\le|I|\le t\}\big\rangle_4,$$

where $t = min\{2r-2,m\}$. Moreover,

$$\mathcal{ZRM}(0,m) = \big\langle\{\mathbf{2}\}\big\rangle_4,$$

$$\mathcal{ZRM}(1,m) = \big\langle\{\mathbf{1}\}\big\rangle_4 + \big\langle\{2P_I(v_1,\ldots,v_m)\,|\,|I|\le 1\}\big\rangle_4.$$

Proof: When $2 \le r \le m$, the equality follows from propositions 7.6 and 7.7. The rest of the cases are obtained applying the definition of $\mathcal{ZRM}(r,m)$. ∎

Proposition 7.9. *$\mathcal{ZRM}(r,m) = \mathcal{ZRM}^*(r,m)$ if and only if $r = 0,1,2,m$ and $m+1$.*

Proof: From Proposition 7.1, if $r = 0,1,2,m$ and $m+1$, then $\mathcal{ZRM}(r,m) = \mathcal{ZRM}^*(r,m)$.

By equation (7.2) and Corollary 7.8, $\mathcal{ZRM}(r,m) = \mathcal{ZRM}^*(r,m)$ if and only if $\big\langle\{2P_I(v_1,\ldots,v_m)\,|\,r\le|I|\le t\}\big\rangle_4 = \big\langle\{2P_I(v_1,\ldots,v_m)\,|\,|I|\le r\}\big\rangle_4$, where $t = min\{2r-2,m\}$; that is, if and only if $r \ge min\{2r-2,m\}$. The equality is given if and only if $r \ge 2r-2$ or $r \ge m$; equivalently, for values $r = 0,1,2,m$ and $m+1$. ∎

7.2 Linearity of $ZRM(r, m)$ codes

Proposition 7.10. *$\mathcal{ZRM}(r, m)$ is a quaternary code of length 2^m and type $4^{k_1}2^{k_2}$, where $k_1 = \sum_{i=0}^{r-1} \binom{m}{i}$ and $k_2 = \sum_{i=r}^{t} \binom{m}{i}$, $t = min\{2r-2, m\}$.*

Proof: By Corollary 7.8,

$$\mathcal{ZRM}(r, m) = \left\langle \{P_I(v_1, \ldots, v_m) \,|\, |I| \leq r-1\} \right\rangle_4 + \left\langle \{2P_I(v_1, \ldots, v_m) \,|\, r \leq |I| \leq t\} \right\rangle_4,$$

where $t = min\{2r-2, m\}$. Note that $\{P_I(v_1, \ldots, v_m) \,|\, |I| \leq t\}$, are linearly independent binary vectors and, applying Lemma 3.1, $\mathcal{ZRM}(r, m)$ is of type $4^{k_1}2^{k_2}$ where $k_1 = \sum_{i=0}^{r-1} \binom{m}{i}$ and $k_2 = \sum_{i=r}^{t} \binom{m}{i}$. ∎

Lemma 7.11. *Let C be a binary linear code and $\mathcal{C} = \left\langle C \right\rangle_4$. Then, $\phi(\mathcal{C})$ is a linear code, where ϕ is a general Gray map.*

Proof: Let $x, y \in C$. By Lemma 7.2, $2xy = x +_b y - (x + y) \in \mathcal{C}$.

Now, consider two codewords $x, y \in \mathcal{C}$. As $\mathcal{C} = \left\langle C \right\rangle_4$, $x = x_1 + \cdots + x_s$ and $y = y_1 + \cdots + y_t$, where $x_i, y_j \in C$ for all $i = 1, \ldots, s; j = 1, \ldots, t$. $2xy = 2(x_1 + \cdots + x_s)(y_1 + \cdots + y_t) = \sum_{i,j} 2x_i y_j \in \mathcal{C}$. Therefore, $\phi(C)$ is a linear code by Theorem 3.4. ∎

Proposition 7.12. *$ZRM(r, m)$ are linear codes and*

$$dim(ZRM(r, m)) = \sum_{i=0}^{r-1} \binom{m}{i} + \sum_{i=0}^{t} \binom{m}{i},$$

where $t = min\{2r-2, m\}$.

Proof: $\mathcal{ZRM}(r, m) = \left\langle RM(r-1, m) \right\rangle_4$ by Proposition 7.7. Then, using Lemma 7.11, $ZRM(r, m) = \phi(\mathcal{ZRM}(r, m))$ is a linear code.

$dim(ZRM(r, m)) = k$, where 2^k is the number of codewords of $\mathcal{ZRM}(r, m)$. By Proposition 7.10, the number of codewords of $\mathcal{ZRM}(r, m)$ is $4^{k_1}2^{k_2} = 2^{2k_1+k_2}$, where $k_1 = \sum_{i=0}^{r-1} \binom{m}{i}$ and $k_2 = \sum_{i=r}^{t} \binom{m}{i}$, $t = min\{2r-2, m\}$. Then, $dim(ZRM(r, m)) = 2\sum_{i=0}^{r-1} \binom{m}{i} + \sum_{i=r}^{t} \binom{m}{i} = \sum_{i=0}^{r-1} \binom{m}{i} + \sum_{i=0}^{t} \binom{m}{i}$. ∎

7.3 Rank and kernel of $ZRM^*(r,m)$ codes

First, we establish the type of the quaternary code $\mathcal{ZRM}^*(r,m)$.

Proposition 7.13. *$\mathcal{ZRM}^*(r,m)$ is a quaternary code of length 2^m and type $4^{k_1}2^{k_2}$, where $k_1 = \sum_{i=0}^{r-1}\binom{m}{i}$ and $k_2 = \binom{m}{r}$.*

Proof. By definition (7.2) of $\mathcal{ZRM}^*(r,m)$ and applying Lemma 3.1. □

By Proposition 7.1 for $r = 0, 1, 2, m, m+1$, $ZRM^*(r,m)$ is a linear code and, therefore, $rank(ZRM^*(r,m)) = dim(ker(ZRM^*(r,m)) = \sum_{i=0}^{r}\binom{m+1}{i}$. We will establish the value of the rank and the dimension of the kernel for the rest of the values of r.

Recall that $ZRM^*(r,m)$ is the image of $\mathcal{ZRM}^*(r,m)$ under a general Gray map, that is, a composition of the extended Gray map and a coordinate permutation. Note that if C is a binary code, then $rank(C) = rank(\pi(C))$ and $dim(ker(C)) = dim(ker(\pi(C)))$ for any coordinate permutation π. That way, in order to obtain the rank and the dimension of the kernel of $ZRM^*(r,m)$ codes, we can apply a specific coordinate permutation to the extended Gray map. In all this section, the Gray map ϕ will be the Gray map defined in 3.4.

Let $I \subseteq \{1, 2, \ldots, m\}$ be a set of indexes. We define the sets $I^+, I^\star \subseteq \{1, 2, \ldots, m+1\}$ as:

$$I^+ = \{i+1 \,|\, i \in I\},$$

$$I^\star = \{1\} \cup \{i+1 \,|\, i \in I\}.$$

Lemma 7.14. *Let $I, J \subseteq \{1, 2, \ldots, m\}$. Then,*

$$\phi(P_I(v_1, \ldots, v_m)P_J(v_1, \ldots, v_m)) = \phi(P_I(v_1, \ldots, v_m))\phi(P_J(v_1, \ldots, v_m)),$$

$$\phi(2P_I(v_1, \ldots, v_m)P_J(v_1, \ldots, v_m)) = \phi(2P_I(v_1, \ldots, v_m))\phi(2P_J(v_1, \ldots, v_m)).$$

Proof: Let consider x_j, y_j the j-th coordinate of $P_I(v_1, \ldots, v_m)$ and $P_J(v_1, \ldots, v_m)$ respectively. Assume $x_j = 0$; then, by one hand, $\phi(x_j y_j) = \phi(0) = (00)$ and

$\phi(x_j)\phi(y_j) = (00)\phi(2y_j) = (00)$ and, by other hand, $\phi(2x_jy_j) = \phi(0) = (00)$ and $\phi(2x_j)\phi(2y_j) = (00)\phi(y_j) = (00)$. Finally, if $x_j = y_j = 1$ then, in the first equation of the lemma, we obtain $\phi(x_jy_j) = (01)$ and $\phi(x_j)\phi(y_j) = (01)(01) = (01)$ and, in the second equation, $\phi(2x_jy_j) = (11)$ and $\phi(2x_j)\phi(2y_j) = (11)(11) = (11)$. ∎

Corollary 7.15. *Let $I \subseteq \{1, 2, \ldots, m\}$. Then, $\phi(P_I(v_1, \ldots, v_m)) = P_{I^\star}(v'_1, \ldots, v'_{m+1})$ and $\phi(2P_I(v_1, \ldots, v_m)) = P_{I^+}(v'_1, \ldots, v_{m+1'})$.*

Proof: By Lemma 5.18 and Lemma 7.14 and due to the fact that $v_i^2 = v_i$ for all $i = 1, \ldots, m$. ∎

Next theorems will give the values of the rank and the dimension of the kernel of $ZRM^*(r,m)$ codes for the other values of r.

Proposition 7.16. *Let r, m be integers such that $0 \leq r \leq m+1$.*

$$\left\langle ZRM^*(r,m) \right\rangle = ZRM(r,m)$$

Proof: It follows from definitions (5.5), (7.1) and (7.2). ∎

Theorem 7.17. *Let r, m be integers such that $3 \leq r \leq m-1$.*

$$rank(ZRM^*(r,m)) = \sum_{i=0}^{r-1} \binom{m}{i} + \sum_{i=0}^{t} \binom{m}{i},$$

where $t = min\{m, 2r-2\}$.

Proof: Due to Propositions 7.16 and 7.12. ∎

By Proposition 7.19, ϕ image of generator vectors of $\mathcal{ZRM}^*(r,m)$ are generator vectors of $RM(r, m+1)$. That way, $ker(ZRM^*(r,m)) \subseteq RM(r, m+1)$. Moreover, order 2 codewords in $ZRM^*(r,m)$ belongs to its kernel, and then, $\phi(2RM(r,m)) \subseteq ker(ZRM^*(r,m))$. Therefore, we obtain the following bounderies to the dimension of the kernel of $ZRM^*(r,m)$:

$$\sum_{i=0}^{r} \binom{m}{i} \leq dim(ker(ZRM^*(r,m))) \leq \sum_{i=0}^{r} \binom{m+1}{i}.$$

Theorem 7.18. *Let r, m be integers such that $3 \leq r \leq m-1$.*

$$dim(ker(ZRM^*(r,m))) = \sum_{i=0}^{r} \binom{m}{i} + m + 1.$$

Proof: As $\phi(2RM(r,m)) \subseteq ker(ZRM^*(r,m))$, we have to check which vectors of $\phi(RM(r-1,m))$ belong to the kernel of $ZRM^*(r,m)$.

Let $P_I(v_1,\ldots,v_m), P_J(v_1,\ldots,v_m) \in RM(r-1,m)$.
$\phi(P_I(v_1,\ldots,v_m)) +_b \phi(P_J(v_1,\ldots,v_m)) = P_{I^*}(v_1,\ldots,v_{m+1}) +_b P_{J^*}(v_1,\ldots,v_{m+1}) \in ZRM^*(r,m)$ if and only if $P_{(I^*\cup J^*)\setminus\{1\}}(v_1,\ldots,v_{m+1}) = P_{I^+\cup J^+}(v_1,\ldots,v_{m+1}) \in ZRM^*(r,m)$. That is, $\phi^{-1}(P_{I^+\cup J^+}(v_1,\ldots,v_{m+1})) = 2P_{I\cup J}(v_1,\ldots,v_m) \in \mathcal{ZRM}^*(r,m)$ or, equivalently, $P_{I\cup J}(v_1,\ldots,v_m) \in RM(r,m)$. So, $\phi(P_I(v_1,\ldots,v_m)) +_b \phi(P_J(v_1,\ldots,v_m)) \in ZRM^*(r,m)$ if and only if $|I\cup J| \leq r$. As $|J| \leq r-1$ and $3 \leq r \leq m-1$, $P_I(v_1,\ldots,v_m) \in ker(ZRM^*(r,m))$ if and only if $|I| \leq 1$.

Therefore, for $3 \leq r \leq m-1$,

$$ker(ZRM^*(r,m)) = \phi(2RM(r,m)) + \{P_I(v_1,\ldots,m) \,|\, |I| \leq 1\}$$

and $dim(ker(ZRM^*(r,m))) = \sum_{i=0}^{r} \binom{m}{i} + m + 1$. ∎

7.4 Relationship between $ZRM(r,m)$ and $RM(r,m)$ codes

Proposition 7.1 established that for $r = 0, 1, 2, m$ and $m+1$, $ZRM(r,m) = RM(r, m+1)$. Whereas both codes, $ZRM(r,m)$ and $RM(r,m)$, are linear codes, only $ZRM(r,m)$ is $\mathbb{Z}_4$-linear code for all values of $0 \leq r \leq m+1$, $m \geq 0$. In this section we will see that $ZRM(r,m)$, in fact, contains $RM(r,m+1)$.

Example 7.4.1. *Let $v_0 = \mathbf{1}, v_1, v_2, v_3, v_4$ generator vectors of $RM(1,4)$. Consider the set $\{P_I(v_1,\ldots,v_4) \,|\, |I| \leq 1\} \cup \{2P_I(v_1,\ldots,v_4) \,|\, |I| \leq 2\}$ that is, by definition, the set of generator vectors of $\mathcal{ZRM}(2,4)$. Such vectors are represented in Table 7.1*

whereas their ϕ image and its correspondence with vectors of length 2^5 $P_I(v'_1,\ldots,v'_5)$, by Corollary 7.15, are given in Table 7.2. It is easy to check that in this case $\{\phi(P_I(v_1,\ldots,v_4)) \,|\, |I| \leq 1\} \cup \{\phi(2P_I(v_1,\ldots,v_4)) \,|\, |I| \leq 2\}$ is exactly $\{P_I(v'_1,\ldots,v'_5) \,|\, |I| \leq 2\}$. That is, the generator vectors of $RM(2,5)$.

v_0	11 11	11 11	11 11	11 11
v_4	00 00	00 00	11 11	11 11
v_3	00 00	11 11	00 00	11 11
v_2	00 11	00 11	00 11	00 11
v_1	01 01	01 01	01 01	01 01
$2v_0$	22 22	22 22	22 22	22 22
$2v_4$	00 00	00 00	22 22	22 22
$2v_3$	00 00	22 22	00 00	22 22
$2v_2$	00 22	00 22	00 22	00 22
$2v_1$	02 02	02 02	02 02	02 02
$2v_3v_4$	00 00	00 00	00 00	22 22
$2v_2v_4$	00 00	00 00	00 22	00 22
$2v_1v_4$	00 00	00 00	02 02	02 02
$2v_2v_3$	00 00	00 22	00 00	00 22
$2v_1v_3$	00 00	02 02	00 00	02 02
$2v_1v_2$	00 02	00 02	00 02	00 02

Table 7.1: Generator vectors of $\mathcal{ZRM}(2,4)$

As we have seen in the last example, $r = 2$ and $m = 4$, the Gray map image of generator vectors of $\mathcal{ZRM}(r,m)$ codes are generator vector of $RM(r,m+1)$. This fact is not true in general; only in the cases that $RM(r,m+1)$ is a $\mathbb{Z}_4$-linear code, that is $r = 0,1,2,m$, do $RM(r,m+1)$ and $ZRM(r,m) = \phi(\mathcal{ZRM}(r,m))$ coincide. In the other cases, however, $RM(r,m+1) \subseteq ZRM(r,m)$. These statements will be proven in the following propositions.

Proposition 7.19. *Let r,m be integers such that $0 \leq r \leq m+1$.*

$$\{P_I(v'_1,\ldots,v'_{m+1}) \,|\, |I| \leq r\} =$$

$$\{\phi(P_I(v_1,\ldots,v_m)) \,|\, |I| \leq r-1\} \cup \{\phi(2P_I(v_1,\ldots,v_m)) \,|\, |I| \leq r\}.$$

Proof: Let be $P_I(v'_1, \ldots, v'_{m+1})$ where $I \subseteq \{1, \ldots, m+1\}$ and $|I| \leq r$.

If $1 \in I$, then let be $J = \{i - 1 \,|\, i \in I, i \neq 1\}$. By definition, $J^\star = I$ and, using Corollary 7.15 $\phi(P_J(v_1, \ldots, v_m)) = P_I(v'_1, \ldots, v'_{m+1})$ where $P_J(v_1, \ldots, v_m) \in RM(r-1, m)$.

If $1 \notin I$, then $J^+ = I$, where $J = \{i - 1 \,|\, i \in I\}$. By Corollary 7.15 $\phi(2P_J(v_1, \ldots, v_m)) = P_I(v'_1, \ldots, v'_{m+1})$ where $2P_J(v_1, \ldots, v_m) \in 2RM(r, m)$. ∎

From the last proposition, all the generators vectors of $RM(r, m+1)$ are in $ZRM(r, m)$. Hence, as both $RM(r, m+1)$ and $ZRM(r, m)$ are linear codes, we obtain the following inclusion.

Corollary 7.20. *Let r, m be integers such that $0 \leq r \leq m+1$. $RM(r, m+1) \subseteq ZRM(r, m)$ and the equality is given for $r = 0, 1, 2, m$.*

Proof: Propositions 7.1 and 7.19. ∎

Proposition 7.21. *Let r, m be integers such that $0 \leq r \leq m$. Then, $\mathcal{ZRM}(r, m-1)$ is the minimum quaternary code such that $\phi(\mathcal{ZRM}(r, m-1))$ contains $RM(r, m)$, where ϕ is the Gray map defined in (3.4).*

Proof: Let r, m be integers such that $0 \leq r \leq m$. Let ϕ be the Gray map defined in (3.4) and $ZRM(r, m) = \phi(\mathcal{ZRM}(r, m))$. If $r \leq 2$ or $r \geq m-1$, then $ZRM(r, m-1) = RM(r, m)$ and the statement is given.

Assume $3 \leq r \leq m-2$ and let $\mathcal{C}$ be the minimum quaternary code such that $\phi(\mathcal{C})$ contains $RM(r, m)$. As $ZRM(r, m-1)$ is a quaternary code and $RM(r, m) \subseteq ZRM(r, m-1)$ by Corollary 7.20, $\phi(\mathcal{C})$ is a subset of $ZRM(r, m-1)$. Now, the equality follows from the fact that $|\phi(\mathcal{C})| = |ZRM(r, m-1)|$ (see Theorem 5.30 and Proposition 7.12). ∎

In fact, if we consider the construction of $RM(r, m)$ of Corollary 5.2:

$$RM(r, m) = \phi(RM(r-1, m-1)) + \phi(2RM(r, m-1)) = \phi(RM(r-1, m-1) + 2RM(r, m-1)).$$

we obtain $\mathcal{C} = \phi^{-1}(RM) = RM(r-1,m-1) + 2RM(r,m-1)$. Therefore, the minimum quaternary code containing $\phi^{-1}(RM)$ is $\langle \mathcal{C} \rangle_4 = \langle RM(r-1,m-1) + 2RM(r,m-1) \rangle_4 = \mathcal{ZRM}(r-1,m)$ by definition of $\mathcal{ZRM}(r,m)$.

Moreover, note that $\mathcal{ZRM}(r,m)$ is the code $\mathcal{C}$ of Theorem 5.30. The dimension obtained in that theorem coincides, effectively, with the dimension of $\phi(\mathcal{ZRM}(r,m))$ of Proposition 7.12.

7.5 Relationship between $ZRM(r,m)$ and $\overline{QRM}(r,m)$ codes

In order to establish the relationship between $\mathcal{ZRM}^*(r,m)$ and $\overline{QRM}(r,m)$ codes, we will consider the definition (7.2) of $\mathcal{ZRM}^*(r,m)$ codes and definition (6.1) of $\mathcal{SRM}(r,m)$ codes; that is,

$$\mathcal{ZRM}^*(r,m) = \langle \{P_I(v_1,\ldots,v_m) \mid |I| \leq r-1\} \rangle_4 + \langle \{2P_I(v_1,\ldots,v_m) \mid |I| \leq r\} \rangle_4,$$
$$\mathcal{SRM}(r,m) = \langle \{P_I(v_1,\ldots,v_m) \mid |I| \leq r\} \rangle_4.$$

By definition of $\alpha()$, $\alpha(\langle \{2P_I(v_1,\ldots,v_m) \mid |I| \leq r\} \rangle_4) = 0$. Thus, $\alpha(ZRM^*(r,m))$ is equal to $\alpha(SRM(r-1,m))$. Moreover, as $\mathcal{SRM}(r,m)$ belongs to the class $\overline{\mathcal{QRM}}(r,m)$ we obtain $\alpha(\mathcal{ZRM}^*(r,m)) = RM(r-1,m)$. Even though, $\mathcal{ZRM}^*(r,m)$ does not belong to $\overline{\mathcal{QRM}}(r-1,m)$ class due to the fact that it is of type $4^{k_1}2^{k_2}$, where $k_1 = \sum_{i=0}^{r-1} \binom{m}{i}$ and $k_2 = \binom{m}{r}$. However, with the above definitions, it is easy to check that

$$\mathcal{SRM}(r-1,m) \subset \mathcal{ZRM}^*(r,m) \subset \mathcal{SRM}(r,m).$$

where $\mathcal{SRM}(r-1,m)$ and $\mathcal{SRM}(r,m)$ belong to the classes $\overline{\mathcal{QRM}}(r-1,m)$ and $\overline{\mathcal{QRM}}(r,m)$ respectively.

Similarly, if we consider the definition of $\mathcal{ZRM}(r,m)$ given in Corollary 7.8, we obtain

$$\mathcal{SRM}(r-1,m) \subset \mathcal{ZRM}(r,m) \subset \mathcal{SRM}(t,m),$$

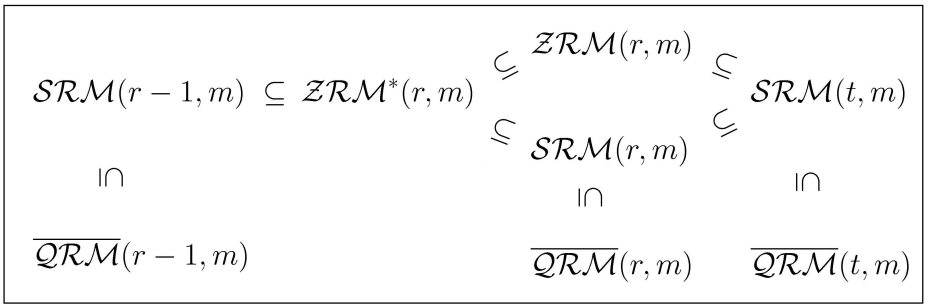

Figure 7.1: Relationship between $ZRM(r,m)$, $ZRM^*(r,m)$ and $\overline{\mathcal{QRM}}(r,m)$ codes

where $t = min\{2r-2, m\}$, and $\mathcal{SRM}(t,m) \subset \overline{\mathcal{QRM}}(t,m)$.

Finally, $\mathcal{SRM}(r-1,m) \subset \mathcal{ZRM}(r,m)$ and $rank(\mathcal{SRM}(r-1,m)) = rank(\mathcal{ZRM}^*(r,m)) = dim(ZRM(r,m))$ by Propositions 6.29, 7.12 and Corollary 7.16. Hence, if $SRM(r-1,m) = \phi(\mathcal{SRM}(r-1,m))$, then

$$\big\langle SRM(r-1,m) \big\rangle = \big\langle ZRM^*(r,m) \big\rangle = ZRM(r,m).$$

$\phi(v_0)$	01 01 01 01	01 01 01 01	01 01 01 01	01 01 01 01	v'_1
$\phi(v_4)$	00 00 00 00	00 00 00 00	01 01 01 01	01 01 01 01	$v'_1v'_5$
$\phi(v_3)$	00 00 00 00	01 01 01 01	00 00 00 00	01 01 01 01	$v'_1v'_4$
$\phi(v_2)$	00 00 01 01	00 00 01 01	00 00 01 01	00 00 01 01	$v'_1v'_3$
$\phi(v_1)$	00 01 00 01	00 01 00 01	00 01 00 01	00 01 00 01	$v'_1v'_2$
$\phi(2v_0)$	11 11 11 11	11 11 11 11	11 11 11 11	11 11 11 11	v'_0
$\phi(2v_4)$	00 00 00 00	00 00 00 00	11 11 11 11	11 11 11 11	v'_5
$\phi(2v_3)$	00 00 00 00	11 11 11 11	00 00 00 00	11 11 11 11	v'_4
$\phi(2v_2)$	00 00 11 11	00 00 11 11	00 00 11 11	00 00 11 11	v'_3
$\phi(2v_1)$	00 11 00 11	00 11 00 11	00 11 00 11	00 11 00 11	v'_2
$\phi(2v_3v_4)$	00 00 00 00	00 00 00 00	00 00 00 00	11 11 11 11	$v'_4v'_5$
$\phi(2v_2v_4)$	00 00 00 00	00 00 00 00	00 00 11 11	00 00 11 11	$v'_3v'_5$
$\phi(2v_1v_4)$	00 00 00 00	00 00 00 00	00 11 00 11	00 11 00 11	$v'_2v'_5$
$\phi(2v_2v_3)$	00 00 00 00	00 00 11 11	00 00 00 00	00 00 11 11	$v'_3v'_4$
$\phi(2v_1v_3)$	00 00 00 00	00 11 00 11	00 00 00 00	00 11 00 11	$v'_2v'_4$
$\phi(2v_1v_2)$	00 00 00 11	00 00 00 11	00 00 00 11	00 00 00 11	$v'_2v'_3$

Table 7.2: ϕ image of generator vectors of $\mathcal{ZRM}(2,4)$

Chapter 8

Conclusion

8.1 Results of the dissertation

8.1.1 Additive codes

Define the generalization of the Gray map as $\varphi : \mathbb{Z}_{2k} \longrightarrow \mathbb{Z}_2^k$ such that:

$$(i) \quad \varphi(i) = (\mathbf{0}^{(k-i)} \mid \mathbf{1}^{(i)}) \quad \forall i = 0, \ldots, k-1, and$$
$$(ii) \quad \varphi(i+k) = \phi(i) + \mathbf{1}^{(k)} \quad \forall i = 0, \ldots, k-1.$$

For any two elements $\varphi(i), \varphi(j) \in \varphi(\mathbb{Z}_{2k})$, define the product

$$\varphi(i) \cdot \varphi(j) = \varphi(i) + \sigma_i(\varphi(j)),$$

where

$$\sigma_i = (1, k, k-1, \ldots, 2)^i$$

(i.e. i left shifts), for all vector $\varphi(i)$, $i = 0, \ldots, 2k-1$.

Among all possible generalizations of the Gray map to $\mathbb{Z}_{2k}$, the one defined above is the only (up to coordinate permutation) that $(\varphi(Z_{2k}), \cdot)$ is a Hamming-compatible code.

Let us define the extended map $\phi : \mathbb{Z}_{2k}^n \longrightarrow \mathbb{Z}_2^{kn}$ such that $\phi(j_1, \ldots, j_n) = (\varphi(j_1), \ldots, \varphi(j_n))$, where φ is defined in (4.1). Finally, we define the permutations $\pi_x = (\sigma_{j_1} | \cdots | \sigma_{j_n})$, for $x = \phi(j_1, \ldots, j_n)$, where σ_i is defined above.

Result 8.1. *If $\mathcal{C}$ is a $\mathbb{Z}_{2k}$-code, then $\phi(\mathcal{C})$ is a propelinear code with associated permutation π_x for all codeword $x \in \phi(\mathcal{C})$. Moreover, if $k > 2$ and $\mathcal{C} \in \mathbb{Z}_{2k}^n$, then $\phi(\mathcal{C})$ is a propelinear but not translation-invariant code.*

Thus, the only codes being translation-invariant are linear codes and $\mathbb{Z}_4$-linear codes.

Result 8.2. *Let $\mathcal{C}$ and $\mathcal{C}^\perp$ be dual $\mathbb{Z}_{2k}$-codes, and $C = \phi(\mathcal{C})$ and $C_\perp = \phi(\mathcal{C}^\perp)$ be their binary images. Then, the weight enumerators $W_C(X,Y)$ and $W_{C_\perp}(X,Y)$ of C and $C_\perp$ respectively, are related by the binary MacWilliams identity*

$$W_{C_\perp}(X,Y) = \frac{1}{|C|} W_C(X+Y, X-Y)$$

if and only if $k = 1, 2$; that is, C is linear or $\mathbb{Z}_4$-linear.

A binary code C of length n is a mixed group code of type $(\mathbb{Z}_{2i_1}^{k_1}, \ldots, \mathbb{Z}_{2i_r}^{k_r})$ and length n if $C = \phi(\mathcal{C})$, where $i_1, \cdots, i_r$ are the minimum values such that $\mathcal{C}$ is a subgroup of $\mathbb{Z}_{2i_1}^{k_1} \times \cdots \times \mathbb{Z}_{2i_r}^{k_r}$ and $\sum_{j=1}^{r} i_j k_j = n$.

Result 8.3. *Let C be a mixed group code of type $(\mathbb{Z}_{2i_1}^{k_1}, \ldots, \mathbb{Z}_{2i_r}^{k_r})$ and length n. Then,*

(i) C is a propelinear code.

(ii) If C is 1-perfect, then C is of type $(\mathbb{Z}_2^k, \mathbb{Z}_4^{(n-k)/2})$ for some $k \in \mathbb{N}$.

Hence, the only 1-perfect binary mixed group codes of type $(\mathbb{Z}_{2i_1}^{k_1}, \ldots, \mathbb{Z}_{2i_r}^{k_r})$ are translation-invariant propelinear codes of type $(k, \frac{n-k}{2})$. In fact, any 1-perfect additive code is a translation-invariant propelinear code of type $(k, \frac{n-k}{2})$.

The different structures, the rank, and the dimension of the kernel of 1-perfect additive codes and extended 1-perfect additive codes are known. If C is a 1-perfect additive code, then the extended code $C^\star$ is an extended 1-perfect additive ($\mathbb{Z}_4$-linear or non $\mathbb{Z}_4$-linear) code. If $C^\star$ is the extended 1-perfect additive non $\mathbb{Z}_4$-linear code of C and we puncture a binary coordinate, then $(C^\star)'$ is isomorphic to C. This is not true if we puncture a quaternary coordinate. In fact, a punctured extended $\mathbb{Z}_4$-linear code is not, in general, a 1-perfect additive.

Result 8.4. *If $C^\star$ is a binary extended 1-perfect $\mathbb{Z}_4$-linear code of length $n+1 \geq 16$ then, the punctured code $(C^\star)'$ 1-perfect is not a 1-perfect additive code up to the case that $C^\star$ equals to the extended of the Hamming code of length 15.*

8.1.2 Reed-Muller codes

The main results obtained concerning Reed-Muller codes are those related with their $\mathbb{Z}_4$-linearity. Even though, we first present a new construction of $RM(r,m)$.

Result 8.5. *Let r, s, m be integers such that $0 \leq r, s \leq m$. Define*

$$C_{r+s} = \{xy \mid x \in RM(r,m), y \in RM(s,m)\}.$$

Then, $\langle C_{r+s} \rangle = RM(t,m)$, where $t = min\{r+s, m\}$.

It is known that $RM(r,m)$ codes are $\mathbb{Z}_4$-linear if and only if $r = 0, 1, 2, m-1$ and m. If C is a $\mathbb{Z}_4$-linear code, then there exists an extended Gray map, ϕ, and a coordinate permutation, π, such that $\pi \circ \phi(\mathcal{C}) = C$ for some quaternary code $\mathcal{C}$. Nevertheless, there may exist a nonisomorphic code $\mathcal{C}'$ and a coordinate permutation π' such that $\pi' \circ \phi(\mathcal{C}') = C$. Whenever a Reed-Muller code is $\mathbb{Z}_4$-linear, up to the case $r = 2$, the following results determine how many nonisomorphic $\mathbb{Z}_4$-codes $\mathcal{C}$ there are such that $\phi(\mathcal{C})$ is permutation-equivalent to $RM(r,m)$ and, in each case, the type of these $\mathbb{Z}_4$-codes.

In this section, let ϕ be the extended Gray map defined as

$$\phi(c) = (\beta(c_1), \ldots, \beta(c_n), \gamma(c_1), \ldots, \gamma(c_n)), \tag{8.1}$$

where $c = (c_1, \ldots, c_n)$ and the image of the usual Gray map of c_i is $(\beta(c_i), \gamma(c_i))$.

Result 8.6. *For $r = 0, m-1$ and m, there exists a unique $\mathbb{Z}_4$-code $\mathcal{C}$ up to isomorphism such that $\phi(\mathcal{C})$ is permutation-equivalent to $RM(r,m)$. Moreover, $\phi^{-1}(RM(r,m))$ is of type $4^0 2^1$, $4^{2^{m-1}-1}2^1$ and $4^{2^{m-1}}$, for $r = 0, m-1$ and m respectively.*

Result 8.7. *Let $m \geq 3$. Let the matrix G_1 be the all columns vectors of the form $2\mathbb{Z}_2^{m-1} \times \{\mathbf{1} \in \mathbb{Z}_4\}$ and the matrix G_2, the all columns vectors of the form $2\mathbb{Z}_2^{m-3} \times \{\mathbf{1} \in \mathbb{Z}_4\} \times \mathbb{Z}_4$. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the $\mathbb{Z}_4$-code generated by G_1 and G_2 respectively. Then, $\phi(\mathcal{C}_1) = RM(1,m)$ and there exist $\pi \in \mathcal{S}_{2^m}$ such that $\pi \circ \phi(\mathcal{C}_2) = RM(1,m)$.*

So, for $r = 0, m-1$ and m, there is a unique quaternary code up to isomorphism such that its image under ϕ is permutation-equivalent to $RM(r,m)$ whereas for $r = 1$ there are two non-isomorphic codes.

Now, we consider $RM(r,m)$ for $3 \leq r \leq m-2$; that is, when the code is not $\mathbb{Z}_4$-linear.

Result 8.8. *Let $\mathcal{C}$ be the minimum quaternary code such that $RM(r,m) \subseteq \phi(\mathcal{C})$. Then, for $3 \leq r \leq m-2$, $C = \phi(\mathcal{C}) = \{RM(r,m) \cup (\bigcup_{r<|I|\leq t, 1 \notin I} P_I(v_1, \ldots, v_m))\}$, and $|C| = 2^k$, where*

$$k = \sum_{i=0}^{r-1} \binom{m-1}{i} + \sum_{i=0}^{t} \binom{m-1}{i},$$

for $t = min\{m-1, 2r-2\}$.

Note that last theorem gives the minimum quaternary code such that $\phi(\mathcal{C})$ contains $RM(r,m)$, where ϕ is the Gray map defined in (8.1). If C is the minimum $\mathbb{Z}_4$-linear code that contains $RM(r,m)$, then C is linear and $\phi^{-1} \circ \pi(C)$ is a quaternary code for some permutation coordinates $\pi \in \mathcal{S}_{2^m}$. Therefore, we obtain an upper bound to the dimension of such code C.

Result 8.9. *Let C be the minimum $\mathbb{Z}_4$-linear code containing $RM(r,m)$. Then,*

$$dim(C) \leq \sum_{i=0}^{r-1} \binom{m-1}{i} + \sum_{i=0}^{t} \binom{m-1}{i},$$

where $t = min\{m-1, 2r-2\}$.

8.1.3 QRM codes

Results of Chapter 6 are published in [BFP05].

Let r, m be integers such that $0 \leq r \leq m$. Let $\mathcal{QRM}(r, m)$ be a quaternary Reed-Muller code of length 2^m. Remember the basic properties of $\mathcal{QRM}(r, m)$.

(i) $\mathcal{QRM}(r, m)$ is of type 4^k, where $k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$.

(ii) $\mathcal{QRM}(r, m) \subset \mathcal{QRM}(r + 1, m)$, $\forall r < m$.

(iii) $\mathcal{QRM}(r, m)^{\perp} = \mathcal{QRM}(m - r - 1, m)$, $\forall r < m$.

(iv) $\alpha(\mathcal{QRM}(r, m)) = RM(r, m)$.

(v) For m odd, $m \geq 3$, $\phi(\mathcal{QRM}(1, m))$ is the Kerdock code K_{m+1} of 2^{m+1}.

(vi) For m odd, $m \geq 3$, $\phi(\mathcal{QRM}(m-2, m))$ is a Preparata-like code of length 2^{m+1}.

We have generalized $\mathcal{QRM}(r, m)$ codes to the class $\overline{\mathcal{QRM}}(r, m)$. The definition of this class is the following.

Definition 8.1.1. *Let r, m be integers such that $0 \leq r \leq m$. Let us define $\overline{\mathcal{QRM}}(r, m)$ a class of quaternary Reed-Muller codes where $\mathcal{C} \in \overline{\mathcal{QRM}}(r, m)$ if and only if:*

(i) The quaternary length of the code $\mathcal{C}$ is 2^m.

(ii) $\mathcal{C}$ is of type 4^k, where
$k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$.

(iii) $\alpha(\mathcal{C}) = RM(r, m)$.

Define the related binary class

$$\overline{QRM}(r, m) = \{C = \phi(\mathcal{C}) \mid \mathcal{C} \in \overline{\mathcal{QRM}}(r, m)\}.$$

Codes $\mathcal{QRM}(r, m)$ belong to $\overline{\mathcal{QRM}}(r, m)$. However, in order to obtain different codes in such class, we present two constructions of codes in $\overline{\mathcal{QRM}}(r, m)$. The first one is a generalized doubling construction. The second, is a contruction in terms of generator matrices.

Result 8.10. *Let $\mathcal{C} \in \overline{\mathcal{QRM}}(r+1,m)$ and $\mathcal{D} \in \overline{\mathcal{QRM}}(r,m)$. Then, the code $\mathcal{C}^*$ defined as $\{(u, u+v) \mid u \in \mathcal{C}, v \in \mathcal{D}\}$ belongs to the class $\overline{\mathcal{QRM}}(r+1,m+1)$.*

Result 8.11. *Let $\mathcal{C}$ be a quaternary code of length 2^m. $\mathcal{C}$ belongs to the class $\overline{\mathcal{QRM}}(r,m)$ if and only if there exist a binary $(\sum_{i=0}^{r}\binom{m}{i} \times 2^m)$ matrix, N, such that the generator matrix of $\mathcal{C}$ is*

$$G = G(r,m) + 2N,$$

where $G(r,m)$ is the generator matrix of $RM(r,m)$ defined in (5.7).

Define the set of matrices that are generator matrices of codes in $\overline{\mathcal{QRM}}(r,m)$:

$$GQ(r,m) = \{G(r,m) + 2N | N \text{ is a binary } (\sum_{i=0}^{r}\binom{m}{i} \times 2^m) \text{ matrix } \}.$$

Result 8.12. *Let $M_1, M_2 \in GQ(r+1,m)$ and $M_4 \in GQ(r,m)$. The matrix*

$$M = \begin{pmatrix} M_1 & M_2 \\ 2N_3 & M_4 \end{pmatrix}, \tag{8.2}$$

where N_3 is a binary $(\sum_{i=0}^{r}\binom{m}{i} \times 2^m)$ matrix, belongs to $GQ(r+1,m+1)$

We would like that codes in $\overline{\mathcal{QRM}}(r,m)$ satisfy similar properties that the ones of $\mathcal{QRM}(r,m)$ given at the beginning of the subsection. Properties of codes in $\overline{\mathcal{QRM}}(r,m)$ are presented in the subsequent results.

Result 8.13. *Let $\mathcal{C} \in \overline{\mathcal{QRM}}(r,m)$, with $1 \leq r \leq m$.*

(i) $\mathcal{C}^{\perp} \in \overline{\mathcal{QRM}}(m-r-1,m)$.

(ii) There exist $\mathcal{D} \in \overline{\mathcal{QRM}}(r-1,m)$ such that $\mathcal{D} \subset \mathcal{C}$.

Result 8.14. *Let P_{2m} be a $\mathbb{Z}_4$-linear Preparata-like code and K_{2m} a $\mathbb{Z}_4$-linear Kerdock-like code of length $n+1 = 2^{2m}$. $P_{2m} \in \overline{QRM}(2m-3, 2m-1)$ and $K_{2m} \in \overline{QRM}(1, 2m-1)$.*

Recall that the image under the Gray map of codes in $\overline{\mathcal{QRM}}(r,m)$ are not linear codes. That way, we calculate the rank and the dimension of the kernel of such codes.

Result 8.15. *Let $\mathcal{C} \in \overline{\mathcal{QRM}}(r,m)$ and $C = \phi(\mathcal{C})$. Then,*

(i) $dim(ker(C)) = \sum_{i=0}^{r} \binom{m}{i} + 1$, if $r < m$ and $dim(ker(C)) = 2^{m+1}$, for $r = m$.

(ii) $rank(C) = \sum_{i=0}^{r} \binom{m}{i} + \sum_{i=0}^{t} \binom{m}{i}$, where $t = min\{2r, m\}$.

For a fixed value of m, codes $RM(r,m)$ conforms a chain of codes:

$$RM(0,m) \subset RM(1,m) \subset \cdots \subset RM(m-1,m) \subset RM(m,m).$$

Due to property (ii) in Result 8.13, we can construct a chain of codes in $\overline{\mathcal{QRM}}(r,m)$. Unlike the case of Reed-Muller codes, this chain is not unique. Given a code $\mathcal{C} \in \overline{\mathcal{QRM}}(r,m)$, there may exist $\mathcal{D}_1, \mathcal{D}_2 \in \overline{\mathcal{QRM}}(r-1,m)$, such that $\mathcal{D}_1 \neq \mathcal{D}_2$ and $\mathcal{D}_1, \mathcal{D}_2 \subset \mathcal{C}$. Moreover, we also can construct a chain of $\overline{\mathcal{QRM}}$ codes in terms of their generator matrices as follows.

Let $\mathcal{C} \subset \overline{\mathcal{QRM}}(r,m)$, and $M = G(r,m) + 2N \in GQ(r,m)$ its generator matrix, for some binary $(\sum_{i=0}^{r} \binom{m}{i} \times 2m)$ matrix, N. If $r \geq 1$, consider the matrix N_{-1} conformed by the first $\sum_{i=0}^{r-1} \binom{m}{i}$ row vectors of N, and, if $r < m$, N_{+1} is a binary $(\binom{m}{r+1} \times 2m)$ matrix. Hence,

$$M_{-1} = G(r-1,m) + 2N_{-1} \in GQ(r-1,m),$$

and

$$M_{+1} = G(r+1,m) + \begin{pmatrix} N \\ N_{+1} \end{pmatrix} \in GQ(r+1,m).$$

Let $\mathcal{C}_{-1} \in \overline{\mathcal{QRM}}(r-1,m)$ and $\mathcal{C}_{+1} \in \overline{\mathcal{QRM}}(r+1,m)$ be the codes generated by M_{-1} and M_{+1} respectively. Then,

$$\mathcal{C}_{-1} \subset \mathcal{C} \subset \mathcal{C}_{+1}.$$

Again, with this construction, code $\mathcal{C}_{+1}$ may not be unique, it depends on the choice of the matrix N_{+1}. We have obtained some results about the chain of codes in $\overline{\mathcal{QRM}}(r,m)$. First, recall some notation.

Let $(\mathcal{C}_0,\mathcal{C}_1,\ldots,\mathcal{C}_{m-1})$ be a chain of codes, $(\mathcal{C}_0,\mathcal{C}_1,\ldots,\mathcal{C}_{m-1})^\perp = (\mathcal{C}_{m-1}^\perp,\mathcal{C}_{m-2}^\perp,\ldots,\mathcal{C}_0^\perp)$ its dual chain, and $d(\mathcal{C}_0,\mathcal{C}_1,\ldots,\mathcal{C}_{m-1}) = (d_0,d_1,\ldots,d_{m-1})$ the minimum distance of the chain where d_i is the minimum distance of $\mathcal{C}_i$. Define the set of chains where all the codes belong to the class $\overline{\mathcal{QRM}}$:

$$\bar{\Gamma} = \{(\mathcal{C}_0,\mathcal{C}_1,\ldots,\mathcal{C}_{m-1}) \mid \mathcal{C}_r \in \overline{\mathcal{QRM}}(r,m), r = 0,\ldots,m-1\}.$$

Result 8.16. *If* $(\mathcal{C}_0,\mathcal{C}_1,\ldots,\mathcal{C}_{m-1}) \in \bar{\Gamma}$ *then,* $(\mathcal{C}_0,\mathcal{C}_1,\ldots,\mathcal{C}_{m-1})^\perp \in \bar{\Gamma}$.

Result 8.17. *Let* $(\mathcal{C}_0,\mathcal{C}_1,\ldots,\mathcal{C}_{m-1}) \in \bar{\Gamma}$, $d\big((\mathcal{C}_0,\mathcal{C}_1,\ldots,\mathcal{C}_{m-1})\big) = (d_0,d_1,\ldots,d_{m-1})$. *Then,*

(i) $2^{m-r} \leq d_r \leq 2^{m-r+1}$, $0 \leq r \leq m$,

(ii) if $m \geq 3$ *odd,* $d_1 \leq 2^m - 2^{(m-1)/2}$,

(iii) if $m \geq 3$ *odd,* $d_{m-2} \leq 6$.

8.1.4 ZRM codes

First, remember the two different definition of codes $\mathcal{ZRM}$ that can be found in the literature.

$$\mathcal{ZRM}(r,m) = \big\langle RM(r-1,m), 2RM(r,m)\big\rangle_4.$$

$$\mathcal{ZRM}^*(r,m) = \big\langle\{P_I(v_1,\ldots,v_m) \mid |I| \leq r-1\}\big\rangle_4 + \big\langle\{2P_I(v_1,\ldots,v_m) \mid |I| \leq r\}\big\rangle_4.$$

Note that we $\mathcal{ZRM}^*(r,m)$ is defined in terms of its generator vectors but not $ZRM(r,m)$. That way, in order to compare both codes, we establish the generator vectors of $\mathcal{ZRM}(r,m)$.

Result 8.18. *Let r, m be integers such that $2 \leq r \leq m+1$. Then,*

$$\mathcal{ZRM}(r,m) = \left\langle \{P_I(v_1,\ldots,v_m) \,|\, |I| \leq r-1\} \right\rangle_4 + \left\langle \{2P_I(v_1,\ldots,v_m) \,|\, r \leq |I| \leq t\} \right\rangle_4,$$

where $t = min\{2r-2, m\}$. Moreover,

$$\mathcal{ZRM}(0,m) = \left\langle \{\mathbf{2}\} \right\rangle_4,$$

$$\mathcal{ZRM}(1,m) = \left\langle \{\mathbf{1}\} \right\rangle_4 + \left\langle \{2P_I(v_1,\ldots,v_m) \,|\, |I| \leq 1\} \right\rangle_4.$$

Now, from the last result and the definition of $\mathcal{ZRM}^*(r,m)$ the next result follows:

Result 8.19. *$\mathcal{ZRM}(r,m) = \mathcal{ZRM}^*(r,m)$ if and only if $r = 0, 1, 2, m$ and $m+1$.*

Let ϕ be the extended Gray map defined in (8.1), let $ZRM(r,m) = \phi(\mathcal{ZRM}(r,m))$ and $ZRM^*(r,m) = \phi(\mathcal{ZRM}^*(r,m))$. When both codes $\mathcal{ZRM}(r,m)$ and $\mathcal{ZRM}^*(r,m)$ coincide, their binary image under ϕ is the Reed-Muller code $RM(r,m+1)$. As these codes differ for the other values of r, we studied their structure and their binary image separately. First, we established the type of $\mathcal{ZRM}(r,m)$.

Result 8.20. *$\mathcal{ZRM}(r,m)$ is a quaternary code of length 2^m and type $4^{k_1}2^{k_2}$, where $k_1 = \sum_{i=0}^{r-1} \binom{m}{i}$ and $k_2 = \sum_{i=r}^{t} \binom{m}{i}$, $t = min\{2r-2, m\}$.*

Binary image under ϕ map of such codes turned out to be linear codes for any values of r and m.

Result 8.21. *$ZRM(r,m)$ are linear codes and*

$$dim(ZRM(r,m)) = \sum_{i=0}^{r-1} \binom{m}{i} + \sum_{i=0}^{t} \binom{m}{i},$$

where $t = min\{2r-2, m\}$.

Result 8.22. *Let r, m be integers such that $0 \leq r \leq m$. Then, $\mathcal{ZRM}(r,m-1)$ is the minimum quaternary code such that $\phi(\mathcal{ZRM}(r,m-1))$ contains $RM(r,m)$, where ϕ is the Gray map defined in (8.1).*

As it was said in the introduction of this dissertation, we would like to prove that the minimum $\mathbb{Z}_4$-linear code containing a Reed-Muller code was a ZRM code. This result has not been achieved, but we have found that the dimension of the minimum $\mathbb{Z}_4$-linear code is less or equal to the dimension of the corresponding ZRM code. Note that the dimension of $\phi(\mathcal{ZRM}(r, m-1))$ in Result 8.21 coincides with the upper bound of the dimension of the minimum $\mathbb{Z}_4$-linear code containing $RM(r, m)$ in Result 8.9.

$\mathcal{ZRM}^*(r, m)$ are not linear codes. We found that the spanned code of $ZRM^*(r, m)$ codes coincide with $ZRM(r, m)$ codes and we calculated the type, the rank and the dimension of the kernel of such codes.

Result 8.23. *Let r, m be integers such that $0 \leq r \leq m+1$.*

$$\left\langle ZRM^*(r, m) \right\rangle = \mathcal{ZRM}(r, m)$$

Result 8.24. *$\mathcal{ZRM}^*(r, m)$ is a quaternary code of length 2^m and type $4^{k_1}2^{k_2}$, where $k_1 = \sum_{i=0}^{r-1} \binom{m}{i}$ and $k_2 = \binom{m}{r}$.*

Result 8.25. *Let r, m be integers such that $3 \leq r \leq m-1$.*

(i) $dim(ker(ZRM^*(r, m))) = \sum_{i=0}^{r} \binom{m}{i} + m + 1.$

(ii) $rank(ZRM^*(r, m)) = \sum_{i=0}^{r-1} \binom{m}{i} + \sum_{i=0}^{t} \binom{m}{i}$, *where* $t = min\{m, 2r-2\}$.

Finally, we establish the relationship between $\mathcal{ZRM}(r, m)$, $\mathcal{ZRM}^*(r, m)$ and the class of quaternary codes $\overline{\mathcal{QRM}}(r, m)$.

Recall the definition of codes $\mathcal{SRM}(r, m) \in \overline{\mathcal{QRM}}(r, m)$

$$\mathcal{SRM}(r, m) = \left\langle \{P_I(v_1, \ldots, v_m) \,|\, |I| \leq r\} \right\rangle_4,$$

and let $SRM(r, m) = \phi(\mathcal{SRM}(r, m))$.

Neither $\mathcal{ZRM}(r, m)$ nor $\mathcal{ZRM}^*(r, m)$ belong to the class $\mathcal{QRM}(r, m)$ because they are not quaternary codes of type 4^k, where $k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$ (Results 8.20, 8.24).

However, we obtain the following inclusions:

$$\mathcal{SRM}(r-1,m) \subset \mathcal{ZRM}^*(r,m) \subset \mathcal{SRM}(r,m),$$

and

$$\mathcal{SRM}(r-1,m) \subset \mathcal{ZRM}(r,m) \subset \mathcal{SRM}(t,m),$$

where $t = min\{2r-2, m\}$.

Finally, $\mathcal{SRM}(r-1,m) \subset \mathcal{ZRM}(r,m)$ and $rank(\mathcal{SRM}(r-1,m)) = dim(ZRM(r,m)) = rank(ZRM^*(r,m))$. Hence,

$$\langle SRM(r-1,m)\rangle = \langle ZRM^*(r,m)\rangle = ZRM(r,m).$$

8.2 Future research

In this section, we point out some still open problems that derive from the dissertation. The first block of open questions is about the relationship between Reed-Muller codes and quaternary codes.

- We have determined how many nonisomorphic $\mathbb{Z}_4$-codes $\mathcal{C}$ there are such that $\phi(\mathcal{C})$ is permutation-equivalent to $RM(r,m)$ when $r = 0, 1, m-1, m$, and the type of such codes is given. There is still remaining the case $r = 2$ in order to determine the number and the type of nonisomorphic quaternary code $\mathcal{C}$ such that $\phi(\mathcal{C})$ is permutation-equivalent to $RM(r,m)$ whenever it is $\mathbb{Z}_4$-linear.

- Among all the unsolved problems, the one we thought is the most important is to find the minimum quaternary code containing $RM(r,m)$. Even though we supposed that $\mathcal{ZRM}(r,m)$ is such minimum quaternary code, we only have proved that it is the minimum under a specific extended Gray map but not in general.

- If the minimum quaternary code of last point is found, it would be interesting to determine, as in the case of $\mathbb{Z}_4$-linear Reed-Muller codes, the number and the

types of nonisomorphic $\mathbb{Z}_4$-codes such that their image, under a general Gray map, have the same dimension as the minimum quaternary code containing $RM(r, m)$.

We have seen that, given a code $\mathcal{C} \in \overline{\mathcal{QRM}}(r, m)$, we can construct different chains of codes in $\overline{\mathcal{QRM}}(r, m)$ containing $\mathcal{C}$. However, there are many open questions related to the chains of codes in $\overline{\mathcal{QRM}}(r, m)$.

- The chain $\Gamma_{\mathcal{QRM}}$ is a self-dual chain, whereas $\Gamma_{\mathcal{SRM}}$ is not. We would like to determine if for any code $\mathcal{C} \in \overline{\mathcal{QRM}}(r, m)$ there exist a self-dual chain of codes containing $\mathcal{C}$. And, otherwise, which are the properties of a code to be included in a self-dual chain.

- If $(C_0, \ldots, C_{m-1}) \in \bar{\Gamma}$, and $d(C_0, \ldots, C_m) = (d_0, \ldots, d_{m-1})$, we know that d_1 and d_{m-2} are the maximum possible minimum distance when C_1 is a quaternary Kerdock-like code and C_{m-2} is a quaternary Preparata-like code. Note that for m odd, $m \geq 3$, $\Gamma_{\mathcal{QRM}}$ contains both, a quaternary Kerdock-like and Preparata-like code.

  We would like to determine if the minimum distance of codes in $\Gamma_{\mathcal{QRM}}$ is the maximum value for any minimum distance of a code in $\overline{\mathcal{QRM}}$ with the same parameters of r and m. If not, it would be nice to determine if it is possible to construct a chain where all codes have the minimum distance as high as possible.

From Reed-Muller codes, we obtain several constructions of quaternary codes related to them (via the Gray map or the modulo 2 map). Nevertheless, there are other constructions of additive codes related to Reed-Muller codes; they are called Additive Reed-Muller codes, $ARM_{\alpha,\beta}(r, m)$ (see [PR97a]). Such a construction provides codes that are subgroups of $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$; that is, additive codes of type (α, β). Moreover, $ARM_{\alpha,0}(r, m) = RM(r, m)$ and $ARM_{0,\beta}(r, m) = \mathcal{ZRM}(r, m)$. In order to extend some results of this dissertation, it would be interesting to calculate the rank and the

kernel of $ARM_{\alpha,\beta}(r, m)$ codes or determine the linearity of the image under ϕ of such codes.

Bibliography

[AGOS99] T. Aoki, P. Gaborit, M. Harada M. Ozeki, and P. Sole. On the covering radius of $\mathbb{Z}_4$-codes and their lattices. *IEEE Transactions on Information Theory 45, 2162-2168*, 1999.

[AHS03] S.V. Avgustinovich, O. Heden, and F.I. Solov'eva. On ranks and kernels of perfect codes. *Probl. Inform. Transmission 39 (4), pp. 341-345*, 2003.

[AJK92] E.F. Assmus Jr and J.D. Key. *Designs and their codes*. Cambridge University Press, 1992.

[AJMJ67] E.F. Assmus Jr. and H.F. Mattson Jr. On tactical configurations and error-correcting codes. *Journal of Combinatorial Theory, vol. 2, pp. 243-257*, 1967.

[AS97] S.V. Avgustinovich and F.I. Solov'eva. Construction of perfect binary codes by sequential translations of α-components. *Probl. Inform. Transmission 33 (3), pp. 202-207*, 1997.

[BCN89] A.E. Brouwer, A.M. Cohen, and A. Neumaier. *Distance-Regular Graphs*. Springer-Verlag, 1989.

[BDHO99] E. Bannai, S.T. Dougherty, M. Harada, and M. Oura. Type II codes, even unimodular lattices, and invariant rings. *IEEE Transactions on Information Theory 45, pp. 1194-1205*, 1999.

[BE48] N.G. Bruijn and P. Erdõs. On a combinatorial problem. *Indagationes Mathematicae 10, pp.421-423*, 1948.

[BF02] J. Borges and C. Fernández. Punctured extended 1-perfect $\mathbb{Z}_4$-linear codes. Technical Report PIRDI-3/02, ETSE, UAB., November 2002.

[BFP05] J Borges, C. Fernández, and K.P. Phelps. Quaternary reed-muller codes. *To appear in IEEE Transactions on Information Theory 51, n.7*, 2005.

[BFR01] J. Borges, C. Fernández, and J Rifà. Every $\mathbb{Z}_{2k}$-code is a binary propelinear code. In *COMB'01*, volume 10, Electronic Notes in Discrete Mathematics, Elsevier Science., 2001.

[BGH83] H. Bauer, B Ganter, and F.B. Hergert. Algebraic techniques for nonlinear codes. *Combinatorica 3, pp. 21-33*, 1983.

[BI84] E. Bannai and T. Ito. *Algebraic Combinatorics I: Association Scheme*. The Benjamin/Cummings Publishing Company, Inc, 1984.

[Bor98] J. Borges. *Codis perfectes, particions i generalitzacions*. PhD thesis, Univ. Autònoma de Barcelona, 1998.

[BPR03] J. Borges, K.P. Phelps, and J. Rifà. The rank and the kernel of 1-perfect additive codes and extended 1-perfect $\mathbb{Z}_4$-linear codes. *IEEE Transactions on Information Theory 49, n.8, pp 2028-2034*, 2003.

[BPRZ03] J Borges, K. T. Phelps, J. Rifà, and V. Zinov'ev. On $\mathbb{Z}_4$-linear preparata-like and kerdock-like codes. *IEEE Transactions on Information Theory 49, n.11, pp. 2834-2843*, 2003.

[BR99] J. Borges and J. Rifà. A characterization of 1-perfect additive codes. *IEEE Transactions on Information Theory 45, pp. 1688-1697*, 1999.

[BS94] A. Bonnecaze and P. Sole. Quaternary constructions of formally self-dual codes. *Springer Lecture Notes in Comp. Sc. 781 pp. 194-206*, 1994.

[BSBM97] A. Bonnecaze, P. Sole, C. Bachoc, and B. Mourrain. Type II codes over $\mathbb{Z}_4$. *IEEE Transactions on Information Theory 43, 969-976*, 1997.

[BSC95] A. Bonnecaze, P. Sole, and A.R. Calderbank. Quaternary quadratic residue codes and unimodular lattices. *IEEE Transactions on Information Theory 41, pp. 366-377*, 1995.

[BVLW83] R.D. Baker, J.H. Van Lint, and R.M. Wilson. On the preparata and goethals codes. *IEEE Transactions on Information Theory 29, pp. 342-345*, 1983.

[Car97] C. Carlet. $\mathbb{Z}_{2^k}$-linear codes. *IEEE Transactions on Information Theory 44, pp. 1543-1547*, 1997.

[CCS97] A.R. Calderbank, P. Cameron, and J.J.. Seidel. $\mathbb{Z}_4$-kerdock codes, orthogonal spreads and extremal euclidean line-sets. *Proc. London Math. Soc (3) 75 pp. 1-720*, 1997.

[CMKH96] A.R. Calderbank, G. McGuire, V. Kumar, and T. Helleseth. Cyclic codes over $\mathbb{Z}_4$, locator polynomials, and Newton's identities. *IEEE Transactions on Information Theory 42, pp. 217-226*, 1996.

[CS95] A.R. Calderbank and N.J.A. Sloane. Modular and p-adic cyclic codes. *Designs, Codes and Cryptography 6, pp. 21-35*, 1995.

[DD02] I.J. Dejter and A.A. Delgado. STS-graphs of perfect codes mod kernel. In *Caribbean Workshop on Hypercube an its relatives*, 2002.

[Dej94] I. J. Dejter. STS-graphical invariant for perfect codes. *J. Combinat. Math. Combinat. Comput. 36, pp. 754-763*, 1994.

[DG75] P Delsarte and J.M. Goethals. Unrestricted codes with the Golay parameters are unique. *Discrete Math. 12, pp. 211-224*, 1975.

[DL98] P. Delsarte and V.I. Levenshtein. Association schemes and coding theory. *IEEE Transactions on Information Theory, 44, 2477-2504*, 1998.

[EV94] T. Etzion and A. Vardy. Perfect binary codes: Constructions, properties and enumeration. *IEEE Transactions on Information Theory 40, pp. 754-763*, 1994.

[EV98] T. Etzion and A. Vardy. On perfect codes and tilings: Problems and solutions. *SIAM J. Discrete Math. 11, Num 2, pp. 205-223*, 1998.

[GvT75] J.M. Goethals and H.C.A. van Tilborg. Uniformly packed codes. *Philips Research 30, pp 9-35*, 1975.

[HKC$^+$94] A Hammons, P.V. Kumar, A.R. Calderbank, N.J.A Sloane, and P. Sole. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes. *IEEE Transactions on Information Theory 40, pp. 301-319*, 1994.

[HLK98] X.-D. Hou, J. T. Lathtonen, and S. Koponen. The reed-muller code $R(r, m)$ is not $\mathbb{Z}_4$-linear for $3 \leq r \leq m-2$. *IEEE Transactions on Information Theory 44, pp. 798-799*, 1998.

[HSG99] M. Harada, P. Sole, and P. Gaborit. Self-dual codes over $\mathbb{Z}_4$ and unimodular lattices: a survey. In *ICAC, International Congress in Algebras and Combinatorics*, volume published by Springer-Verlag, pp.255-275, 1999.

[Kan83] William H. Kantor. On the inequivalence of generalized preparata codes. *IEEE Transactions on Information Theory 29, pp. 345-348*, 1983.

[Ker72] A.M. Kerdock. A class of low-rate nonlinear codes. *Information and Control 20, pp. 182-187*, 1972.

[Kro01] D.S. Krotov. $\mathbb{Z}_4$-linear Hadamard and extended perfect codes. In *International Workshop on Coding and Cryptography*, volume Paris (France) pp. 329-334, Jan. 8-12, 2001.

[KS02] Z. Kobayashi and T. Sekiguchi. On a characterization of the standard Gray code by using its edge type on a hypercube. *Information Processing Letters 81, pp. 231-237*, 2002.

[LeV95] J.M. LeVan. *Designs and codes*. PhD thesis, Auburn University, 1995.

[Mar01] E. Martínez. *Estructura de métricas no-Hamming*. PhD thesis, Universidad de Valladolid, April 2001.

[Mol86] M Mollard. A generalized parity function and its use in the construction of perfect codes. *SIAM J. Algebraic Discrete Methods 7, pp. 113-115*, 1986.

[MPR83] R.A. Mathon, K. Phelps, and A. Rosa. Small triple systems and their properties. *Ars Combin. 15, pp. 3-110*, 1983.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Publishing Company, Amsterdam, 1977.

[Mul54] D.E. Muller. Application of boolean algebra to switching circuit design and error detection. *IEEE Transaction on Computers 3, pp. 6-12*, 1954.

[PHB98] V. S. Pless, W. C. Huffman, and R. A. Brualdi. *Handbook of Coding Theory : Volume I*. North-Holland, 1998.

[Phe83] K. T. Phelps. A combinatorial construction of perfect codes. *SIAM J. Algebraic Discrete Methods 4, pp. 398-403*, 1983.

[PL95] K. T. Phelps and M. LeVan. Kernels of nonlinear Hamming codes. *Designs, Codes and Cryptography 6, pp. 247-257*, 1995.

[Ple68] V. Pless. On the uniqueness of the Golay codes. *J. Combin. Theory 5, pp. 215-228*, 1968.

[PR97a] J. Pujol and J. Rifà. Additive reed-muller codes. In *IEEE International Symposium on Information Theory*, 1997.

[PR97b] J. Pujol and J. Rifà. Translation-invariant propelinear codes. *IEEE Transactions on Information Theory 43, n. 2, pp. 590-598*, 1997.

[PR02] K. T. Phelps and J. Rifà. On binary 1-perfect additive codes: some structural properties. *IEEE Transactions on Information Theory 48, .n 9, pp. 2587-2592*, 2002.

[Pre68] F.P. Preparata. A class of optimum nonlinear double-error correcting codes. *Information and Control 13, pp. 378-400*, 1968.

[PRV04] K. T. Phelps, J. Rifà, and M. Villanueva. Rank and kernel of additive ($\mathbb{Z}_4$-linear and non $\mathbb{Z}_4$-linear) Hadamard codes. In *Proceedings of Algebraic and Combinatorial Coding Theory. ACCT'04*, pages 327–332, Kranevo, Bulgaria, June 2004.

[PRV05] K. T. Phelps, J. Rifà, and M. Villanueva. On the additive ($\mathbb{Z}_4$-linear and non $\mathbb{Z}_4$-linear) Hadamard codes. Rank and kernel. *Accepted in IEEE Transactions on Information Theory*, 2005.

[RBH89] J. Rifà, J. M. Basart, and L. Huguet. On completely regular propelinear codes. In *6th International Conference, AAECC-6*, volume 357 LNCS, pp. 341-355, 1989.

[Ree54] I.S. Reed. A class of multiple-error-correcting codes and the decoding schemes. *IRE Transactions on Information Theory 4, pp. 38-49*, 1954.

[Rif99] J. Rifà. Well-ordered steiner triple systems and 1-perfect partitions of the n-cube. *SIAM J. Discrete Math. 12, n. 1, pp. 35-47*, 1999.

[Sno73] S. L. Snover. *The uniqueness of the Nordstrom-Robinson code and the Golay binary codes*. PhD thesis, Michigan State University, 1973.

[Sol81] F.I. Solov'eva. On binary nongroup codes. *Methody Discretnogo Analiza 37, pp. 65-76*, 1981.

[Sol88] F.I. Solov'eva. Factorization of code-generating disjunctive normal forms. *Methody Discretnogo Analiza 47, pp. 66-88*, 1988.

[Sol00] F.I Solov'eva. Switching and perfect codes. In *Numbers, Information and Complexity*, volume pp. 311-324. Kluwer Academic Publishers, 2000.

[SZZ71] N.V. Semakov, V.A. Zinov'ev, and G.V. Zaitsev. Uniformly packed codes. *Problems of Information Tranmission 7(1), pp.30-39*, 1971.

[SZZ72] N.V. Semakov, V.A. Zinov'ev, and G.V. Zaitsev. On duality of preparata and kerdock codes. *Fith All-Union Conf. on Coding Theory part 2, pp.55-58 (in Russian)*, 1972.

[SZZ73] N.V. Semakov, V.A. Zinov'ev, and G.V. Zaitsev. Interrelation of preparata and hamming ccodes and extension of hamming codes to new double-error-correcting codes. *Proc. of Second Intern. Sympo. on Inform. Theory (Tsahkadsor, Armenia), pp.257-263*, 1973.

[Tie73] A. Tietäväinen. On the nonexistence of perfect codes over finite fields. *SIAM J. Appl. Math. 24, pp.88-96*, 1973.

[Vas62] J.L. Vasil'ev. On nongroup close-packed codes. *Problemy Kibernitiki 8, pp. 337-339*, 1962.

[Vil01] M. Villanueva. *On rank and kernel of perfect codes.* PhD thesis, Univ. Autònoma de Barcelona, 2001.

[VP02] M. Villanueva and K. Phelps. On perfect codes: rank and kernel. *Designs, Codes and Cryptography 27, n. 3, pp. 183-194*, 2002.

[Wan97] Z.-X. Wan. *Quaternary Codes.* World Scientific, 1997.

[WCC19] H.S. White, F.N. Cole, and L.D. Cummings. Complete classification of the triad systems of fifteen elements. *Mem. Mat. Acad. Sci. USA, 2nd memoir, 14, pp. 1-89*, 1919.

[ZL73] V.A. Zinov'ev and V.K. Leont'ev. The nonexistence of perfect codes over Galois fields. *Probl. Control and Inform. Theory 2, pp. 123-132*, 1973.

Index

Cristina Fernández Córdoba

Bellaterra, June 2005