UAB
Universitat Autònoma de Barcelona

Departament d' Enginyeria de la Informació i de les Comunicacios

On Quaternary Linear Reed-Muller Codes

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

by Jaume Pernas

Supervised by Dr. Mercè Villanueva and Dr. Jaume Pujol

Bellaterra, May 2012

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, May 2012

Dr. Mercè Villanueva Gay (Adviser)

Dr. Jaume Pujol Capdevila (Adviser)

Committee:

Dr. Joaquim Borges Ayats
Dr. Steven Dougherty
Dr. Leo Storme
Dr. Josep Rifà i Coma (substitute)
Dr. Patrick Solé (substitute)

a la meva família

Abstract

Recently, new families of quaternary linear Reed-Muller codes $\mathcal{RM}_s$ have been introduced. They satisfy that, under the Gray map, the corresponding $\mathbb{Z}_4$-linear codes have the same parameters and properties (length, dimension, minimum distance, inclusion, and duality relation) as the codes of the binary linear Reed-Muller family. The kernel of a binary code C is $K(C) = \{x \in \mathbb{Z}_2^n \ : \ C + x = C\}$. The dimension of the kernel is a structural invariant for equivalent binary codes. In this work, the dimension of the kernel for these new families of $\mathbb{Z}_4$-linear Reed-Muller codes is established. This result is sufficient to give a full classification of these new families of $\mathbb{Z}_4$-linear Reed-Muller codes up to equivalence.

A quaternary linear Hadamard code $\mathcal{C}$ is a code over $\mathbb{Z}_4$ that under the Gray map, the corresponding $\mathbb{Z}_4$-linear code is a binary Hadamard code. It is well known that quaternary linear Hadamard codes are included in the $\mathcal{RM}_s$ families of codes. The permutation automorphism group of a quaternary linear code $\mathcal{C}$ of length n is defined as PAut($\mathcal{C}$) $= \{\sigma \in S_n : \sigma(\mathcal{C}) = \mathcal{C}\}$. In this dissertation, the order of the permutation automorphism group of all quaternary linear Hadamard codes is established. Moreover, these groups are completely characterized by providing their generators and also by computing the orbits of their action on $\mathcal{C}$. Since the dual of a Hadamard code is an extended 1-perfect code in the quaternary sense, the permutation automorphism group of the quaternary linear extended 1-perfect codes is also established.

A la literatura recent hi podem trobar la introducció de noves famílies de codis de Reed-Muller quaternaris lineals $\mathcal{RM}_s$. Les imatges d' aquests nous codis a través del mapa de Gray són codis binaris $\mathbb{Z}_4$-lineals que comparteixen els paràmetres i les propietats (longitud, dimensió, distància mínima, inclusió, i relació de dualitat) amb la família de codis de Reed-Muller binaris lineals. El kernel d' un codi binari C es defineix com $K(C) = \{x \in \mathbb{Z}_2^n : C + x = C\}$. La dimensió del kernel és un invariant estructural per els codis binaris equivalents. Part d' aquesta tesi consisteix en establir els valors de la dimensió del kernel per aquestes noves famílies de codis de Reed-Muller $\mathbb{Z}_4$-lineals. Tot i que dos codis $\mathbb{Z}_4$-lineals no equivalents poden compartir el mateix valor de la dimensió del kernel, en el cas dels codis de Reed-Muller $\mathcal{RM}_s$ aquest resultat es suficient per donar-ne una classificació completa.

Per altra banda, un codi quaternari lineal de Hadamard $\mathcal{C}$, és un codi que un cop li hem aplicat el mapa de Gray obtenim un codi binari de Hadamard. És conegut que els codis de Hadamard quaternaris formen part de les famílies de codis quaternaris de Reed-Muller $\mathcal{RM}_s$. Definim el grup de permutacions d' un codi quaternari lineal com PAut$(\mathcal{C}) = \{\sigma \in S_n : \sigma(\mathcal{C}) = \mathcal{C}\}$. Com a resultat d' aquesta tesi també s' estableix l' ordre dels grups de permutacions de les famílies de codis de Hadamard quaternaris. A més a més, aquests grups són caracteritzats proporcionant la forma dels seus generadors i la forma de les òrbites del grup PAut$(\mathcal{C})$ actuant sobre el codi $\mathcal{C}$. Sabem que el codi dual, en el sentit quaternari, d' un codi de Hadamard és un codi 1-perfecte estès. D' aquesta manera els resultats obtinguts sobre el grup de permutacions es poden transportar a una família de codis quaternaris 1-perfectes estesos.

Preface

This dissertation shows much of the work that I had done during my PhD degree in the Departament d' Enginyeria de la Informació i les Comunicacions at the Universitat Autònoma de Barcelona. It is presented as a compendium of publications, thus the contributions are appended to this document in the form of publications to conferences and/or journals.

As it is already common at the Combinatorics, Coding and Security Group, where this thesis has been developed, the name of the authors of the publications appended to this document appear in the corresponding documents in alphabetical order.

This work has been partially supported by the Spanish Government MICINN under grants TIN2010-17358, MTM2001-13856-E and also by the Comissionat per a Universitats i Recerca del DIUE de la Generalitat de Catalunya under grant 2009SGR1224.

Contents

Chapter 1

Introduction

The best way to start reading a thesis is a good thought. So, let me say you "This wohk is great". As you have seen, it is not as good as it looks because there is an error. Very quickly you replace "wohk" by "work" and the meaning becomes clear. You have used some coding theory techniques to solve this situation by detecting and correcting an error, but how did you do it? In your subconscious, three assumptions has been made:

1. You are looking for an English word.
2. You are looking for a four-letter word.
3. The most likely situation is that one letter is wrong instead of more than one.

Assumption 1 allowed us to detect the error. There are lots of four-letter words in English, but assumption 3 is justifying the choose of word "work", which is probably the only English word we could make by changing one letter. In other situation, if we had received the word "oork" we would have chosen lots of possible words by switching only one letter, i.e. "work, pork, cork, ...". So, we would have not corrected the error. Finally, if we had received an English word, but not the sent one, we would not have caught the error. Say for example "fork".

The above situation is an example of a decoder algorithm in a digital communication scheme. This is crucial in telecommunication, where data is sent over a noisy channel where information might change before it is received. The aim of coding theory is to

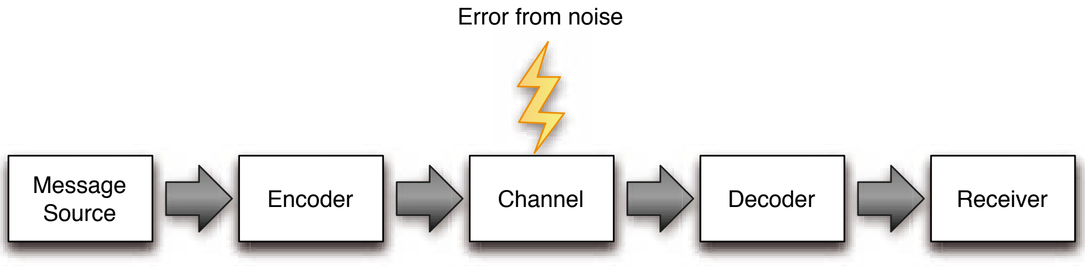

Figure 1.1: Communication scheme

find codes which allow to encode and decode in an easy way, to detect and correct errors produced in the channel, and to maximize the data transferred by unit per time.

In 1948, Claude Shannon started coding theory with the publication [Sha48]. For more than 50 years, coding theory has grown up feeding on mathematics and engineering and has became a pillar of the Information Society. There are applications to almost every area of communication such as satellite and cellular telephone transmission, Internet connections, compact disc recording, and data storage.

A digital communication scheme is formed by a source which sends information to a receiver through a transmission channel. In this channel, there might exist some noise which changes some bits of the sent information.

The encoder adds redundancy to the information generated by the source. When this information is received, the decoder can use this redundancy to detect and correct the errors added by the transmission channel. Recall the English code example. We corrected "wohk" to "work" because words like "wojk , kohk, ..." has no sense in English. Thus, the redundancy in the language is helpful for communication purposes. In other words, all the possible words of a fixed length are not English words. Only a subset of these combinations are part of the English code.

Historically, in coding theory, the binary alphabet is commonly used insted of the English one. Thus, codes are subsets of $\mathbb{Z}_2^n$, which is the space of binary words of length n. We call them binary codes. Recalling assumption 1, we need an easy way to know which words are part of the code and which are not. In English, there are the Oxford dictionaries. In $\mathbb{Z}_2^n$, if you do not want to store an explicit list of codewords, you can use linear codes. In other words, you can use the algebraic structure of the vector space. Thus, for any linear code there is a generator matrix and a parity check matrix which makes easier the use of the code than looking at a dictionary. Imagine that “operating” with a small set of words, you could generate any English word.

On the other hand, it is known that there exist some binary nonlinear codes with good properties. Indeed, there exist several binary nonlinear codes having twice as many codewords as the best binary linear code with the same length and minimum distance. Among these codes, there are the Preparata-like and Kerdock-like codes. Whenever a code is nonlinear, there are two invariants of the code that give information about how far is that code to be linear: the rank and dimension of the kernel.

An important step in coding theory was achieved when it was proved that the nonlinear codes mentioned above could be considered as quaternary linear codes under the Gray map image [Nec89]. The term $\mathbb{Z}_4$-linear code is used to denote such a binary code with an algebraic structure over $\mathbb{Z}_4$, whereas the codes defined as subsets of $\mathbb{Z}_4$ are called *quaternary linear codes*.

One of the simplest and most important family of binary linear codes is the Reed-Muller family of codes, denoted by RM. The importance of these codes lies in the fact that they are relatively easy to encode and decode using majority-logic circuits. In general, the Reed-Muller codes are not $\mathbb{Z}_4$-linear codes, but in 2007, a way to construct families of quaternary linear codes denoted by $\mathcal{RM}_s$ such that, under the Gray map, the corresponding $\mathbb{Z}_4$-linear codes have exactly the same properties as the binary linear Reed-Muller codes was presented [PRS07, PRS09]. In this dissertation, we will focus on these quaternary linear Reed-Muller codes.

This dissertation is presented and organized as a compendium of publications. Because of the space constraints of most of the publications, the contributions appended to this document do not include many details nor a complete background on the topic they deal with. It is for this reason that we found convenient to provide the appropriate background and introduce some of the main definitions and techniques of coding theory in Chapter 2. In that chapter you will find all the definitions about binary and quaternary codes as well as the concepts of equivalence between codes. Chapter 3 gives an introduction to the $\mathcal{RM}_s$ families of quaternary linear Reed-Muller codes. Chapter 4 reviews and summarizes the results of the publications making up this dissertation, shows the storyline that links them up, and discusses their relevance. Finally, Chapter 5 concludes this dissertation and proposes some future lines of research. A copy of all contributions comprising this compendium is provided at the end of this document, ordered by publication date.

Chapter 2

Coding Theory

This chapter is a review of coding theory. There are definitions and results which will be used on subsequent chapters and contributions. Section 2.1 starts by introducing some concepts related to binary codes. For more information about classic coding theory see [MS77, PHB98]. In Section 2.2, there are the basics concepts about quaternary linear codes and how they are connected with the concept of $\mathbb{Z}_4$-linear codes. A more extensive review can be found in [HKC$^+$94, Wan97]. Section 2.3 contains a review of the extended 1-perfect codes and Hadamard codes which will be included in the families of quaternary linear Reed-Muller codes $\mathcal{RM}_s$. In Section 2.4, the concept of equivalence between codes is introduced. This leads us to the definition of the permutation automorphism group of a code. Finally, in Section 2.5, the concepts of rank and dimension of the kernel of a binary code are introduced.

2.1 Binary codes

Let $\mathbb{Z}_2$ be the ring of integers modulo two. Let $\mathbb{Z}_2^n$ be the set of all binary words of length n. Any nonempty subset C of $\mathbb{Z}_2^n$ is a *binary code* and a subgroup of $\mathbb{Z}_2^n$ is called a *binary linear code* or a $\mathbb{Z}_2$*-linear code*. The elements of a code are called codewords. Since $\mathbb{Z}_2$ is a finite field, the dimension of a binary linear code C, denoted by k, can be defined as the dimension of the linear subspace C in $\mathbb{Z}_2$.

The *Hamming distance* $d_H(u,v)$ between two words $u,v \in \mathbb{Z}_2^n$ is the number of coordinates in which u and v differ. The *Hamming weight* of a word $u \in \mathbb{Z}_2^n$, denoted by $w_H(u)$, is the number of nonzero coordinates of u. If C is a binary code, then we assume that $\mathbf{0} \in C$, where $\mathbf{0}$ is the all-zero codeword. In general, a bold number will be a codeword where this number is repeated in all the coordinates. The *minimum Hamming distance* d of C is the minimum value of $d_H(u,v)$ for $u,v \in C$ satisfying $u \neq v$. The *minimum Hamming weight* of C, denoted by $w_H(C)$, is the minimum value of $w_H(u)$ for $u \in C \setminus \{\mathbf{0}\}$. The *error correcting capability* is $e = \lfloor \frac{d-1}{2} \rfloor$ and C is an e-error correcting binary code.

The *covering radius* of a binary code C, denoted by ρ, is the maximum value of $d(v,C)$ over all words $v \in \mathbb{Z}_2^n$. In terms of Hamming spheres, it is the smallest integer ρ such that the spheres with that radius centered at the codewords of C cover the whole space.

Let A_i be the number of codewords of Hamming weight i in a binary code C, then the set $\{A_0, \dots, A_n\}$ is called the *weight distribution* of C. The *weight enumerator* of C is defined as the polynomial $W_C(X,Y) = \sum_{i=0}^{n} A_i X^{n-i} Y^i$, which is an homogenous polynomial of degree n in X and Y.

Consider the *translate classes* of a binary code C, $C + x = \{u + x : u \in C\}$, where the word $x \in \mathbb{Z}_2^n$. If C is a binary linear code, then the translate classes are also called *cosets*. Each word of $\mathbb{Z}_2^n$ of weight less than or equal to e is on a different translate of C. A binary code C is called *distance invariant* if the weight distribution of $C + v$ is the same for any $v \in C$. If C is distance invariant and $\mathbf{0} \in C$, then the minimum Hamming distance and the minimum Hamming weight coincide.

The *inner product* for any two words $u,v \in \mathbb{Z}_2^n$ is defined as:

$$\langle u, v \rangle = \sum_{i=1}^{n} u_i v_i \in \mathbb{Z}_2.$$

If $\langle u, v \rangle = 0$, then u and v are called *orthogonal*. Let C be a binary code, we define the *orthogonal code of* C, denoted by $C^\perp$, as the set of codewords which are orthogonal to all codewords of C:

$$C^\perp = \{x \in \mathbb{Z}_2^n : \langle x, u \rangle = 0 \; \forall u \in C\}.$$

When C is a linear code, then $C^\perp$ is called the *dual* of the code C. If $C \subset C^\perp$ then C is called *self-orthogonal* code and, if $C = C^{\perp}$ then C is called *self-dual* code. The following relation between the weight enumerator of a code and its dual is called the MacWilliams identity [MS77].

$$W_{C^{\perp}}(X,Y) = \frac{1}{|C|} W_C(X+Y, X-Y). \tag{2.1}$$

In the literature [MS77], there are examples of binary nonlinear codes with better parameters than any binary linear codes. This makes interesting the study of binary nonlinear codes despite the lack of linear structure.

For example, the Preparata codes are an infinite family of codes, denoted by $P(m)$ of length 2^m with 2^{2^m-2m} codewords and minimum distance 6 for all even $m \geq 4$. Moreover, the Kerdock codes are another family of codes, denoted by $K(m)$ of length 2^m with 2^{2m} codewords and minimum distance $2^{m-1} - 2^{(m-2)/2}$. Despite these two families contains codes which are nonlinear they hold the MacWilliams transform (see Equation 2.1). This fact suggests a kind of duality relation, which will be clarified in Section 2.2. The point which makes interesting to study binary nonlinear codes is that sometimes we find great nonlinear codes. For example, the codes $P(m)$ and $K(m)$ appear to contain at least twice as many codewords as the best linear code with the same length and minimum distance.

2.2 Quaternary linear codes

Let $\mathbb{Z}_4$ be the integers ring modulo 4. Let $\mathbb{Z}_4^n$ be the set of all quaternary words of length n. Any nonempty subset $\mathcal{C}$ of $\mathbb{Z}_4^n$ is a *quaternary code* of length n and if $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$ then $\mathcal{C}$ is called a *quaternary linear code*.

In contrast to binary codes, the metric used with quaternary codes is not the Hamming one, but the Lee metric. We define the *Lee weights* over the elements in $\mathbb{Z}_4$ as: $w_L(0) = 0$, $w_L(1) = w_L(3) = 1$, $w_L(2) = 2$. The *Lee weight* of a word $u \in \mathbb{Z}_4^n$ is the addition of the weights of its coordinates, whereas the *Lee distance* $d_L(u,v)$ between two words $u, v \in \mathbb{Z}_4^n$ is defined as $d_L(u,v) = w_L(u-v)$. The *minimum Lee distance* of a quaternary code $\mathcal{C}$ is the minimum value of $d_L(u,v)$ for $u, v \in \mathcal{C}$ satisfying $u \neq v$. The *minimum Lee weight* of a quaternary code $\mathcal{C}$, denoted by $w_L(\mathcal{C})$, is the minimum value of $w_L(u)$ for $u \in \mathcal{C} \setminus \{\mathbf{0}\}$.

The Gray map, $\phi : \mathbb{Z}_4^n \longrightarrow \mathbb{Z}_2^{2n}$ given by $\phi((v_1, \dots, v_n)) = (\varphi(v_1), \dots, \varphi(v_n))$, where $\varphi(0) = (0,0)$, $\varphi(1) = (0,1)$, $\varphi(2) = (1,1)$, $\varphi(3) = (1,0)$, is an isometry which transforms Lee distances over $\mathbb{Z}_4^n$ into Hamming distances over $\mathbb{Z}_2^{2n}$. Therefore, the minimum Lee weight of a quaternary code $\mathcal{C}$ coincides with the minimum Hamming weight of $C = \phi(\mathcal{C})$. Thus, if $\phi(\mathcal{C})$ is distance invariant we can say that $\mathcal{C}$ is distance invariant and if $\mathbf{0} \in \mathcal{C}$ then, the minimum Lee weight and the minimum Lee distance coincide.

Let $\mathcal{C}$ be a quaternary linear code. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$, it is isomorphic to an abelian structure $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, $\mathcal{C}$ is of type $2^\gamma 4^\delta$ as a group, it has $|\mathcal{C}| = 2^{\gamma+2\delta}$ codewords and $2^{\gamma+\delta}$ of these have order two. The binary image $C = \phi(\mathcal{C})$ of any quaternary linear code $\mathcal{C}$ of length n and type $2^\gamma 4^\delta$ is called a $\mathbb{Z}_4$-*linear code* of length $2n$ and type $2^\gamma 4^\delta$.

Two quaternary linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ both of length n and type $2^\gamma 4^\delta$ are said to be *permutation equivalent*, if one can be obtained from the other by permuting the coordinates. The concept of equivalent codes is deeply discussed in Section 2.4.

Let $\mathcal{C}$ be a quaternary linear code. Although $\mathcal{C}$ is not a free module, every codeword is uniquely expressible in the form

$$\sum_{i=1}^{\gamma} \lambda_i u_i + \sum_{j=1}^{\delta} \mu_j v_j,$$

where $\lambda_i \in \mathbb{Z}_2$ for $1 \leq i \leq \gamma$, $\mu_j \in \mathbb{Z}_4$ for $1 \leq j \leq \delta$ and u_i, v_j are codewords in $\mathbb{Z}_4^n$ of order two and four, respectively. The codewords u_i, v_j give us a generator matrix $\mathcal{G}$ of size $(\gamma + \delta) \times n$ for the code $\mathcal{C}$. In [HKC$^+$94], it was shown that any quaternary linear code of type $2^\gamma 4^\delta$ is permutation equivalent to a quaternary linear code with a canonical generator matrix of the form

$$\mathcal{G}_S = \left(\begin{array}{ccc} 2T & 2I_\gamma & \mathbf{0} \\ \hline S & R & I_\delta \end{array} \right), \tag{2.2}$$

where R, T are matrices over $\mathbb{Z}_2$ of size $\delta \times \gamma$ and $\gamma \times (n - \gamma - \delta)$, respectively; and S is a matrix over $\mathbb{Z}_4$ of size $\delta \times (n - \gamma - \delta)$.

Example 1 *Let $\mathcal{C}$ be a quaternary linear code with generator matrix*

$$\mathcal{G} = \left(\begin{array}{cccccccc} 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ \hline 2 & 0 & 2 & 1 & 1 & 1 & 2 & 1 \\ 0 & 0 & 0 & 2 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 & 1 & 3 & 1 \end{array}\right).$$

The code $\mathcal{C}$ is permutation equivalent using the permutation $(7,8)$ to a quaternary linear code $\mathcal{C}'$ with the generator matrix $\mathcal{G}'$ in the canonical form showed in Matrix (2.2), where

$$\mathcal{G}' = \left(\begin{array}{cccccccc} 0 & 0 & 0 & 2 & 2 & 2 & 0 & 0 \\ \hline 2 & 0 & 2 & 3 & 3 & 1 & 1 & 0 \\ 2 & 0 & 2 & 3 & 1 & 0 & 0 & 1 \end{array}\right).$$

Therefore, the code $\mathcal{C}$ is of type $4^2 2^1$, so it has $4^2 2 = 32$ codewords.

The following two lemmas were proved for quaternary words and quaternary linear codes, respectively, in [HKC$^+$94]. Let $u * v$ denote the component-wise product, for any $u, v \in \mathbb{Z}_4^n$.

Lemma 1 ([HKC$^+$94, Wan97]) *For all $u, v \in \mathbb{Z}_4^n$, we have*

$$\phi(u+v) = \phi(u) + \phi(v) + \phi(2u * v).$$

Note that if u or v are words in $\mathbb{Z}_4^n$ of order two, then $\phi(u+v) = \phi(u) + \phi(v)$.

Lemma 2 ([HKC$^+$94, Wan97]) *Let $\mathcal{C}$ be a quaternary linear code. The $\mathbb{Z}_4$-linear code $C = \phi(\mathcal{C})$ is a binary linear code if and only if $2u * v \in \mathcal{C}$ for all $u, v \in \mathcal{C}$.*

Note that if $\mathcal{G}$ is a generator matrix of a quaternary linear code $\mathcal{C}$ and $\{u_i\}_{i=1}^{\gamma}$ and $\{v_j\}_{j=0}^{\delta}$ the rows of order two and order four in $\mathcal{G}$, respectively, the $\mathbb{Z}_4$-linear code $C = \phi(\mathcal{C})$ is a binary linear code if and only if $2v_j * v_k \in \mathcal{C}$, for all j, k satisfying $1 \leq j < k \leq \delta$.

The usual *inner product* for any two words $u, v \in \mathbb{Z}_4^n$ is defined as:

$$\langle u, v\rangle = u{\cdot}I_n{\cdot}v^t,$$

where I_n is the identity matrix of size n.

Let $K_2 = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$ be a matrix over $\mathbb{Z}_4$ and define $K_n = \bigotimes_{j=1}^{\log_2 n} K_2$ for any $n = 2^m$, where $\bigotimes$ denotes the Kronecker product of matrices. The *Kronecker inner product* for any two words $u, v \in \mathbb{Z}_4^{2^m}$ is defined as:

$$\langle u, v\rangle_{\otimes n} = u{\cdot}K_n{\cdot}v^t.$$

Given a quaternary linear code $\mathcal{C}$ of length n, the *quaternary dual code* of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined as

$$\mathcal{C}^\perp = \{u \in \mathbb{Z}_4^n \ : \ \langle u, v\rangle = 0 \text{ for all } v \in \mathcal{C}\}.$$

Given a quaternary linear code $\mathcal{C}$ of length $n = 2^m$, the *quaternary Kronecker dual code* of $\mathcal{C}$, denoted by $\mathcal{C}_\otimes^\perp$, is defined as

$$\mathcal{C}_\otimes^\perp = \{u \in \mathbb{Z}_4^n \ : \ \langle u, v\rangle_{\otimes n} = 0 \text{ for all } v \in \mathcal{C}\}.$$

Note that $\langle u, v\rangle_{\otimes n} = u{\cdot}K_n{\cdot}v^t = \langle u, v{\cdot}K_n\rangle$. Hence, both quaternary dual codes are the same by changing some coordinates of sign. We will talk more carefully about code equivalences in Section 2.4. For both inner products, the dual code is also a quaternary linear code, that is a subgroup of $\mathbb{Z}_4^n$.

Given a quaternary linear code $\mathcal{C}$ of length n and type $2^\gamma 4^\delta$, the quaternary dual code is of length n and type $2^\gamma 4^{n-\gamma-\delta}$ [HKC+94]. If the generator matrix $\mathcal{G}$ of $\mathcal{C}$ is in the canonical form given by Matrix (2.2) then, the generator matrix $\mathcal{H}_S$ of the dual code $\mathcal{C}^\perp$ can be computed as follows:

$$\mathcal{H}_S = \left(\begin{array}{ccc} \mathbf{0} & 2I_\gamma & 2R^t \\ \hline I_{n-\gamma-\delta} & T^t & -(S+RT)^t \end{array}\right). \tag{2.3}$$

Example 2 *Since the generator matrix $\mathcal{G}'$ of $\mathcal{C}'$ in Example 1 is written in the canonical form then, the generator matrix $\mathcal{H}'$ of $\mathcal{C}'^{\perp}$ can be computed using Matrix (2.3). The generator matrix of $\mathcal{C}^{\perp}$ is the matrix $\mathcal{H}$ applying the permutation $(7, 8)$ to $\mathcal{H}'$, where*

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

Therefore, the code $\mathcal{C}^{\perp}$ is of type $4^5 2^1$, so it has $4^5 2 = 2048$ codewords.

The weight enumerator polynomial of $\mathcal{C}^{\perp}$ is related to the weight enumerator polynomial of $\mathcal{C}$ by the MacWilliams identity [Del73] showed in Section 2.1. The corresponding binary code $\phi(\mathcal{C}^{\perp})$ is denoted by $C_{\perp}$ and called the $\mathbb{Z}_4$-*dual code* of C. Notice that C and $C_{\perp}$ are not dual in the binary linear sense, but the weight enumerator polynomial of $C_{\perp}$ is the MacWilliams transform (see Equation 2.1) of the weight enumerator polynomial of C.

$$\begin{tikzcd} \mathcal{C} \arrow[r, "\text{quaternary dual}"] & \mathcal{C}^{\perp} \arrow[d, "\phi"] \\ C \arrow[u, "\phi^{-1}"] & C_{\perp} \end{tikzcd}$$

In recent years, quaternary linear codes have attracted the attention of the coding community as several notorious binary nonlinear codes like Kerdock codes and Preparata codes were found to be binary images under the Gray map of a quaternary linear code [Nec89, HKC^{+}94]. This discovery opened the way for a broader study of quaternary codes, which has constituted a rapidly growing area of coding theory. As we said in Section 2.1, Kerdock and Preparata codes holds the MacWilliams identity. That is because they are $\mathbb{Z}_4$-dual codes.

This dissertation is focused on quaternary linear codes and $\mathbb{Z}_4$-linear codes. However, it is interesting to mention that there is a generalization of these codes called $\mathbb{Z}_2\mathbb{Z}_4$-additive codes and $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, respectively [RBH89, PR97b].

A code $\mathcal{C}$ is $\mathbb{Z}_2\mathbb{Z}_4$-additive if the set of coordinates can be partitioned into two subsets X and Y such that the punctured code of $\mathcal{C}$ by deleting the coordinates outside X (respectively, Y) is a binary linear code (respectively, a quaternary linear code). Their corresponding binary images, via the Gray map, are called $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. The fundamental parameters as well as the standard forms for generator and parity-check matrices and the duality concepts of these codes are studied in [BFCP$^+$10].

2.3 Extended 1-perfect and Hadamard codes

Let C be a binary code of length n. The code C is said to be *perfect* if for some integer $r \geq 0$, every $x \in \mathbb{Z}_2^n$ is within distance r from exactly one codeword of C. This definition is equivalent to say that the covering radius of the code C coincides with the error correcting capability e of the code C. Thus, C is said to be an $e-perfect$ code.

In [ZL73, Tie73], it is shown that the only parameters for nontrivial binary perfect codes are the 3-perfect Golay code of length 23 and the 1-perfect codes of length $n = 2^m - 1$. We will focus on the 1-perfect ones.

Binary 1-perfect codes have length $n = 2^m - 1$ and minimum distance 3. They have 2^{n-m} codewords. Binary linear 1-perfect codes are unique up to equivalence, they are the well-known *Hamming codes* and they exist for any $m \geq 2$. On the other hand, there are lots of binary nonlinear 1-perfect codes and they exist for any $m \geq 4$.

Given a binary 1-perfect code of length $2^m - 1$, when we add an even parity coordinate to all codewords, we obtain a binary code of length $n = 2^m$ with minimum distance 4. These codes are called *extended 1-perfect codes*. It is known that there are quaternary linear codes such that, under the Gray map, they became *$\mathbb{Z}_4$-linear extended 1-perfect codes*. We call them *quaternary linear extended 1-perfect codes*.

Given $m \geq 1$, a binary code with 2^{m+1} codewords, minimum distance 2^{m-1} and length $n = 2^m$ is called a *Hadamard code*. In a Hadamard code, all the codewords, except the all-one and all-zero codewords, have Hamming weight $n/2$, where n is the length of the code.

The dual code of the extended Hamming code of length $n = 2^m$ is the linear Hadamard code. Moreover, the $\mathbb{Z}_4$-dual code of every $\mathbb{Z}_4$-linear extended 1-perfect code is a $\mathbb{Z}_4$-linear

Hadamard code [Kro01]. There are quaternary linear codes such that, under the Gray map, they become $\mathbb{Z}_4$*-linear Hadamard codes*. We call these codes *quaternary linear Hadamard codes*. Moreover, the quaternary dual of a quaternary linear extended 1-perfect code is a quaternary linear Hadamard code.

There is a recursive construction for the generator matrices of the quaternary linear Hadamard codes. We can contruct one generator matrix $\mathcal{H}_{\delta,m}$ for every $m \geq 1$ and $1 \leq \delta \leq \lfloor \frac{m+1}{2} \rfloor$ in the following way:

$$\mathcal{H}_{1,1} = \begin{pmatrix} 1 \end{pmatrix};$$

$$\mathcal{H}_{\delta,m} = \begin{pmatrix} \mathcal{H}_{\delta,m-1} & \mathcal{H}_{\delta,m-1} \\ \mathbf{0} & \mathbf{2} \end{pmatrix} \text{ if } m > 2\delta - 1,\ \delta \geq 1;$$

$$\mathcal{H}_{\delta,m} = \begin{pmatrix} \mathcal{H}_{\delta-1,m-2} & \mathcal{H}_{\delta-1,m-2} & \mathcal{H}_{\delta-1,m-2} & \mathcal{H}_{\delta-1,m-2} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \end{pmatrix} \text{ if } m = 2\delta - 1,\ \delta \geq 2.$$

Example 3 *For $m = 5$, we can construct the following three generator matrices for quaternary linear Hadamard codes. Note that, every $\mathcal{H}_{\delta,m}$ is the parity check matrix of the quaternary linear extended 1-perfect code denoted by $\mathcal{E}_{\delta,m}$.*

$$\mathcal{H}_{1,5} = \left(\begin{array}{cccccccccccccccc} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ \hline 0&2&0&2&0&2&0&2&0&2&0&2&0&2&0&2 \\ 0&0&2&2&0&0&2&2&0&0&2&2&0&0&2&2 \\ 0&0&0&0&2&2&2&2&0&0&0&0&2&2&2&2 \\ 0&0&0&0&0&0&0&0&2&2&2&2&2&2&2&2 \end{array}\right).$$

$$\mathcal{H}_{2,5} = \left(\begin{array}{cccccccccccccccc} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3 \\ \hline 0&0&0&0&2&2&2&2&0&0&0&0&2&2&2&2 \\ 0&0&0&0&0&0&0&0&2&2&2&2&2&2&2&2 \end{array}\right).$$

$$\mathcal{H}_{3,5} = \left(\begin{array}{cccccccccccccccc} \hline 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3 \\ 0&0&0&0&1&1&1&1&2&2&2&2&3&3&3&3 \end{array}\right).$$

2.4 Equivalent codes

In this section, we ask when two codes are “essentially the same”. We term this concept “equivalence”. Usually, we are interested in properties of codes, such as the weight distribution, which remains unchanged when passing from one code to another that is essentially the same.

Two binary linear codes could be considered “the same” if they were isomorphic as vector spaces. However, in that case the concept of weight is lost: codewords of one weight may be sent to codewords of different weight by the isomorphism. Moreover, we are interested in equivalences between codes which could be nonlinear or over other rings. Clearly, any permutation of coordinates or translation by one word, which sends one code to another one, preserves the weight of codewords, regardless of the field or even a ring. This idea leads us to the definitions of code equivalences.

Let S_n be the symmetric group of permutations on the set $\{1, \dots, n\}$, where $id \in S_n$ is the identity permutation. Let R be a ring. The group operation in S_n is the function composition, denoted by $\circ$. The composition $\sigma_1 \circ \sigma_2$ maps any element x to $\sigma_1(\sigma_2(x))$. A $\sigma \in S_n$ acts linearly on words of R^n by permuting the coordinates, $\sigma((c_1, c_2, \dots, c_n)) = (c_{\sigma^{-1}(1)}, c_{\sigma^{-1}(2)}, \dots, c_{\sigma^{-1}(n)})$.

Two codes $C_1 \subseteq R^n$ and $C_2 \subseteq R^n$ are said to be *equivalent* if there is a word $x \in R^n$ and a coordinate permutation π such that $C_2 = \{x + \pi(c) \ : \ c \in C_1\}$. They are said to be *permutation equivalent* if there is a permutation of coordinates which sends C_1 to C_2. The set of coordinate permutations that map a code C to itself forms a group called the *permutation automorphism group* of the code C denoted by $\mathrm{PAut}(C)$. Hence, if C is a code of length n, then $\mathrm{PAut}(C)$ is a subgroup of the symmetric group S_n.

When we are considering codes over a ring which is not $\mathbb{Z}_2$, equivalence could take a more general form. Despite the permutation equivalence, there are more general maps which preserve the Lee weight of codewords. These maps also include those which multiply the coordinates of the codewords by units of the ring.

A *monomial matrix* is a square matrix with exactly one nonzero divisor entry in each row and column. A monomial matrix M can be represented as a product of a diagonal matrix D and a permutation matrix P. Hence, $M = DP$. Note that the entries in the diagonal of D should be units. Thus, in $\mathbb{Z}_4$ means that the entries are 1 or 3.

Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two linear codes of the same length over the ring R. Let $\mathcal{G}_1$ be the generator matrix of $\mathcal{C}_1$. Then $\mathcal{C}_1$ and $\mathcal{C}_2$ are *monomially equivalent* if there is a monomial matrix M so that $\mathcal{G}_1 M$ is a generator matrix of $\mathcal{C}_2$. Moreover, if two quaternary linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are monomially equivalent then, the corresponding $\mathbb{Z}_4$-linear codes $C_1 = \phi(\mathcal{C}_1)$ and $C_2 = \phi(\mathcal{C}_2)$ are permutation equivalent.

As it happens in the permutation equivalence case, now the set of monomial matrices that map a code $\mathcal{C}$ to itself forms the group $\mathrm{MAut}(\mathcal{C})$ called the *monomial automorphism group* of $\mathcal{C}$. Since any permutation can be seen as a permutation matrix, in general, $\mathrm{PAut}(\mathcal{C})$ is a subgroup of $\mathrm{MAut}(\mathcal{C})$.

Let $\mathcal{C}$ be a quaternary linear code. Let $C = \phi(\mathcal{C})$ be the binary image under the Gray map, that is, the corresponding $\mathbb{Z}_4$-linear code. In this situation we can study three groups: $\mathrm{PAut}(\mathcal{C})$, $\mathrm{MAut}(\mathcal{C})$ and $\mathrm{PAut}(C)$. As we said, $\mathrm{PAut}(\mathcal{C}) \subseteq \mathrm{MAut}(\mathcal{C})$. Finally, the study of $\mathrm{MAut}(\mathcal{C})$ can help to determine a subgroup of $\mathrm{PAut}(C)$.

In the literature, we can find several studies of the permutation automorphism groups of some known binary codes. The permutation automorphism group of the $\mathbb{Z}_2\mathbb{Z}_4$-linear extended 1-perfect codes, which include the $\mathbb{Z}_4$-linear extended 1-perfect codes, was studied in [Kro11]. Moreover, the permutation automorphism group of the span of the same codes was studied in [PR02]. In general, the permutation automorphism group of (nonlinear) binary 1-perfect codes was studied before, obtaining some partial results [HPW09, Hed05, ASH05, FCPV11].

Let us recall some fundamental concepts of group theory applied to the permutation automorphism group $A = \mathrm{PAut}(C)$ acting on the code C. On the one hand, the *orbit* of a codeword $u \in C$ under the action of A is the set $A(u) = \{\sigma(u) : \sigma \in A\}$. Note that, since A is the permutation automorphism group of C, $A(u) \subseteq C$. Moreover, two codewords $u, v \in C$ are said to be *A-equivalent* if there exists a permutation $\sigma \in A$ such that $\sigma(u) = v$. Since this is an equivalence relation, C is partitioned into classes or *orbits*. If there is only one orbit, it is said that the action is *transitive*. On the other hand, the *stabilizer* of $u \in C$ in A is the subgroup $N^u = \{\sigma \in A : \sigma(u) = u\}$. Finally, the orbit-stabilizer theorem shows that $|A| = |A(u)||N^u|$ for all $u \in A$ [Cam99].

2.5 Rank and dimension of the kernel

In Section 2.4, we showed when two codes are "essentially the same" introducing the concept of equivalence. Now, given two binary codes we want to answer whether they are equivalent or not. We can solve this situation by doing an exhaustive search of all permutations, but it is an NP-hard problem. Thus, we will use invariants of binary codes to solve it.

We will use the rank and dimension of the kernel for binary codes. These two invariants do not always give a full classification of codes, since two nonequivalent codes could have the same rank and dimension of the kernel. In spite of that, they can help in classification, since if two codes have different ranks or dimension of the kernel, they are nonequivalent.

We will focus on $\mathbb{Z}_4$-linear codes. Recall that $\mathbb{Z}_4$-linear code is a binary code which is the Gray map image of a quaternary linear code. Let $\mathcal{C}$ be a quaternary linear code of length n and type $2^\gamma 4^\delta$ and let $C = \phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_4$-linear code of length $2n$. The *rank* r_C of a binary code C is the dimension of the linear span of the codewords of C. We will talk about the rank of a quaternary linear code $\mathcal{C}$ or the rank of the corresponding $\mathbb{Z}_4$-linear code $C = \phi(\mathcal{C})$ as the same value. Thus, $r_C = r_{\mathcal{C}}$. The rank of $\mathbb{Z}_4$-linear codes was studied in [FCPV08], where the authors showed that there exists a $\mathbb{Z}_4$-linear code C with $r_C = rank(C)$ for any possible value of r_C.

The following theorem shows the lower and the upper bounds for the rank of any quaternary linear code. Moreover, it also proves that there always exists a quaternary linear code for every possible value of the rank between these bounds.

Theorem 3 ([FCPV10, FCPV08]) *There exists a quaternary linear code $\mathcal{C}$ of length n and type $2^\gamma 4^\delta$ with rank $r_{\mathcal{C}}$ for any*

$$r_{\mathcal{C}} \in \{\gamma + 2\delta, \ldots, \min(n+\delta,\ \gamma + 2\delta + \binom{\delta}{2})\}.$$

Note that when $r_{\mathcal{C}} = \gamma + 2\delta$, the corresponding $\mathbb{Z}_4$-linear code by using the Gray map is a binary linear code, and it corresponds to the lower bound of the rank.

The kernel of a binary code C is $K(C) = \{x \in \mathbb{Z}_2^n \ :\ C + x = C\}$. Let $\mathcal{C}$ be a quaternary linear code and let $C = \phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_4$-linear code with kernel

$K(C)$ of dimension k_C. The kernel of $\mathcal{C}$, denoted by $\mathcal{K}(\mathcal{C})$, is defined as the inverse Gray map image of $K(C)$, that is $\mathcal{K}(\mathcal{C}) = \phi^{-1}(K(C))$. Furthermore, the dimension of the kernel of $\mathcal{C}$ is defined as the dimension of the kernel of $C = \phi(\mathcal{C})$, and is denoted by $k_{\mathcal{C}}$.

Lemma 4 ([FCPV10, FCPV08]) *Let $\mathcal{C}$ be a quaternary linear code. Then,*

$$\mathcal{K}(\mathcal{C}) = \{u : u \in \mathcal{C} \text{ and } 2u * v \in \mathcal{C}, \forall v \in \mathcal{C}\}.$$

Note that if $\mathcal{G}$ is a generator matrix of a quaternary linear code $\mathcal{C}$, then $u \in \mathcal{K}(\mathcal{C})$ if and only if $u \in \mathcal{C}$ and $2u * v \in \mathcal{C}$ for all $v \in \mathcal{G}$. Moreover, by Lemma 4, all codewords of order two in $\mathcal{C}$ belong to $\mathcal{K}(\mathcal{C})$. It is also clear that if the word $\mathbf{1}$ belongs to $\mathcal{C}$, then it is also in $\mathcal{K}(\mathcal{C})$. Finally, note that $\mathcal{K}(\mathcal{C})$ is a linear subcode of $\mathcal{C}$ [FCPV10, FCPV08].

The following theorem shows the lower and the upper bounds for the dimension of the kernel of any quaternary linear code. Furthermore, it also proves that there always exists a quaternary linear code for every possible value of the dimension of the kernel.

Theorem 5 ([FCPV08]) *There exists a quaternary linear code $\mathcal{C}$ of length n and type $2^\gamma 4^\delta$ with dimension of the kernel of $\mathcal{C}$ as $k_{\mathcal{C}}$ for any*

$$k_{\mathcal{C}} \in \begin{cases} \{\gamma+\delta, \ldots, \gamma+2\delta-2, \gamma+2\delta\} & \textit{if} \quad s \geq 2 \\ \{\gamma+2(\delta-\lceil\frac{\delta-1}{2}\rceil), \ldots, \gamma+2(\delta-1), \gamma+2\delta\} & \textit{if} \quad s = 1 \\ \{\gamma+2\delta\} & \textit{if} \quad s = 0, \end{cases}$$

where $s = n - \gamma - \delta$.

Note that when $k_{\mathcal{C}} = \gamma + 2\delta$, the corresponding $\mathbb{Z}_4$-linear code is a binary linear code, and it corresponds to the upper bound for the dimension of the kernel.

In Section 2.3, we defined the $\mathbb{Z}_4$-linear Hadamard and $\mathbb{Z}_4$-linear extended 1-perfect codes. In [Kro01], a full classification of such codes using these two invariants is given. One of the most fundamentals parts of this dissertation is the classification of the $\mathbb{Z}_4$-linear Reed-Muller codes presented in Chapter 3, which contain the $\mathbb{Z}_4$-linear Hadamard and $\mathbb{Z}_4$-linear extended 1-perfect codes.

The dimension of the kernel and the rank of $\mathbb{Z}_4$-linear Hadamard codes $H_{\delta,m} = \phi(\mathcal{H}_{\delta,m})$ of type $2^\gamma 4^\delta$ and $\mathbb{Z}_4$-linear extended 1-perfect codes $E_{\delta,m} = \phi(\mathcal{E}_{\delta,m})$ of type $2^{\bar\gamma}4^{\bar\delta}$ were studied in [BPR03, PRV04, Kro01]. Specifically,

$$k_{H_{\delta,m}} = \begin{cases} \gamma + 2\delta & \text{if} \quad \delta = 1, 2; \\ \gamma + \delta + 1 & \text{if} \quad \delta \geq 3; \end{cases} \tag{2.4}$$

$$k_{E_{\delta,m}} = \begin{cases} \bar\gamma + \bar\delta + m & \text{if} \quad \delta = 1; \\ \bar\gamma + \bar\delta + 2 & \text{if} \quad \delta = 2; \\ \bar\gamma + \bar\delta + 1 & \text{if} \quad \delta \geq 3; \end{cases} \tag{2.5}$$

$$r_{H_{\delta,m}} = \begin{cases} \gamma + 2\delta & \text{if} \quad \delta = 1, 2; \\ \gamma + 2\delta + \binom{\delta-1}{2} & \text{if} \quad \delta \geq 3; \end{cases} \tag{2.6}$$

$$r_{E_{\delta,m}} = \bar\gamma + 2\bar\delta + \delta = 2^{m-1} + \bar\delta; \tag{2.7}$$

$$\text{except } r_{E_{1,4}} = 11.$$

Recall that the codes $\mathcal{H}_{\delta,m}$ and $\mathcal{E}_{\delta,m}$ are quaternary duals. Thus, you can compute the type of the dual code by using the equations $\bar\gamma = \gamma$ and $\bar\delta = 2^{m-1} - \gamma - \delta$.

Example 4 *For $m = 5$, we have $\delta \in \{1, 2, 3\}$. See Example 3 for the generator matrices of the three codes $\mathcal{H}_{\delta,m}$. The same matrices are the parity check matrices of the three dual codes $\mathcal{E}_{\delta,m}$. Now, we show the rank and dimension of kernel of their corresponding $\mathbb{Z}_4$-linear codes:*

$$\begin{array}{ccc|ccc} k_{H_{1,5}} & = & 6 & r_{H_{1,5}} & = & 6 \\ k_{H_{2,5}} & = & 6 & r_{H_{2,5}} & = & 6 \\ k_{H_{3,5}} & = & 4 & r_{H_{3,5}} & = & 7 \\ \hline k_{E_{1,5}} & = & 20 & r_{E_{1,5}} & = & 27 \\ k_{E_{2,5}} & = & 16 & r_{E_{2,5}} & = & 28 \\ k_{E_{3,5}} & = & 14 & r_{E_{3,5}} & = & 29 \end{array}$$

It is proved that $H_{1,5}$ and $H_{2,5}$ are equivalent codes. Then, for $m = 5$ there are only two nonequivalent $\mathbb{Z}_4$-linear Hadamard codes and three nonequivalent $\mathbb{Z}_4$-linear extended 1-perfect codes.

The point is that the Gray map images of $\mathcal{H}_{1,5}$ and $\mathcal{H}_{2,5}$ are two $\mathbb{Z}_4$-linear equivalent codes but, the Gray map images of their dual codes $\mathcal{E}_{1,5}$ and $\mathcal{E}_{2,5}$ are nonequivalent. Observe that the quaternary dual operation is not preserving the nonequivalence of $\mathbb{Z}_4$-linear codes.

The next two theorems generalizes these classification results. Note that Theorem 6 was proved using the dimension of the kernel and Theorem 7 was proved using the rank.

Theorem 6 ([Kro01]) *For each $\delta \in \{1, \ldots, \lfloor (m-1)/2 \rfloor\}$ there exists a unique (up to equivalence) $\mathbb{Z}_4$-linear Hadamard code C of length $2^m \geq 16$, such that the code of C is of type $2^\gamma 4^\delta$ where $\gamma = m + 1 - 2\delta$.*

Theorem 7 ([Kro01]) *For each $\delta \in \{1, \ldots, \lfloor (m+1)/2 \rfloor\}$ there exists a unique (up to equivalence) $\mathbb{Z}_4$-linear extended 1-perfect code C of length $2^m \geq 16$, such that the $\mathbb{Z}_4$-dual code of C is of type $2^\gamma 4^\delta$ where $\gamma = m + 1 - 2\delta$.*

Chapter 3

Reed-Muller codes

In this chapter, the Reed-Muller codes will be explained. First of all, binary linear Reed-Muller codes and their parameters and properties will be presented. Then, we will talk about some families of quaternary linear Reed-Muller codes proposed in different papers trying to generalize the binary linear Reed-Muller family of codes. Finally, we will present the $\mathcal{RM}_s$ families of codes as a good generalization of the binary linear Reed-Muller codes.

3.1 Binary linear Reed-Muller codes

The usual binary linear Reed-Muller family of codes is one of the oldest interesting family of codes. The first construction of such codes was presented by Muller in [Mul54]. Later, the decoding algorithm was presented by Reed in [Ree54]. This family will be denoted by RM. The codes in this family are easy to decode and their combinatorial properties are of great interest to produce new optimal codes.

The binary linear *r*th-order Reed-Muller code $RM(r,m)$ with $0 \leq r \leq m$ and $m \geq 1$ can be described by using the Plotkin construction as follows [MS77]:

$$RM(r,m) \quad = \quad \{(u|u+v) : u \in RM(r,m-1),\, v \in RM(r-1,m-1)\},$$

where $RM(0,m)$ is the repetition code $\{\mathbf{0},\mathbf{1}\}$, $RM(m,m)$ is the universe code, and "|" denotes concatenation. For $m=1$, there are only two codes: the repetition code $RM(0,1)$

and the universe code $RM(1,1)$. For every code $RM(r,m)$, its generator matrix will be denoted by $G_{(r,m)}$. The codes in the $\mathcal{RM}$ family have the parameters and properties quoted in the following lemma.

Lemma 8 ([MS77]) *A binary linear* r*th-order Reed-Muller code $RM(r,m)$ with $m \geq 1$ and $0 \leq r \leq m$ has the following parameters and properties:*

1. *the length is $n = 2^m$;*
2. *the minimum distance is $d = 2^{m-r}$;*
3. *the dimension is $k = \sum_{i=0}^{r} \binom{m}{i}$;*
4. *the code $RM(r-1,m)$ is a subcode of $RM(r,m)$ for $0 < r \leq m$;*
5. *the code $RM(r,m)$ is the dual code of $RM(m-1-r,m)$ for $0 \leq r < m$.*

Example 5 *For $m = 2$, there are three binary linear Reed-Muller codes and the generator matrices $G_{(r,m)}$ are:*

$$G_{(0,2)} = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}; \quad G_{(1,2)} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}; \quad G_{(2,2)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

It is easy to check that these three codes satisfy all the parameters and properties quoted in Lemma 8.

3.2 New Plotkin constructions

One way to construct the RM family of codes is by using the Plotkin construction. In this subsection, two generalizations of the Plotkin construction over quaternary linear codes will be introduced.

Definition 9 (Plotkin Construction) *Let $\mathcal{A}$ and $\mathcal{B}$ be two quaternary linear codes of length n, types $2^{\gamma_{\mathcal{A}}}4^{\delta_{\mathcal{A}}}$ and $2^{\gamma_{\mathcal{B}}}4^{\delta_{\mathcal{B}}}$, and minimum distances $d_{\mathcal{A}}$ and $d_{\mathcal{B}}$, respectively. A new quaternary linear code $\mathcal{PC}(\mathcal{A},\mathcal{B})$ is defined as*

$$\mathcal{PC}(\mathcal{A},\mathcal{B}) = \{(u|u+v) : u \in \mathcal{A}, v \in \mathcal{B}\}.$$

It is easy to see that if $\mathcal{G}_{\mathcal{A}}$ and $\mathcal{G}_{\mathcal{B}}$ are generator matrices of $\mathcal{A}$ and $\mathcal{B}$, respectively, then the matrix

$$\mathcal{G}_{PC} = \left(\begin{array}{cc} \mathcal{G}_{\mathcal{A}} & \mathcal{G}_{\mathcal{A}} \\ 0 & \mathcal{G}_{\mathcal{B}} \end{array} \right)$$

is a generator matrix of the code $\mathcal{PC}(\mathcal{A},\mathcal{B})$. Moreover, the code $\mathcal{PC}(\mathcal{A},\mathcal{B})$ is of length $2n$, type $2^{\gamma_{\mathcal{A}}+\gamma_{\mathcal{B}}}4^{\delta_{\mathcal{A}}+\delta_{\mathcal{B}}}$, and minimum distance $d = \min\{2d_{\mathcal{A}}, d_{\mathcal{B}}\}$ [PRS07, PRS09].

Definition 10 (BQ-Plotkin Construction) *Let $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ be three quaternary linear codes of length n; types $2^{\gamma_{\mathcal{A}}}4^{\delta_{\mathcal{A}}}$, $2^{\gamma_{\mathcal{B}}}4^{\delta_{\mathcal{B}}}$, and $2^{\gamma_{\mathcal{C}}}4^{\delta_{\mathcal{C}}}$; and minimum distances $d_{\mathcal{A}}$, $d_{\mathcal{B}}$, and $d_{\mathcal{C}}$, respectively. Let $\mathcal{G}_{\mathcal{A}}$, $\mathcal{G}_{\mathcal{B}}$, and $\mathcal{G}_{\mathcal{C}}$ be generator matrices of the codes $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$, respectively. A new code $\mathcal{BQ}(\mathcal{A},\mathcal{B},\mathcal{C})$ is defined as the quaternary linear code generated by*

$$\mathcal{G}_{BQ} = \left(\begin{array}{cccc} \mathcal{G}_{\mathcal{A}} & \mathcal{G}_{\mathcal{A}} & \mathcal{G}_{\mathcal{A}} & \mathcal{G}_{\mathcal{A}} \\ 0 & \mathcal{G}'_{\mathcal{B}} & 2\mathcal{G}'_{\mathcal{B}} & 3\mathcal{G}'_{\mathcal{B}} \\ 0 & 0 & \hat{\mathcal{G}}_{\mathcal{B}} & \hat{\mathcal{G}}_{\mathcal{B}} \\ 0 & 0 & 0 & \mathcal{G}_{C} \end{array} \right),$$

where $\mathcal{G}'_{\mathcal{B}}$ is the matrix obtained from $\mathcal{G}_{\mathcal{B}}$ after switching twos by ones in their $\gamma_{\mathcal{B}}$ rows of order two, and $\hat{\mathcal{G}}_{\mathcal{B}}$ is the matrix obtained from $\mathcal{G}_{\mathcal{B}}$ after removing their $\gamma_{\mathcal{B}}$ rows of order two.

The code $\mathcal{BQ}(\mathcal{A},\mathcal{B},\mathcal{C})$ is of length $4n$, type $2^{\gamma_{\mathcal{A}}+\gamma_{\mathcal{C}}}4^{\delta_{\mathcal{A}}+\gamma_{\mathcal{B}}+2\delta_{\mathcal{B}}+\delta_{\mathcal{C}}}$, and minimum distance $d = \min\{4d_{\mathcal{A}}, 2d_{\mathcal{B}}, d_{\mathcal{C}}\}$ [PRS07, PRS09].

3.3 Quaternary linear Reed-Muller codes

In [HKC$^+$94], Hammons, Kumar, Calderbank, Sloane, and Solé showed that several families of binary codes are $\mathbb{Z}_4$-linear. In particular, they proved that the binary linear *r*th-order Reed-Muller code $RM(r,m)$ is $\mathbb{Z}_4$-linear for $r = 0, 1, 2, m-1, m$ and is not $\mathbb{Z}_4$-linear for $r = m-2$ $(m \geq 5)$. In a subsequent work, Hou, Lahtonen, and Koponen [HLK98] proved that $RM(r,m)$ is not $\mathbb{Z}_4$-linear for $3 \leq r \leq m-2$ $(m \geq 5)$.

In the recent literature [BFP05, BFCP08, HKC$^+$94, PR97a, Sol07, Wan97], several families of quaternary linear codes have been proposed and studied trying to generalize the RM family. However, when the corresponding $\mathbb{Z}_4$-linear codes are taken, they do not satisfy all the properties quoted in Lemma 8. Finally, in [PRS07, PRS09], new quaternary linear Reed-Muller families, denoted by $\mathcal{RM}_s$, such that the corresponding $\mathbb{Z}_4$-linear codes have the parameters and properties described in Lemma 8, were proposed.

Now, we will try to explain briefly the differences between all these quaternary Reed-Muller families trying to generalize the binary linear Reed-Muller codes. In [HKC$^+$94], a construction of codes, called $\mathcal{QRM}$ and based on $\mathbb{Z}_4$-linear codes, such that after doing modulo two we obtain the binary linear Reed-Muller codes is introduced. The code $\mathcal{QRM}(1,m)$ is a quaternary linear Kerdock code and its orthogonal code $\mathcal{QRM}(m-2,m)$ is a quaternary linear Preparata code. This result is generalized in [BFP05], where a class $\overline{\mathcal{QRM}(r,m)}$ of quaternary codes is described, which includes $\mathcal{QRM}(r,m)$ codes, as well as all the quaternary linear Kerdock and quaternary linear Preparata codes. In [BFP05, BFCP08] such family of codes is studied, and their parameters and the dimension of the kernel and rank are computed.

In [PR97a], a generalization of the Plotkin construction to construct a new family of Reed-Muller codes called $\mathcal{ARM}$ is introduced. In [Sol07], a Plotkin construction to obtain a sequence of quaternary linear Reed-Muller codes called $\mathcal{LRM}$ families is used. In both last quoted constructions, the images of the obtained codes under the Gray map are binary codes with the same parameters as the binary linear Reed-Muller codes. However, they do not satisfy the properties 4 and 5 quoted in Lemma 8.

It was a natural question to ask for the existence of families of quaternary linear codes such that, under the Gray map, the corresponding $\mathbb{Z}_4$-linear codes have the same parameters and properties as the well-known family of binary linear Reed-Muller codes. In these new families presented in [PRS07, PRS09], like in the usual $RM(r,m)$ family, the code with $r = 1$ has to be a Hadamard code and the code with $r = m-2$ has to be an extended 1-perfect code.

Let s, r, m be three integers such that $m \geq 2$, $0 \leq r \leq m$, and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$. The generator matrix $\mathcal{G}_{s(r,m)}$ of the quaternary linear rth-order Reed-Muller code of the family s denoted by $\mathcal{RM}_s(r,m)$ can be constructed in a recursive way by using the Plotkin construction given by Definition 9 as follows:

$$\mathcal{RM}_s(r,m) = \mathcal{PC}(\mathcal{RM}_s(r,m-1), \mathcal{RM}_s(r-1,m-1)),$$

where $\mathcal{RM}_s(r,m)$ with $r < 0$ is defined as the zero code, $\mathcal{RM}_s(0,m)$ is defined as the repetition code with only the all-zero and all-two vectors, and $\mathcal{RM}_s(r,m)$ with $r \geq m$ is defined as the whole space $\mathbb{Z}_4^{m-1}$. Moreover, for $m = 1$, there is only one family with $s = 0$, and in this family there are only the zero, repetition and universe codes for $r < 0$, $r = 0$ and $r > 0$, respectively. In this case, the generator matrix of $\mathcal{RM}_0(0,1)$ is $\mathcal{G}_{0(0,1)} = \begin{pmatrix} 2 \end{pmatrix}$ and the generator matrix of $\mathcal{RM}_0(1,1)$ is $\mathcal{G}_{0(1,1)} = \begin{pmatrix} 1 \end{pmatrix}$.

Example 6 *For $m = 2$, the generator matrices of $\mathcal{RM}_0(r,2)$, $0 \leq r \leq 2$, are the following:*

$$\mathcal{G}_{0(0,2)} = \begin{pmatrix} 2 & 2 \end{pmatrix}; \quad \mathcal{G}_{0(1,2)} = \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}; \quad \mathcal{G}_{0(2,2)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Note that when m is odd, the $\mathcal{RM}_s$ family with $s = \frac{m-1}{2}$ can not be generated by using this construction. The first time that a new family is generated, we will use the BQ-Plotkin construction instead of the Plotkin construction. In this case, for any $m \geq 3$ and odd, given $\mathcal{RM}_{s-1}(r,m-2)$, $\mathcal{RM}_{s-1}(r-1,m-2)$ and $\mathcal{RM}_{s-1}(r-2,m-2)$, the $\mathcal{RM}_s(r,m)$ code can be constructed by using the BQ-Plotkin construction given by Definition 10 as follows:

$$\mathcal{RM}_s(r,m) = \mathcal{BQ}(\mathcal{RM}_{s-1}(r,m-2), \mathcal{RM}_{s-1}(r-1,m-2), \mathcal{RM}_{s-1}(r-2,m-2)).$$

Example 7 *For $m = 3$, there are two families. The $\mathcal{RM}_0$ family can be generated by using the Plotkin construction. On the other hand, the new $\mathcal{RM}_1$ family has to be generated by*

Table 3.1: $\mathcal{RM}_s(r,m)$ codes: (γ,δ)

m	r s	0	1	2	3	4	5	6
1	0	(1,0)	(0,1)					
2	0	(1,0)	(1,1)	(0,2)				
3	0	(1,0)	(2,1)	(1,3)	(0,4)			
	1	(1,0)	(0,2)	(1,3)	(0,4)			
4	0	(1,0)	(3,1)	(3,4)	(1,7)	(0,8)		
	1	(1,0)	(1,2)	(1,5)	(1,7)	(0,8)		
5	0	(1,0)	(4,1)	(6,5)	(4,11)	(1,15)	(0,16)	
	1	(1,0)	(2,2)	(2,7)	(2,12)	(1,15)	(0,16)	
	2	(1,0)	(0,3)	(2,7)	(0,13)	(1,15)	(0,16)	
6	0	(1,0)	(5,1)	(10,6)	(10,16)	(5,26)	(1,31)	(0,32)
	1	(1,0)	(3,2)	(4,9)	(4,19)	(3,27)	(1,31)	(0,32)
	2	(1,0)	(1,3)	(2,10)	(2,20)	(1,28)	(1,31)	(0,32)

using the BQ-Plotkin construction. The generator matrices of $\mathcal{RM}_1(r,3)$, $0 \leq r \leq 3$, *are the following:*

$$\mathcal{G}_{1(0,3)} = \begin{pmatrix} 2 & 2 & 2 & 2 \end{pmatrix}; \quad \mathcal{G}_{1(1,3)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \end{pmatrix};$$

$$\mathcal{G}_{1(2,3)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}; \quad \mathcal{G}_{1(3,3)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Table 3.1 shows codes in the $\mathcal{RM}_s$ families for $1 \leq m \leq 6$. Each code is represented by (γ,δ), where $2^\gamma 4^\delta$ is the type of the code.

In [PRS07, PRS09], it is proved that these new families of quaternary linear Reed-Muller codes, denoted by $\mathcal{RM}_s$, satisfy that, under the Gray map, the corresponding $\mathbb{Z}_4$-linear codes have the same parameters and properties (length, dimension, minimum distance, inclusion and duality relationship) as the well known RM family. Contrary to the binary linear case, where there is only one RM family, in the quaternary case there are $\lfloor \frac{m+1}{2} \rfloor$ families for each value of m. These families will be distinguished by using subindexes s from the set $\{0, \ldots, \lfloor \frac{m-1}{2} \rfloor\}$.

Lemma 11 ([PRS07, PRS09]) *A quaternary linear Reed-Muller code $\mathcal{RM}_s(r, m)$, with $m \geq 1$, $0 \leq r \leq m$, and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$, has the following parameters and properties:*

1. *the binary length is $N = 2^m$;*
2. *the minimum distance is $d = 2^{m-r}$;*
3. *the number of codewords is 2^k, where $k = \sum_{i=0}^{r} \binom{m}{i}$;*
4. *the code $\mathcal{RM}_s(r-1, m)$ is a subcode of $\mathcal{RM}_s(r, m)$ for $0 < r \leq m$; The code $\mathcal{RM}_s(0, m)$ is the repetition code with only one nonzero codeword (the all-two vector). The code $\mathcal{RM}_s(m, m)$ is the whole space $\mathbb{Z}_4^{2^{m-1}}$ and $\mathcal{RM}_s(m-1, m)$ is the even code (i.e. the code with all the vectors of even weight);*
5. *the codes $\mathcal{RM}_s(1, m)$ and $\mathcal{RM}_s(m-2, m)$, after the Gray map, are $\mathbb{Z}_4$-linear Hadamard and $\mathbb{Z}_4$-linear extended perfect codes, respectively;*
6. *the code $\mathcal{RM}_s(r, m)$ is the dual code of $\mathcal{RM}_s(m-1-r, m)$ for $-1 \leq r \leq m$.*

All the contributions in this dissertation will be in the context of the $\mathcal{RM}_s$ families of Reed-Muller codes. Actually, different properties like the rank, the dimension of the kernel and the automorphism groups will be studied for such codes.

Chapter 4

Contributions

In this chapter, we summarize the results of the contributions making up this dissertation. Chapters 2 and 3 have already given a background that relates the articles appended to this document. However, we summarize it here, with the aim of justifying the thematic unity of this compendium.

The aforesaid contributions are the publications listed below.

(i) Pernas, J.; Pujol, J.; Villanueva, M., *Kernel Dimension for Some Families of Quaternary Reed-Muller Codes*. (MMICS) Lecture Notes in Computer Science, vol. 5393., pp: 128-141. ISSN: 0302-9743. December 2008.

(ii) Pernas, J.; Pujol, J.; Villanueva, M., *Rank for Some Families of Quaternary Reed-Muller Codes*. (18AAECC) Lecture Notes in Computer Science, vol. 5527., pp: 43-52. ISSN: 0302-9743. June 2009.

(iii) Pernas, J.; Pujol, J.; Villanueva, M., *Classification for Some Families of Quaternary Reed-Muller Codes*. IEEE Transactions on Information Theory, vol. 57, no. 9, pp. 6043–6051. September 2011.

(iv) Pernas, J.; Pujol, J.; Villanueva, M., *On the Permutation Automorphism Group of Quaternary Linear Hadamard Codes*. 3rd International Castle Meeting on Coding Theory and Applications, Servei de publicacions UAB, pp. 213-218. September 2011.

(v) Pernas, J.; Pujol, J.; Villanueva, M., *Characterization of the Automorphism Group o Quaternary Linear Hadamard Codes*. Accepted to Designs, Codes and Cryptography, February 2012.

Contributions (i), (ii) and (iv) are published in conference proceedings. Actually, contributions (i) and (ii) correspond to conferences in the CORE ranking scored as a C and B, respectively. Contribution (iii) is an article published in a journal with an impact factor of $2.73(Q1)$ in the JCR(2010). Contribution (v) is also an article accepted in a journal with an impact factor of $0.83(Q2)$ in the JCR(2010).

4.1 Classification of Reed-Muller Codes

In Section 3.3, the $\mathcal{RM}_s$ families of quaternary linear Reed-Muller codes are described. Remember that given $m \geq 1$ and $r \in \{0, \dots, m\}$, there is one code $\mathcal{RM}_s(r, m)$ for every $s \in \{0, \dots, \lfloor \frac{m-1}{2} \rfloor\}$. By Lemma 11, we know the parameters of these $\lfloor \frac{m+1}{2} \rfloor$ codes. The length is 2^m, the minimum distance is 2^{m-r}, and the number of codewords is 2^k, where $k = \sum_{i=0}^{r} \binom{m}{i}$. Given r and m, all the codes share the same parameters for every s. Although having the same parameters, the corresponding $\mathbb{Z}_4$-linear codes could be nonequivalent.

The aim of the publications (i), (ii) and (iii) is to give a full classification of the $\mathcal{RM}_s$ families of Reed-Muller codes. That is, to proof the nonequivalence of $\phi(\mathcal{RM}_s(r, m))$ codes for every $s \in \{0, \dots, \lfloor \frac{m-1}{2} \rfloor\}$. As it was done before with the $\mathbb{Z}_4$-linear Hadamard codes and $\mathbb{Z}_4$-linear extended 1-perfect codes (see Section 2.5), the rank and dimension of the kernel will help in giving this classification.

In Section 2.3, quaternary linear Hadamard codes and their construction are introduced. These Hadamard codes are included in the $\mathcal{RM}_s$ families. Indeed, the codes $\mathcal{RM}_s(1, m)$ are the quaternary linear Hadamard codes. As it is known, the quaternary dual code of a quaternary linear Hadamard code is a quaternary linear extended 1-perfect code. Thus, the codes $\mathcal{RM}_s(m-2, m)$ are the quaternary linear extended 1-perfect codes.

In [Kro01], the rank of the codes $\phi(\mathcal{RM}_s(1, m))$, where $m \geq 4$, is established. The author proved that the rank of the $\mathcal{RM}_0(1, m)$ and $\mathcal{RM}_1(1, m)$ are the same and they have different value for the rest of cases $s \in \{2, \dots, \lfloor \frac{m-1}{2} \rfloor\}$. Hence, the author claimed that there were $\lfloor\frac{m-1}{2}\rfloor$ nonequivalent $\mathbb{Z}_4$-linear Hadamard codes. In the same article [Kro01], the dimension of the kernel of the codes $\phi(\mathcal{RM}_s(m-2,m))$, where $m \geq 4$, is established too. The dimension of the kernel is different for every $s \in \{0,\dots,\lfloor\frac{m-1}{2}\rfloor\}$. Thus, the author claimed that there were $\lfloor\frac{m+1}{2}\rfloor$ nonequivalent $\mathbb{Z}_4$-linear extended 1-perfect codes. Contributions (i), (ii) and (iii) were motivated by these results and with the aim to complete the classification for the codes $\phi(\mathcal{RM}_s(r,m))$ where $m \geq 4$ and $r \in \{2,\dots,m-3\}$.

Contribution (i) represents the first study of the dimension of kernel of the $\mathcal{RM}_0(r,m)$ codes. When $s = 0$, there are no order four codewords in the generator matrix except the all-one codeword (see construction in Section 3.3). That fact makes easier to work with the family of codes $\mathcal{RM}_0$. Thus, in (i) we established the dimension of the kernel for the $\mathcal{RM}_0$ family of codes and we suggested that a generalization of the method used should work for rest of the $\mathcal{RM}_s$ families.

In Contribution (ii), we tried to compute the rank for all $\mathcal{RM}_s(r,m)$ families of codes. Our hope was that working with the rank could be easier than working with the kernel. However, it was even harder than the kernel, so we just established the rank for the codes $\mathcal{RM}_s(2,m)$ and $\mathcal{RM}_s(m-3,m)$ with $s \in \{2,\dots,\lfloor\frac{m-1}{2}\rfloor\}$. After that, we realized that we should go back to the computation of the dimension of the kernel.

Finally, in contribution (iii) we gave the full classification of the corresponding $\mathbb{Z}_4$-linear codes of the $\mathcal{RM}_s$ families of Reed-Muller codes. To solve the problem, we established the dimension of the kernel of every $\mathcal{RM}_s(r,m)$ code, where $m \geq 1$, $r \in \{0,\dots,m\}$, and $s \in \{0,\dots,\lfloor\frac{m-1}{2}\rfloor\}$. We realized that the method used in (i) was too complicated to be generalized for $s \in \{1,\dots,\lfloor\frac{m-1}{2}\rfloor\}$. Moreover, in [RR08] was proved that $\mathcal{RM}_0(r,m) = \mathcal{ZRM}^-(r,m-1)$. The $\mathcal{ZRM}^-(r,m-1)$ codes were introduced in [BFCP08] as well as their dimension of the kernel. Since the case $s = 0$ was indirectly solved then, we focused on the general case for $s \geq 1$ and finally we claimed Theorem 12, which establishes the value of the dimension of the kernel for each code. Table 4.1 shows the dimension of the kernel for all $\mathcal{RM}_s(r,m)$ codes with $m \leq 6$. Before claiming the full classification given by Theorem 13, it was necessary to prove that the cases where the dimension of the kernel are the same, the codes are equivalent.

Theorem 12 *For all $m \geq 1$, $r \in \{0,\dots,m\}$ and $s \in \{0,\dots,\lfloor\frac{m-1}{2}\rfloor\}$ the dimension of the kernel of $\mathcal{RM}_s(r,m)$ of type $2^\gamma 4^\delta$ is*

Table 4.1: Type $2^\gamma 4^\delta$ and dimension of the kernel $k_{s(r,m)}$ for all $\mathcal{RM}_s(r,m)$ codes with $m \leq 6$, showing them in the form (γ, δ) $k_{s(r,m)}$

m	s \ r	0	1	2	3	4	5	6
1	0	(1,0) 1	(0,1) 2					
2	0	(1,0) 1	(1,1) 3	(0,2) 4				
3	0	(1,0) 1	(2,1) 4	(1,3) 7	(0,4) 8			
	1	(1,0) 1	(0,2) 4	(1,3) 7	(0,4) 8			
4	0	(1,0) 1	(3,1) 5	(3,4) 11	(1,7) 15	(0,8) 16		
	1	(1,0) 1	(1,2) 5	(1,5) 8	(1,7) 15	(0,8) 16		
5	0	(1,0) 1	(4,1) 6	(6,5) 16	(4,11) 20	(1,15) 31	(0,16) 32	
	1	(1,0) 1	(2,2) 6	(2,7) 11	(2,12) 16	(1,15) 31	(0,16) 32	
	2	(1,0) 1	(0,3) 4	(2,7) 11	(0,13) 14	(1,15) 31	(0,16) 32	
6	0	(1,0) 1	(5,1) 7	(10,6) 22	(10,16) 32	(5,26) 37	(1,31) 63	(0,32) 64
	1	(1,0) 1	(3,2) 7	(4,9) 15	(4,19) 25	(3,27) 32	(1,31) 63	(0,32) 64
	2	(1,0) 1	(1,3) 5	(2,10) 13	(2,20) 23	(1,28) 30	(1,31) 63	(0,32) 64

1. $k_{s(0,m)} = 1$, $k_{s(m-1,m)} = 2^m - 1$, $k_{s(m,m)} = 2^m$.

2. If $s = 0$*,*

$$k_{0(r,m)} = \begin{cases} \gamma + 2\delta & \textit{for} \quad r = 1 \\ \gamma + \delta + m & \textit{for} \quad r \in \{2, \dots, m-2\}. \end{cases}$$

3. If $s = 1$*,* $k_{1(r,m)} = \gamma + \delta + 2$ *for* $r \in \{1, 2, \dots, m-2\}$*.*

4. If $s \geq 2$*,* $k_{s(r,m)} = \gamma + \delta + 1$ *for* $r \in \{1, 2, \dots, m-2\}$*, except* $k_{2(2,5)} = \gamma + \delta + 2 = 11$*.*

Theorem 13 *For all* $m \geq 3$ *and* $r = 1$*, there are at least* $\lfloor \frac{m-1}{2} \rfloor$ *nonequivalent binary codes with the same parameters as the code* $RM(1,m)$*.*

For all $m \geq 4$ *and* $2 \leq r \leq m-2$*, there are at least* $\lfloor \frac{m+1}{2} \rfloor$ *nonequivalent binary codes with the same parameters as the code* $RM(r,m)$*, except when* m *is odd, and* r *is even. In this case, there are at least* $\frac{m-1}{2}$ *nonequivalent binary codes with the same parameters as the code* $RM(r,m)$*.*

4.2 Permutation automorphism groups

The vector spaces considered in coding theory usually have both metrical and algebraic structures. From the point of view of the parameters of an error-correcting code, the metrical one is the most important, while the algebraic properties give an advantage in constructing codes, developing coding and decoding algorithms, and other applications. In this section, we will talk about these algebraic properties of codes, the permutation automorphism group of a quaternary linear code. Actually, in contributions (iv) and (v), we characterized the permutation automorphism group of the $\mathcal{RM}_s(1,m)$ and $\mathcal{RM}_s(m-2,m)$ codes.

Recall the definition of the permutation automorphism group of a quaternary linear code given in Section 2.4:

$$\text{PAut}(\mathcal{C}) = \{\sigma \in S_n : \sigma(\mathcal{C}) = \mathcal{C}\},$$

where $\mathcal{C}$ is a quaternary linear code and S_n the symmetric group on a set of n symbols.

The order of the group $\mathrm{PAut}(\mathcal{C})$ is an invariant of the code $\mathcal{C}$. Thus, knowing this group order could be used for classification purposes like the dimension of the kernel or the rank. The permutation automorphism group gives a lot of information of the code. It can help to establish metrical properties, like the weight distribution, or it can be useful in some other practical goals like in the decoding algorithms.

In the literature, we can find several studies of the permutation automorphism groups for some known binary codes. The permutation automorphism group of $\mathbb{Z}_2\mathbb{Z}_4$-linear extended 1-perfect codes, which include the $\mathbb{Z}_4$-linear extended 1-perfect codes, was studied in [Kro11]. Moreover, the permutation automorphism group of the span of the same codes was studied in [PR02]. In general, the permutation automorphism group of (nonlinear) binary 1-perfect codes has also been studied before, obtaining some partial results [HPW09, Hed05, ASH05, FCPV11]. Note that all these results are focused on the permutation automorphism groups of binary codes. Our work is focused on the permutation automorphism group of a quaternary linear code despite the code could be seen as a binary code under the Gray map.

Initially, we had considered to study the permutation automorphism group of all the families of quaternary linear Reed-Muller codes $\mathcal{RM}_s$ presented in Chapter 3. Quickly, we realized that it would be better to start with the $\mathcal{RM}_s(1,m)$ and $\mathcal{RM}_s(m-2,m)$ codes. Since the permutation automorphism group of the dual code is the same as the original code, we studied both cases at once. Recall that $\mathcal{RM}_s(1,m)$ are the quaternary linear Hadamard codes and the $\mathcal{RM}_s(m-2,m)$ are the quaternary linear extended 1-perfect codes. Both codes are described in Section 2.3.

In order to study the permutation automorphism group of the $\mathcal{RM}_s(1,m)$, we have computed them for some fixed s and m using an algorithm presented in [Feu09]. Contribution (iv) is an extended abstract presented at the International Castle Meeting on Coding Theory and Applications in 2011. The main result was to establish the order of the permutation automorphism groups for the Hadamard codes $\mathcal{RM}_s(1,m)$ and their duals $\mathcal{RM}_s(m-2,m)$. In (iv), there is a sketch of the proof for the order of that group. Looking for a characterization of the $\mathrm{PAut}(\mathcal{RM}_s(1,m))$ we obtained a classification of its codewords by computing the orbits of their action on $\mathcal{RM}_s(1,m)$.

Finally, in contribution (v), the results about the order of the permutation automorphism group of the quaternary linear Hadamard codes are proved. Moreover, the groups are completely characterized by giving a method to describe the generators of the group. Theorem 14 and Corollary 15 give the order of these groups, and Table 4.2 shows some examples.

Theorem 14 *Let $\mathcal{H}_{s,m}$ be the quaternary linear Hadamard code of length $n = 2^{m-1}$, where $m \geq 1$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$. The order of the permutation automorphism group $P_{s,m} = \mathrm{PAut}(\mathcal{H}_{s,m})$ is*

(i) $|P_{0,1}| = 1$;

(ii) $|P_{s,m}| = |P_{s-1,m-2}| \cdot 4^{s-1} \cdot (2^{2s+2} - 2^{s+2})$, *if* $m = 2s+1$, $s \geq 1$;

(iii) $|P_{s,m}| = |P_{s,m-1}| \cdot 2^{m-s-2} \cdot (2^{m-s} - 2^{s+1})$, *if* $m > 2s+1$, $s \geq 0$.

Corollary 15 *Let $\mathcal{H}_{s,m}$ be the quaternary linear Hadamard code of length $n = 2^{m-1}$, where $m \geq 1$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$. Let $\mathcal{E}_{s,m} = \mathcal{H}_{s,m}^{\perp}$ be its quaternary dual code, which is a quaternary linear extended 1-perfect code. Then,* $\mathrm{PAut}(\mathcal{H}_{s,m}) = \mathrm{PAut}(\mathcal{E}_{s,m})$.

Table 4.2: Order of $P_{s,m} = \mathrm{PAut}(\mathcal{H}_{s,m})$ for $1 \leq m \leq 8$.

m s	1	2	3	4	5	6	7	8
0	1	2	$2^3 \cdot 3$	$2^6 \cdot 3 \cdot 7$	$2^{10} \cdot 3 \cdot 7 \cdot 15$	$\dots$	$\dots$	$\dots$
1			2^3	2^6	$2^{10} \cdot 3$	$2^{15} \cdot 3 \cdot 7$	$2^{21} \cdot 3 \cdot 7 \cdot 15$	$\dots$
2					$2^9 \cdot 3$	$2^{14} \cdot 3$	$2^{20} \cdot 3^2$	$2^{27} \cdot 3^2 \cdot 7$
3							$2^{18} \cdot 3 \cdot 7$	$2^{25} \cdot 3 \cdot 7$

4.3 MAGMA implementation

MAGMA is a software package designed to solve computationally hard problems in algebra, number theory, geometry and combinatorics. Currently, it supports the basic facilities for linear codes over integer residue rings and Galois rings (see [CB94]), including additional functionality for the special case of codes over $\mathbb{Z}_4$, or equivalently quaternary linear codes.

New functions that expand the current functionality for codes over $\mathbb{Z}_4$ have been developed as a contribution of this dissertation. Since the MAGMA version $2.15 - 15$, version 1.2 of this package is included by default and it is not necessary to be installed. However, the latest version 1.4 can be downloaded from `http://www.ccg.uab.cat` as well as its reference manual [PPV12b].

The functions included in the developed package expand the current functionality for codes over $\mathbb{Z}_4$ in MAGMA. Specifically, there are functions which give new constructions for some families ($\mathcal{RM}_s$, $\mathcal{LRM}$) of codes over $\mathbb{Z}_4$ and constructions to obtain new codes over $\mathbb{Z}_4$ from given codes over $\mathbb{Z}_4$ (Chapter 3). Moreover, efficient functions for computing the rank and dimension of the kernel of any code over $\mathbb{Z}_4$ are also included, as well as general functions to compute the coset leaders for a subcode in a code over $\mathbb{Z}_4$. Finally, there are also functions to compute the permutation automorphism group for Hadamard and extended 1-perfect codes over $\mathbb{Z}_4$, and their cardinal.

Chapter 5

Conclusion

5.1 Summary

Coding theory was introduced in [Sha48] in order to provide reliability in communications. The discipline was born with the aim to solve an engineering problem using an important mathematical background. Sometimes it is difficult to know if you are doing coding theory or pathological mathematics. The study of the apparently useless mathematical objects is more than enough to make me happy. Moreover, when you ask for the "utility" concept in the research context, it becomes fuzzy. I am sure that the study of the automorphism group of some combinatorial objects will not change the world, but it has changed me. And I think that it was the most important goal of the PhD.

This dissertation was developed as a compendium of publications. That means that other people, who are experts in this area, found interesting the presented results. This system is a good metric for "utility". Maybe it is not the best since, a priori, lots of experts can be wrong about what is interesting or not. However, the learning process has not finished with the PhD and thus, all together we will improve this "utility" metric.

The results presented in this dissertation are all included in the scope of quaternary linear Reed-Muller codes $\mathcal{RM}_s$. We can separate them in three blocks.

First of all, we established the dimension of the kernel for every code $\mathcal{RM}_s(r,m)$, where $m \geq 1$, $r \in \{0,\dots,m\}$ and $s \in \{0,\dots,\lfloor\frac{m-1}{2}\rfloor\}$, included in the $\mathcal{RM}_s$ families. We also studied the rank of $\mathcal{RM}_s(2,m)$ and $\mathcal{RM}_s(m-3,m)$ codes. Using the results of the dimension of the kernel, the corresponding $\mathbb{Z}_4$-linear codes to the $\mathcal{RM}_s$ families were classified up to code equivalence. These results can be found in [PPV08, PPV09, PPV11a].

The second part is about the permutation automorphism group of quaternary linear Hadamard codes and quaternary linear extended 1-perfect codes. These codes are included in the $\mathcal{RM}_s$ families. They are the $\mathcal{RM}_s(1, m)$ and $\mathcal{RM}_s(m-2, m)$ codes, respectively. Actually, we established the order and the generators of their permutation automorphism groups. We also studied the structure of such codes, since we classified their codewords into orbits on the action of its permutation automorphism group. These contributions can be found in [PPV11b, PPV12a].

Finally, we implemented a package, which is included by default in MAGMA software. This package gives a collection of functions to work with quaternary linear codes. We implemented functions to construct the $\mathcal{RM}_s$ families as well as other quaternary linear Reed-Muller families like $\mathcal{LRM}$. Moreover, there are efficient functions to compute the rank and the kernel of a quaternary code. You can also find functions to compute the permutation automorphism group for quaternary Hadamard and extended 1-perfect codes, and their cardinal.

5.2 Future Research

In this section, we point out some open problems that derive from this dissertation and deserve further investigation.

First of all, it would be interesting to give a classification of the families of $\mathbb{Z}_2\mathbb{Z}_4$-linear Reed-Muller codes introduced in [PRR09] by computing the rank or the dimension of the kernel, just as it was done in this dissertation for the $\mathbb{Z}_4$-linear Reed-Muller codes. Also related to these families of $\mathbb{Z}_2\mathbb{Z}_4$-linear Reed-Muller codes, it would be interesting to develop a MAGMA package providing the tools to construct them.

Another open problem is to complete the permutation automorphism group of all codes in the $\mathcal{RM}_s$ families. It does not seem easy to solve. To establish the group for the Hadamard case, we used the highly regular structure of the code. The same technique could be very painful for the general case. Moreover, the studied permutation automorphism group could be extended to the monomial automorphism group. Remember that the

$\mathrm{PAut}(\mathcal{C})$ is a subgroup of $\mathrm{MAut}(\mathcal{C})$. Finally, it could be interesting to study the relation between the $\mathrm{MAut}(\mathcal{C})$ and $\mathrm{PAut}(\phi(\mathcal{C}))$.

Bibliography

[ASH05] S. V. Avgustinovich, F. I. Solov' eva, and O. Heden. On the structure of symmetry groups of vasil' ev codes. *Advances in Mathematics of Communications*, 41(2):105–112, 2005.

[BFCP08] J. Borges, C. Fernandez-Cordoba, and K.T. Phelps. $\mathcal{ZRM}$ codes. *IEEE T. Inform. Theory.*, 54(1):380–386, Jan. 2008.

[BFCP$^+$10] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. Villanueva. $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality. *Designs, Codes and Cryptography*, 54(2):167–179, 2010.

[BFP05] J. Borges, C. Fernandez, and K.T. Phelps. Quaternary Reed-Muller codes. *IEEE T. Inform. Theory.*, 51(7):2686–2691, July 2005.

[BPR03] J. Borges, K.T. Phelps, and J. Rifà. The rank and kernel of extended 1-perfect $\mathbb{Z}_4$-linear and additive non $\mathbb{Z}_4$-linear codes. *IEEE Transactions on Information Theory*, 49(8):2028–2034, 2003.

[Cam99] P. Cameron. *Permutation Groups*. Cambridge University Press, 1999.

[CB94] J. Cannon and W. Bosma. *Handbook of Magma Functions*. University of Sydney Press, Sydney, Australia, 1994.

[Del73] P. Delsarte. Four fundamental parameter of a code and their combinatorial significance. *Information and Control*, 23:407–438, 1973.

[FCPV08] C. Fernandez-Cordoba, J. Pujol, and M. Villanueva. On rank and kernel of $\mathbb{Z}_4$-linear codes. *Lecture Notes in Computer Science*, 5228:46–55, 2008.

[FCPV10] C. Fernandez-Cordoba, J. Pujol, and M. Villanueva. $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel. *Designs, Codes and Cryptography*, 56(1):43–59, 2010.

[FCPV11] C. Fernandez-Cordoba, K.T. Phelps, and M. Villanueva. Involutions in binary perfect codes. *IEEE Transactions on Information Theory*, 57(9):5926–5931, 2011.

[Feu09] T. Feulner. The automorphism groups of linear codes and canonical representatives of their semilinear isometry classes. *Advances in Mathematics of Communications*, 3(4):363–383, 2009.

[Hed05] O. Heden. On the symmetry group of perfect 1-error correcting binary codes. *J. Combin. Math. Comput.*, 52:109–115, 2005.

[HKC$^+$94] A Hammons, P.V. Kumar, A.R. Calderbank, N.J.A Sloane, and P. Solé. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes. *IEEE Transactions on Information Theory*, 40:301–319, 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*, 44:798–799, 1998.

[HPW09] O. Heden, F. Pasticci, and T. Westerbäck. On the existence of extended perfect binary codes with trivial symmetry group. *Advances in Mathematics of Communications*, 3(3):295–309, 2009.

[Kro01] D.S. Krotov. $\mathbb{Z}_4$-linear Hadamard and extended perfect codes. In *International Workshop on Coding and Cryptography*, volume 8-12, pages 329–334, Paris, France, January 2001.

[Kro11] D.S. Krotov. On the Automorphism Groups of the Additive 1-Perfect Binary Codes. In M. Villanueva and J. Borges, editors, *3rd International Castle Meeting on Coding Theory and Applications*, pages 171–176, Cardona, Spain, September 2011.

[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*, 3:6–12, 1954.

[Nec89] A. A. Nechaev. Kerdock codes in a cyclic form. *Discrete Mathematics*, 1(4):123–139, 1989.

[PHB98] V. S. Pless, W. C. Huffman, and R. A. Brualdi. *Handbook of Coding Theory : Volume I.* North-Holland, 1998.

[PPV08] J. Pernas, J. Pujol, and M. Villanueva. Kernel dimension for some families of quaternary Reed-Muller codes. *Lecture Notes in Computer Science (MMICS)*, 5393:128–141, December 2008.

[PPV09] J. Pernas, J. Pujol, and M. Villanueva. Rank for some families of quaternary Reed-Muller codes. *Lecture Notes in Computer Science (18AAECC)*, 5527:43–52, June 2009.

[PPV11a] J. Pernas, J. Pujol, and M. Villanueva. Classification for some families of quaternary Reed-Muller codes. *IEEE Transactions on Information Theory*, 57(9):6043–6051, September 2011.

[PPV11b] J. Pernas, J. Pujol, and M. Villanueva. On the permutation automorphism group of quaternary linear Hadamard codes. *3rd International Castle Meeting on Coding Theory and Applications*, pages 213–218, September 2011.

[PPV12a] J. Pernas, J. Pujol, and M. Villanueva. Characterization of the automorphism group o quaternary linear Hadamard codes. *to apper in Designs, Codes and Cryptography*, 2012.

[PPV12b] J. Pernas, J. Pujol, and M. Villanueva. *Codes Over $\mathbb{Z}_4$. A Magma Package. v1.4.* Universitat Autònoma de Barcelona, Bellaterra, Spain, 2012.

[PR97a] J. Pujol and J. Rifà. Additive Reed-Muller codes. In *IEEE International Symposium on Information Theory*, page 508, Ulm, Germany, 1997.

[PR97b] J. Pujol and J. Rifà. Translation-invariant propelinear codes. *IEEE Transactions on Information Theory*, 43(2):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(9):2587–2592, 2002.

[PRR09] J. Pujol, J. Rifà, and L. Ronquillo. Construction of Additive Reed-Muller Codes. *Lecture Notes in Computer Science (18AAECC)*, 5527:223–226, June 2009.

[PRS07] J. Pujol, J. Rifà, and F. I. Solov'eva. Quaternary Plotkin constructions and Quaternary Reed-Muller codes. *Lecture Notes in Computer Science*, 4851:148–157, 2007.

[PRS09] J. Pujol, J. Rifà, and F. I. Solov'eva. Construction of $\mathbb{Z}_4$-linear Reed-Muller codes. *IEEE Transactions on Information Theory*, 55(1):99–104, 2009.

[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.

[RBH89] J. Rifà, J. M. Basart, and L. Huguet. On completely regular propelinear codes. In *6th International Conference, AAECC-6*, volume 357, pages 341–355, 1989.

[Ree54] I.S. Reed. A class of multiple-error-correcting codes and the decoding schemes. *IRE Transactions on Information Theory*, 4:38–49, 1954.

[RR08] J. Rifà and L. Ronquillo. About the $\mathbb{Z}_4$-linear Reed-Muller $ZRM^{-}(r, m-1)$ and $RM_s(r, m)$ codes. In *VI Jornadas de Matemática Discreta y Algorítmica*, pages 517–526, Lleida, July 2008.

[Sha48] C.E. Shannon. A mathematical theory of communication. *Bell system technical journal*, 27, 1948.

[Sol07] F.I. Solov'eva. On $\mathbb{Z}_4$-linear codes with the parameters of Reed-Muller codes. *Problems of Information Transmission*, 43(1):26–32, 2007.

[Tie73] A. Tietäväinen. On the nonexistence of perfect codes over finite fields. *SIAM J. Appl. Math.*, 24:88–96, 1973.

[Wan97] Z.-X. Wan. *Quaternary Codes*. World Scientific, 1997.

[ZL73] V. A. Zinov'ev and V. K. Leont'ev. The nonexistence of perfect codes over Galois fields. *Probl. Control and Inform. Theory*, 2:123–132, 1973. (in Russian).

Appendices

Appendix A

Kernel Dimension for Some Families of Quaternary Reed-Muller codes

Kernel Dimension for Some Families of Quaternary Reed-Muller Codes*

J. Pernas, J. Pujol, and M. Villanueva

Dept. of Information and Communications Engineering,
Universitat Autònoma de Barcelona, Spain
{jaume.pernas,jaume.pujol,merce.villanueva}@autonoma.edu

Abstract. Recently, new families of quaternary linear Reed-Muller codes such that, after the Gray map, the corresponding $\mathbb{Z}_4$-linear codes have the same parameters and properties as the codes in the usual binary linear Reed-Muller family have been introduced. A structural invariant, the kernel dimension, for binary codes can be used to classify these $\mathbb{Z}_4$-linear codes. The kernel dimension for these $\mathbb{Z}_4$-linear codes is established generalizing the known results about the kernel dimension for $\mathbb{Z}_4$-linear Hadamard and $\mathbb{Z}_4$-linear extended 1-perfect codes.

Keywords: Kernel dimension, quaternary codes, Reed-Muller codes, $\mathbb{Z}_4$-linear codes.

1 Introduction

Let $\mathbb{Z}_2$ and $\mathbb{Z}_4$ be the ring of integers modulo 2 and modulo 4, respectively. Let $\mathbb{Z}_2^n$ be the set of all binary vectors of length n and let $\mathbb{Z}_4^n$ be the set of all quaternary vectors of length n. Any nonempty subset C of $\mathbb{Z}_2^n$ is a binary code and a subgroup of $\mathbb{Z}_2^n$ is called a *binary linear code* or a $\mathbb{Z}_2$*-linear code.* Equivalently, any nonempty subset $\mathcal{C}$ of $\mathbb{Z}_4^n$ is a quaternary code and a subgroup of $\mathbb{Z}_4^n$ is called a *quaternary linear code.*

The *Hamming distance* $d_H(u,v)$ between two vectors $u,v \in \mathbb{Z}_2^n$ is the number of coordinates in which u and v differ. The *Hamming weight* of a vector $u \in \mathbb{Z}_2^n$, denoted by $w_H(u)$, is the number of nonzero coordinates of u. The *minimum Hamming distance* of a binary code C is the minimum value of $d_H(u,v)$ for $u,v \in C$ satisfying $u \neq v$. The *minimum Hamming weight* of a binary code C, denoted by $w_{min}(C)$, is the minimum value of $w_H(u)$, for $u \in C \setminus \{0\}$.

We define the *Lee weights* over the elements in $\mathbb{Z}_4$ as: $w_L(0) = 0$, $w_L(1) = w_L(3) = 1$, $w_L(2) = 2$. The *Lee weight* of a vector $u \in \mathbb{Z}_4^n$, denoted by $w_L(u)$, is the addition of the weights of its coordinates, whereas the *Lee distance* $d_L(u,v)$ between two vectors $u,v \in \mathbb{Z}_4^n$ is $d_L(u,v) = w_L(u-v)$. The *minimum Lee distance* of a quaternary code $\mathcal{C}$ is the minimum value of $d_L(u,v)$ for $u,v \in \mathcal{C}$ satisfying $u \neq v$. The *minimum Lee weight* of a quaternary code $\mathcal{C}$, denoted by $w_{min}(\mathcal{C})$, is the minimum value of $w_L(0,u)$, for $u \in \mathcal{C} \setminus \{0\}$.

* This work was supported in part by the Spanish MEC and the European FEDER under Grant MTM2006-03250.

J. Calmet, W. Geiselmann, J. Müller-Quade (Eds.): Beth Festschrift, LNCS 5393, pp. 128–141, 2008.

The Gray map, $\phi : \mathbb{Z}_4^n \longrightarrow \mathbb{Z}_2^{2n}$ given by $\phi(v_1, \dots, v_n) = (\varphi(v_1), \dots, \varphi(v_n))$ where $\varphi(0) = (0,0)$, $\varphi(1) = (0,1)$, $\varphi(2) = (1,1)$, $\varphi(3) = (1,0)$, is an isometry which transforms Lee distances defined in a quaternary code $\mathcal{C}$ over $\mathbb{Z}_4^n$ to Hamming distances defined in the corresponding binary code $C = \phi(\mathcal{C})$. Therefore, $w_{min}(\mathcal{C}) = w_{min}(C)$. Note that the binary length of the binary code C is $N = 2n$.

Let $\mathcal{C}$ be a quaternary linear code. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$, it is isomorphic to an abelian structure $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, $\mathcal{C}$ is of type $2^\gamma 4^\delta$ as a group, it has $|\mathcal{C}| = 2^{\gamma+2\delta}$ codewords and $2^{\gamma+\delta}$ codewords of order two. Moreover, the binary image $C = \phi(\mathcal{C})$ of any quaternary linear code $\mathcal{C}$ of length n and type $2^\gamma 4^\delta$ is called a $\mathbb{Z}_4$-*linear code* of binary length $N = 2n$ and type $2^\gamma 4^\delta$.

Two binary codes C_1 and C_2 of length n are said to be *isomorphic* if there is a coordinate permutation π such that $C_2 = \{\pi(c) \ : \ c \in C_1\}$. They are said to be *equivalent* if there is a vector $a \in \mathbb{Z}_2^n$ and a coordinate permutation π such that $C_2 = \{a + \pi(c) \ : \ c \in C_1\}$ [14]. Two quaternary linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ both of length n and type $2^\gamma 4^\delta$ are said to be *monomially equivalent*, if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. They are said to be *permutation equivalent* if they differ only by a permutation of coordinates [12]. Note that if two quaternary linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are monomially equivalent, then the corresponding $\mathbb{Z}_4$-linear codes $C_1 = \phi(\mathcal{C}_1)$ and $C_2 = \phi(\mathcal{C}_2)$ are isomorphic.

Two structural invariants for binary codes are the rank and dimension of the kernel. The *rank* of a binary code C, denoted by r_C, is simply the dimension of $\langle C \rangle$, which is the linear span of the codewords of C. The *kernel* of a binary code C, denoted by $K(C)$, is the set of vectors that leave C invariant under translation, i.e. $K(C) = \{x \in \mathbb{Z}_2^n \ : \ C + x = C\}$. If C contains the all-zero vector, then $K(C)$ is a binary linear subcode of C. In general, C can be written as the union of cosets of $K(C)$, and $K(C)$ is the largest such linear code for which this is true [1]. The dimension of the kernel of C will be denoted by k_C.

These two invariants do not give a full classification of binary codes, since two nonequivalent binary codes could have the same rank and dimension of the kernel. In spite of that, they can help in classification, since if two binary codes have different ranks or dimensions of the kernel, they are nonequivalent.

In [10], Hammons et al. showed that several families of binary codes are $\mathbb{Z}_4$-linear. In particular, they considered the binary linear Reed-Muller family of codes, denoted by RM, and proved that the binary linear rth-order Reed-Muller code $RM(r,m)$ of length 2^m is $\mathbb{Z}_4$-linear for $r = 0, 1, 2, m-1, m$ and is not $\mathbb{Z}_4$-linear for $r = m-2$ $(m \geq 5)$. In a subsequent work [11], Hou et al. proved that $RM(r,m)$ is not $\mathbb{Z}_4$-linear for $3 \leq r \leq m-2$ $(m \geq 5)$.

It is well-known that an easy way to built the binary linear Reed-Muller family of codes RM is using the Plotkin construction [14]. In [16],[17], new quaternary Plotkin constructions were introduced to build new families of quaternary linear Reed-Muller codes, denoted by $\mathcal{RM}_s$. The quaternary linear Reed-Muller codes $\mathcal{RM}_s(r,m)$ of length 2^{m-1}, for $m \geq 1$, $0 \leq r \leq m$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$, in these new families satisfy that the corresponding $\mathbb{Z}_4$-linear codes have the same parameters and properties (length, dimension, minimum distance, inclusion and duality relationship) as the binary linear codes in the well-known RM family. Contrary to the binary linear case, where there is only one family, in the quaternary case there are $\lfloor \frac{m+1}{2} \rfloor$ families for each value of m. These families will be distinguished using subindexes s from the set $\{0, \ldots, \lfloor \frac{m-1}{2} \rfloor\}$.

The dimension of the kernel and rank have been studied for some families of $\mathbb{Z}_4$-linear codes [2],[5],[6],[13],[15]. In the RM family, the $RM(1,m)$ and $RM(m-2,m)$ binary codes are a linear Hadamard and extended 1-perfect code, respectively. Recall that a Hadamard code of length $n = 2^m$ is a binary code with $2n$ codewords and minimum Hamming distance $n/2$, and an extended 1-perfect code of length $n = 2^m$ is a binary code with 2^{n-m} codewords and minimum Hamming distance 4. Equivalently, in the $\mathcal{RM}_s$ families, the corresponding $\mathbb{Z}_4$-linear code of any $\mathcal{RM}_s(1,m)$ and $\mathcal{RM}_s(m-2,m)$ is a Hadamard and extended 1-perfect code, respectively [16],[17]. For the corresponding $\mathbb{Z}_4$-linear codes of $\mathcal{RM}_s(1,m)$ and $\mathcal{RM}_s(m-2,m)$, the rank and kernel dimension were studied and computed in [6],[13],[15]. Specifically,

$$k_H = \begin{cases} \gamma + \delta + 1 & \text{if } s \geq 2 \\ \gamma + 2\delta & \text{if } s = 0,1 \end{cases} \quad \text{and} \quad k_P = \begin{cases} \bar{\gamma} + \bar{\delta} + 1 & \text{if } s \geq 2 \\ \bar{\gamma} + \bar{\delta} + 2 & \text{if } s = 1 \\ \bar{\gamma} + \bar{\delta} + m & \text{if } s = 0. \end{cases}, \qquad (1)$$

where $H = \phi(\mathcal{RM}_s(1,m))$ of type $2^\gamma 4^\delta$ and $P = \phi(\mathcal{RM}_s(m-2,m))$ of type $2^{\bar{\gamma}} 4^{\bar{\delta}}$.

The aim of this paper is the study of the dimension of the kernel for the quaternary linear Reed-Muller families of codes $\mathcal{RM}_s$, generalizing the known results about the kernel dimension for the $\mathcal{RM}_s(1,m)$ and $\mathcal{RM}_s(m-2,m)$ codes. The paper is organized as follows. In Section 2, we recall some properties related to quaternary linear codes and the kernel of these codes. Moreover, we describe the construction of the $\mathcal{RM}_s$ families of codes. In Section 3, we establish the dimension of the kernel for all codes in the $\mathcal{RM}_s$ family with $s = 0$. In Section 4, we give the main results about the kernel dimension for all the $\mathcal{RM}_s$ families. Finally, the conclusions are given in Section 5.

Magma is a software package designed to solve computationally hard problems in algebra, number theory, geometry and combinatorics. Currently it supports the basic facilities for linear codes over integer residue rings and Galois rings (see [7]), including additional functionality for the special case of codes over $\mathbb{Z}_4$, or equivalently quaternary linear codes. New functions that expand the current functionality for codes over $\mathbb{Z}_4$ have been developed by the authors as a new package. Specifically, these functions allow to construct the $\mathcal{RM}_s$ families and some Plotkin constructions for quaternary linear codes. Moreover, efficient functions for computing the rank and dimension of the kernel of any quaternary linear code are included. A beta version of this new package and the manual with the description of all functions can be downloaded from the web page `http://www.ccg.uab.cat`.

2 Preliminaries

2.1 Quaternary Linear Codes

Let $\mathcal{C}$ be a quaternary linear code of length n and type $2^\gamma 4^\delta$. Although $\mathcal{C}$ is not a free module, every codeword is uniquely expressible in the form

$$\sum_{i=1}^{\gamma} \lambda_i u_i + \sum_{j=1}^{\delta} \mu_j v_j,$$

where $\lambda_i \in \mathbb{Z}_2$ for $1 \leq i \leq \gamma$, $\mu_j \in \mathbb{Z}_4$ for $1 \leq j \leq \delta$ and u_i, v_j are vectors in $\mathbb{Z}_4^n$ of order two and four, respectively. The vectors u_i, v_j give us a generator matrix $\mathcal{G}$ of size $(\gamma+\delta) \times n$ for the code $\mathcal{C}$. Moreover, $\mathcal{G}$ will also be used to denote the set of all vectors u_i, v_j.

In [10], it was shown that any quaternary linear code of type $2^\gamma 4^\delta$ is permutation equivalent to a quaternary linear code with a canonical generator matrix of the form

$$\begin{pmatrix} 2T & 2I_\gamma & \mathbf{0} \\ S & R & I_\delta \end{pmatrix},$$

where R, T are matrices over $\mathbb{Z}_2$ of size $\delta \times \gamma$ and $\gamma \times (n-\gamma-\delta)$, respectively; and S is a matrix over $\mathbb{Z}_4$ of size $\delta \times (n-\gamma-\delta)$.

The concepts of duality for quaternary linear codes were also studied in [10], where the inner product for any two vectors $u, v \in \mathbb{Z}_4^n$ is defined as

$$u \cdot v = \sum_{i=1}^{n} u_i v_i \in \mathbb{Z}_4.$$

Then, the *dual code* of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined in the standard way

$$\mathcal{C}^\perp = \{v \in \mathbb{Z}_4^n \ : \ u \cdot v = 0 \text{ for all } u \in \mathcal{C}\}.$$

The corresponding binary code $\phi(\mathcal{C}^\perp)$ is denoted by $C_\perp$ and called the $\mathbb{Z}_4$-*dual code* of C. Moreover, the dual code $\mathcal{C}^\perp$, which is also a quaternary linear code, is of type $2^\gamma 4^{n-\gamma-\delta}$.

The all-zero and all-one vector will be denoted by $\mathbf{0}$ and $\mathbf{1}$, respectively. It will be clear by the context whether we refer to binary vectors or quaternary vectors.

Let $\mathcal{C}$ be a quaternary linear code and let $C = \phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_4$-linear code with kernel $K(C)$. The kernel of $\mathcal{C}$, denoted by $\mathcal{K}(\mathcal{C})$, is defined as the inverse Gray map image of $K(C)$, that is $\mathcal{K}(\mathcal{C}) = \phi^{-1}(K(C))$. Furthermore, the dimension of the kernel of $\mathcal{C}$ is defined as the dimension of the kernel of $C = \phi(\mathcal{C})$, and also denoted by $k_{\mathcal{C}}$.

Let $u * v$ denote the component-wise product for any $u, v \in \mathbb{Z}_4^n$.

Lemma 1 ([8],[9]). *Let $\mathcal{C}$ be a quaternary linear code. Then,*

$$\mathcal{K}(\mathcal{C}) = \{u \ : \ u \in \mathcal{C} \text{ and } 2u * v \in \mathcal{C}, \forall v \in \mathcal{C}\}.$$

Note that if $\mathcal{G}$ is a generator matrix of a quaternary linear code $\mathcal{C}$, then $u \in \mathcal{K}(\mathcal{C})$ if and only if $u \in \mathcal{C}$ and $2u * v \in \mathcal{C}$ for all $v \in \mathcal{G}$. Moreover, by Lemma 1, all codewords of order two in $\mathcal{C}$ belong to $\mathcal{K}(\mathcal{C})$. It is also clear that if the vector $\mathbf{1}$ belongs to $\mathcal{C}$, then it is also in $\mathcal{K}(\mathcal{C})$. Finally, note that $\mathcal{K}(\mathcal{C})$ is a linear subcode of $\mathcal{C}$ [8],[9].

2.2 Quaternary Linear Reed-Muller Codes

Recall that a binary linear rth-order Reed-Muller code $RM(r, m)$ with $0 \leq r \leq m$ and $m \geq 2$ can be described using the Plotkin construction as follows [14]:

$$RM(r, m) = \{(u|u + v) \; : \; u \in RM(r, m - 1), \, v \in RM(r - 1, m - 1)\},$$

where $RM(0, m)$ is the repetition code $\{\mathbf{0}, \mathbf{1}\}$, $RM(m, m)$ is the universe code, and "|" denotes concatenation. For $m = 1$, there are only two codes: the repetition code $RM(0, 1)$ and the universe code $RM(1, 1)$. This RM family has the parameters and properties quoted in the following proposition.

Proposition 2 ([14]). *A binary linear* r*th-order Reed-Muller code $RM(r, m)$ with $m \geq 1$ and $0 \leq r \leq m$ has the following parameters and properties:*

1. *the length is $n = 2^m$;*
2. *the minimum Hamming distance is $d = 2^{m-r}$;*
3. *the dimension is $k = \sum_{i=0}^{r} \binom{m}{i}$;*
4. *the code $RM(r - 1, m)$ is a subcode of $RM(r, m)$ for $0 < r \leq m$;*
5. *the code $RM(r, m)$ is the dual code of $RM(m - 1 - r, m)$ for $0 \leq r < m$.*

In the recent literature [2],[3],[10],[18],[19] several families of quaternary linear codes have been proposed and studied trying to generalize the RM family. However, when the corresponding $\mathbb{Z}_4$-linear codes are taken, they do not satisfy all the properties quoted in Proposition 2. In [16],[17], new quaternary linear Reed-Muller families, $\mathcal{RM}_s$, such that the corresponding $\mathbb{Z}_4$-linear codes have the parameters and properties described in Proposition 2, were proposed. The following two Plotkin constructions are necessary to generate these new $\mathcal{RM}_s$ families.

Definition 3 (Plotkin Construction). *Let $\mathcal{A}$ and $\mathcal{B}$ be two quaternary linear codes of length n, types $2^{\gamma_\mathcal{A}} 4^{\delta_\mathcal{A}}$ and $2^{\gamma_\mathcal{B}} 4^{\delta_\mathcal{B}}$, and minimum distances $d_\mathcal{A}$ and $d_\mathcal{B}$, respectively. A new quaternary linear code $\mathcal{PC}(\mathcal{A}, \mathcal{B})$ is defined as*

$$\mathcal{PC}(\mathcal{A}, \mathcal{B}) = \{(u|u + v) \; : \; u \in \mathcal{A}, v \in \mathcal{B}\}.$$

It is easy to see that if $\mathcal{G}_\mathcal{A}$ and $\mathcal{G}_\mathcal{B}$ are generator matrices of $\mathcal{A}$ and $\mathcal{B}$, respectively, then the matrix

$$\mathcal{G}_{PC} = \begin{pmatrix} \mathcal{G}_\mathcal{A} & \mathcal{G}_\mathcal{A} \\ 0 & \mathcal{G}_\mathcal{B} \end{pmatrix}$$

is a generator matrix of the code $\mathcal{PC}(\mathcal{A}, \mathcal{B})$. Moreover, the code $\mathcal{PC}(\mathcal{A}, \mathcal{B})$ is of length $2n$, type $2^{\gamma_\mathcal{A} + \gamma_\mathcal{B}} 4^{\delta_\mathcal{A} + \delta_\mathcal{B}}$, and minimum distance $d = min\{2d_\mathcal{A}, d_\mathcal{B}\}$ [16],[17].

Definition 4 (BQ-Plotkin Construction). *Let $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ be three quaternary linear codes of length n; types $2^{\gamma_\mathcal{A}}4^{\delta_\mathcal{A}}$, $2^{\gamma_\mathcal{B}}4^{\delta_\mathcal{B}}$, and $2^{\gamma_\mathcal{C}}4^{\delta_\mathcal{C}}$; and minimum distances $d_\mathcal{A}$, $d_\mathcal{B}$, and $d_\mathcal{C}$, respectively. Let $\mathcal{G}_\mathcal{A}$, $\mathcal{G}_\mathcal{B}$, and $\mathcal{G}_\mathcal{C}$ be generator matrices of the codes $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$, respectively. A new code $\mathcal{BQ}(\mathcal{A},\mathcal{B},\mathcal{C})$ is defined as the quaternary linear code generated by*

$$\mathcal{G}_{BQ} = \begin{pmatrix} \mathcal{G}_\mathcal{A} & \mathcal{G}_\mathcal{A} & \mathcal{G}_\mathcal{A} & \mathcal{G}_\mathcal{A} \\ 0 & \mathcal{G}'_\mathcal{B} & 2\mathcal{G}'_\mathcal{B} & 3\mathcal{G}'_\mathcal{B} \\ 0 & 0 & \hat{\mathcal{G}}_\mathcal{B} & \hat{\mathcal{G}}_\mathcal{B} \\ 0 & 0 & 0 & \mathcal{G}_C \end{pmatrix},$$

where $\mathcal{G}'_\mathcal{B}$ is the matrix obtained from $\mathcal{G}_\mathcal{B}$ after switching twos by ones in their $\gamma_\mathcal{B}$ rows of order two, and $\hat{\mathcal{G}_\mathcal{B}}$ is the matrix obtained from $\mathcal{G}_\mathcal{B}$ after removing their $\gamma_\mathcal{B}$ rows of order two.

The code $\mathcal{BQ}(\mathcal{A},\mathcal{B},\mathcal{C})$ is of length $4n$, type $2^{\gamma_\mathcal{A}+\gamma_\mathcal{C}}4^{\delta_\mathcal{A}+\gamma_\mathcal{B}+2\delta_\mathcal{B}+\delta_\mathcal{C}}$, and minimum distance $d = min\{4d_\mathcal{A}, 2d_\mathcal{B}, d_\mathcal{C}\}$ [16],[17].

Now, the quaternary linear Reed-Muller codes $\mathcal{RM}_s(r,m)$ of length 2^{m-1}, for $m \geq 1$, $0 \leq r \leq m$, and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$, will be defined. For the recursive construction it will be convenient to define them also for $r < 0$ and $r > m$. We begin by considering the trivial cases. The code $\mathcal{RM}_s(r,m)$ with $r < 0$ is defined as the zero code. The code $\mathcal{RM}_s(0,m)$ is defined as the repetition code with only the all-zero and all-two vectors. The code $\mathcal{RM}_s(r,m)$ with $r \geq m$ is defined as the whole space $\mathbb{Z}_4^{m-1}$. For $m = 1$, there is only one family with $s = 0$, and in this family there are only the zero, repetition and universe codes for $r < 0$, $r = 0$ and $r \geq 1$, respectively. In this case, the generator matrix of $\mathcal{RM}_0(0,1)$ is $\mathcal{G}_{0(0,1)} = \begin{pmatrix} 2 \end{pmatrix}$ and the generator matrix of $\mathcal{RM}_0(1,1)$ is $\mathcal{G}_{0(1,1)} = \begin{pmatrix} 1 \end{pmatrix}$.

For any $m \geq 2$, given $\mathcal{RM}_s(r,m-1)$ and $\mathcal{RM}_s(r-1,m-1)$ codes, where $0 \leq s \leq \lfloor \frac{m-2}{2} \rfloor$, the $\mathcal{RM}_s(r,m)$ code can be constructed in a recursive way using the Plotkin construction given by Definition 3 as follows:

$$\mathcal{RM}_s(r,m) = \mathcal{PC}(\mathcal{RM}_s(r,m-1), \mathcal{RM}_s(r-1,m-1)).$$

For example, for $m = 2$, the generator matrices of $\mathcal{RM}_0(r,2)$, $0 \leq r \leq 2$, are the following:

$$\mathcal{G}_{0(0,2)} = \begin{pmatrix} 2 \; 2 \end{pmatrix}; \quad \mathcal{G}_{0(1,2)} = \begin{pmatrix} 0 \; 2 \\ 1 \; 1 \end{pmatrix}; \quad \mathcal{G}_{0(2,2)} = \begin{pmatrix} 1 \; 0 \\ 0 \; 1 \end{pmatrix}.$$

Note that when m is odd, the $\mathcal{RM}_s$ family with $s = \frac{m-1}{2}$ can not be generated using the Plotkin construction. In this case, for any $m \geq 3$, m odd and $s = \frac{m-1}{2}$, given $\mathcal{RM}_{s-1}(r,m-2)$, $\mathcal{RM}_{s-1}(r-1,m-2)$ and $\mathcal{RM}_{s-1}(r-2,m-2)$, the $\mathcal{RM}_s(r,m)$ code can be constructed using the BQ-Plotkin construction given by Definition 4 as follows:

$$\mathcal{RM}_s(r,m) = \mathcal{BQ}(\mathcal{RM}_{s-1}(r,m-2), \mathcal{RM}_{s-1}(r-1,m-2), \mathcal{RM}_{s-1}(r-2,m-2)).$$

For example, for $m = 3$, there are two families. The $\mathcal{RM}_0$ family can be generated using the Plotkin construction. On the other hand, the $\mathcal{RM}_1$ family has to be generated using the BQ-Plotkin construction. The generator matrices of $\mathcal{RM}_1(r,3)$, $0 \le r \le 3$, are the following: $\mathcal{G}_{1(0,3)} = \begin{pmatrix} 2\,2\,2\,2 \end{pmatrix}$;

$$\mathcal{G}_{1(1,3)} = \begin{pmatrix} 1\,1\,1\,1 \\ 0\,1\,2\,3 \end{pmatrix}; \quad \mathcal{G}_{1(2,3)} = \begin{pmatrix} 1\,1\,1\,1 \\ 0\,1\,2\,3 \\ 0\,0\,1\,1 \\ 0\,0\,0\,2 \end{pmatrix}; \quad \mathcal{G}_{1(3,3)} = \begin{pmatrix} 1\,1\,1\,1 \\ 0\,1\,2\,3 \\ 0\,0\,1\,1 \\ 0\,0\,0\,1 \end{pmatrix}.$$

Table 1 shows the type $2^{\gamma}4^{\delta}$ of all these $\mathcal{RM}_s(r,m)$ codes for $m \le 7$.

The following proposition summarizes the parameters and properties of these $\mathcal{RM}_s$ families of codes.

Proposition 5 ([16],[17]). *A quaternary linear Reed-Muller code $\mathcal{RM}_s(r,m)$, with $m \ge 1$, $0 \le r \le m$, and $0 \le s \le \lfloor \frac{m-1}{2} \rfloor$, has the following parameters and properties:*

1. *the length is $n = 2^{m-1}$;*
2. *the minimum Lee distance is $d = 2^{m-r}$;*
3. *the number of codewords is 2^k, where $k = \sum_{i=0}^{r} \binom{m}{i}$;*
4. *the code $\mathcal{RM}_s(r-1,m)$ is a subcode of $\mathcal{RM}_s(r,m)$ for $0 \le r \le m$;*
5. *the codes $\mathcal{RM}_s(1,m)$ and $\mathcal{RM}_s(m-2,m)$, after the Gray map, are $\mathbb{Z}_4$-linear Hadamard and $\mathbb{Z}_4$-linear extended perfect codes, respectively;*
6. *the code $\mathcal{RM}_s(r,m)$ is the dual code of $\mathcal{RM}_s(m-1-r,m)$ for $-1 \le r \le m$.*

In the next two sections, for all these codes $\mathcal{RM}_s(r,m)$ we will establish the dimension of the kernel, which will be denoted by $k_{s(r,m)}$ instead of $k_{\mathcal{RM}_s(r,m)}$.

3 Kernel Dimensions for the $\mathcal{RM}_s$ Family with $s = 0$

In this section, we will compute the dimension of the kernel for the quaternary linear Reed-Muller codes in the $\mathcal{RM}_s$ family with $s = 0$. As we have shown in Subsection 2.2, these codes can be constructed using the Plotkin construction.

Let $\mathcal{C}$ be a quaternary linear code. The code $2\mathcal{C}$ is obtained from $\mathcal{C}$ by multiplying by two all codewords of $\mathcal{C}$. Note that if $\mathcal{G}$ is a generator matrix of $\mathcal{C}$, then $2\mathcal{G}$ is a generator matrix of $2\mathcal{C}$.

Lemma 6. *For all $m \ge 1$ and $r \in \{0,\ldots,m-1\}$, $2\mathcal{RM}_0(r+1,m) \subseteq \mathcal{RM}_0(r,m)$.*

Proof. We proceed by induction. For $m = 1$, there are the zero, repetition and universe codes for $r < 0$, $r = 0$, and $r > 0$, respectively. The lemma is true for these codes.

For $m \ge 2$, assume that the result is true. Let $\mathcal{G}_{r-1,m-1}$, $\mathcal{G}_{r,m-1}$ and $\mathcal{G}_{r+1,m-1}$ be generator matrices of $\mathcal{RM}_0(r-1,m-1)$, $\mathcal{RM}_0(r,m-1)$ and $\mathcal{RM}_0(r+1,m-1)$, respectively. Using the Plotkin construction given by Definition 3 we obtain two new codes $\mathcal{RM}_0(r,m)$ and $\mathcal{RM}_0(r+1,m)$ with generator matrices

$$\mathcal{G}_{r,m} = \begin{pmatrix} \mathcal{G}_{r,m-1} & \mathcal{G}_{r,m-1} \\ 0 & \mathcal{G}_{r-1,m-1} \end{pmatrix}, \mathcal{G}_{r+1,m} = \begin{pmatrix} \mathcal{G}_{r+1,m-1} & \mathcal{G}_{r+1,m-1} \\ 0 & \mathcal{G}_{r,m-1} \end{pmatrix},$$

respectively. Since $2\mathcal{RM}_0(r+1,m-1) \subseteq \mathcal{RM}_0(r,m-1)$, the submatrix $2(\mathcal{G}_{r+1,m-1} \;\; \mathcal{G}_{r+1,m-1})$ generates a code contained in the code generated by the submatrix $(\mathcal{G}_{r,m-1} \;\; \mathcal{G}_{r,m-1})$. The same argument can be used for the submatrices $(0 \;\; \mathcal{G}_{r,m-1})$ and $(0 \;\; \mathcal{G}_{r-1,m-1})$. Thus the code $2\mathcal{RM}_0(r+1,m)$ generated by $2\mathcal{G}_{r+1,m}$ is contained in the code $\mathcal{RM}_0(r,m)$ generated by $\mathcal{G}_{r,m}$. □

Let W^{m-1} be the set of order four vectors $\{w_1^{m-1}, \ldots, w_m^{m-1}\}$ over $\mathbb{Z}_4^{2^{m-1}}$ defined as follows:

$$\begin{aligned} w_1^{m-1} &= 1^{2^{m-1}} = \mathbf{1}, \\ w_i^{m-1} &= (0^{2^{m-i}} | 1^{2^{m-i}})^{2^{i-2}}, \;\; \text{for } i \in \{2,\ldots,m\}. \end{aligned}$$

Note that, for $i \in \{2,\ldots,m-1\}$, we have that $(w_i^{m-2} | w_i^{m-2}) = w_{i+1}^{m-1}$.

By Proposition 5, since the corresponding $\mathbb{Z}_4$-linear code of any $\mathcal{RM}_s(1,m)$ is a Hadamard code, $\mathbf{1} \in \mathcal{RM}_s(1,m)$ [13]. Moreover, for all $r \geq 1$, the vector $\mathbf{1} \in \mathcal{RM}_s(r,m)$ by the inclusion property, and also belongs to the kernel of $\mathcal{RM}_s(r,m)$ by Lemma 1.

Lemma 7. *For all $m \geq 2$ and $r \in \{2,\ldots,m\}$, W^{m-1} is a subset of $\mathcal{RM}_0(r,m)$.*

Proof. It is clear that $w_1^{m-1} = \mathbf{1} \in \mathcal{RM}_0(r,m)$ for $r \geq 1$ and $\mathbf{0} \in \mathcal{RM}_0(r,m)$ for $r \geq 0$. Hence, for $m = 1$, $W^0 = \{\mathbf{1}\}$ is a subset of $\mathcal{RM}_0(1,1)$. For $m \geq 2$, the subsequent $\mathcal{RM}_0(r,m)$ codes are obtained using the Plotkin construction given by Definition 3 as follows:

$$\mathcal{RM}_0(r,m) = \mathcal{PC}(\mathcal{RM}_0(r,m-1), \mathcal{RM}_0(r-1,m-1)).$$

We proceed by induction on m. For $m = 2$, we have the set $W^1 = \{w_1^1, w_2^1\}$ and the lemma is true, since $\mathcal{RM}_0(r,2)$ is the universe code for $r \geq 2$.

For $m \geq 3$, since $\mathbf{0} \in \mathcal{RM}_0(r,m-1)$ and $\mathbf{1} \in \mathcal{RM}_0(r-1,m-1)$ for $r \geq 2$, then $(\mathbf{0}|\mathbf{0}+\mathbf{1}) = w_2^{m-1} \in \mathcal{RM}_0(r,m)$ for $r \geq 2$. In general, if $x \in \mathcal{RM}_0(r,m-1)$, then $(x|x+\mathbf{0}) = (x|x) \in \mathcal{RM}_0(r,m)$. Since $w_i^{m-2} \in \mathcal{RM}_0(r,m-1)$, for $r \geq 2$ and $2 \leq i \leq m-1$, it is clear that $(w_i^{m-2}|w_i^{m-2}) = w_{i+1}^{m-1} \in \mathcal{RM}_0(r,m)$. Therefore, $w_i^{m-1} \in \mathcal{RM}_0(r,m)$ for $r \geq 2$ and $1 \leq i \leq m$. □

By Lemma 7, for all $m \geq 2$ and $r \in \{2,\ldots,m\}$, there is a generator matrix $\mathcal{G}_{0(r,m)} = \begin{pmatrix} \mathcal{G}_\gamma \\ \mathcal{G}_\delta \end{pmatrix}$ of the code $\mathcal{RM}_0(r,m)$ of type $2^\gamma 4^\delta$, such that W^{m-1} is a submatrix of $\mathcal{G}_\delta$, where $\mathcal{G}_\gamma$ and $\mathcal{G}_\delta$ are the γ and δ generators of order two and four, respectively. In Proposition 10, for all $m \geq 4$ and $r \in \{2,\ldots,m-2\}$, we will show that the kernel of $\mathcal{RM}_0(r,m)$ is generated by the matrix

$$\begin{pmatrix} \mathcal{G}_\gamma \\ 2\mathcal{G}_\delta \\ W^{m-1} \end{pmatrix}. \tag{2}$$

Lemma 8. *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two quaternary linear codes of length n with generator matrices $\mathcal{G}_1$ and $\mathcal{G}_2$, respectively, such that $\mathcal{C}_2 \subseteq \mathcal{C}_1$. Let $\mathcal{C} = \mathcal{PC}(\mathcal{C}_1, \mathcal{C}_2)$ of length $2n$. If $x \in \mathcal{C}_1$ and $y \in \mathcal{C}_2$, then $(x|x+y) \in \mathcal{K}(\mathcal{C})$ if and only if $x \in \mathcal{K}(\mathcal{C}_1)$, $2y * u \in \mathcal{C}_2$, and $2x * v \in \mathcal{C}_2$, for all $u \in \mathcal{G}_1$ and $v \in \mathcal{G}_2$.*

Proof. The codeword $(x|x+y) \in \mathcal{K}(\mathcal{C})$ if and only if $2(x|x+y) * (u|u) \in \mathcal{C}$ and $2(x|x+y) * (0|v) \in \mathcal{C}$ for all u, v in $\mathcal{G}_1, \mathcal{G}_2$, respectively. That means $(2x * u|2x * u + 2y * u) \in \mathcal{C}$, $\forall u \in \mathcal{G}_1$, and $(0|2x * v + 2y * v) \in \mathcal{C}$, $\forall v \in \mathcal{G}_2$. That is, $x \in \mathcal{K}(\mathcal{C}_1)$ and $2y * u \in \mathcal{C}_2$, $\forall u \in \mathcal{G}_1$, and $2x * v + 2y * v \in \mathcal{C}_2$, $\forall v \in \mathcal{G}_2$. Note that since $\mathcal{C}_2 \subseteq \mathcal{C}_1$, the condition $2y * u \in \mathcal{C}_2$ $\forall u \in \mathcal{G}_1$ implies that $2y * v \in \mathcal{C}_2$ $\forall v \in \mathcal{G}_2$. Therefore, $2x * v + 2y * v \in \mathcal{C}_2$ $\forall v \in \mathcal{G}_2$ is simplified to $2x * v \in \mathcal{C}_2$ $\forall v \in \mathcal{G}_2$. □

Note that if $2y * u \in \mathcal{C}_2$ for all $u \in \mathcal{G}_1$, then $y \in \mathcal{K}(\mathcal{C}_2)$. Furthermore, x could not belong to $\mathcal{C}_2$, but if $x \in \mathcal{C}_2$ then $x \in \mathcal{K}(\mathcal{C}_2)$.

Proposition 9. *For all $m \geq 1$ and $r \in \{0, 1, 2, m-1, m\}$, the corresponding $\mathbb{Z}_4$-linear code of $\mathcal{RM}_0(r, m)$ is a binary linear code.*

Proof. For $r = 0$, $r = m-1$ and $r = m$, the corresponding $\mathbb{Z}_4$-linear codes of $\mathcal{RM}_0(r, m)$ are the repetition, the even weight and the universe codes, respectively, which are binary linear codes. For $r = 1$, the corresponding $\mathbb{Z}_4$-linear code of $\mathcal{RM}_0(r, m)$ is the binary linear Hadamard code [16],[17].

Finally, for $r = 2$, the $\mathcal{RM}_0(2, m)$ code is constructed as $\mathcal{PC}(\mathcal{RM}_0(2, m-1), \mathcal{RM}_0(1, m-1))$. We proceed by induction on m. For $m = 2$, the code $\mathcal{RM}_0(2, 2)$ is the universe code. For $m \geq 3$, we can assume that $\phi(\mathcal{RM}_0(2, m-1))$ and $\phi(\mathcal{RM}_0(1, m-1))$ are binary linear codes. The generator matrix of $\mathcal{RM}_0(2, m)$ only have vectors of the form $(x|x)$ and $(0|y)$ for all $x \in \mathcal{G}_{0(2,m-1)}$, $y \in \mathcal{G}_{0(1,m-1)}$. By Lemmas 6 and 8, since $x \in \mathcal{K}(\mathcal{RM}_0(2, m-1))$ and the only vector of order four in the generator matrix of $\mathcal{RM}_0(1, m-1))$ is $\mathbf{1}$, the vector $(x|x) \in \mathcal{K}(\mathcal{RM}_0(2, m))$, $\forall x \in \mathcal{G}_{0(2,m-1)}$. By Lemmas 6, 8 and the same argument, the vector $(0|y) \in \mathcal{K}(\mathcal{RM}_0(2, m))$, $\forall y \in \mathcal{G}_{0(1,m-1)}$. Thus all the vectors in the generator matrix of $\mathcal{RM}_0(2, m)$ belong to the kernel of $\mathcal{RM}_0(2, m)$. Therefore, the corresponding $\mathbb{Z}_4$-linear code of $\mathcal{RM}_0(2, m)$ is a binary linear code. □

Let A and B be two matrices. If B is a submatrix of A, then we will use $A \setminus B$ to denote the matrix A without the rows of B. Recall that we will also use A and B to denote the set of row vectors of A and B, respectively. Moreover, if $B \subseteq A$ then we will use $A \setminus B$ to denote the set of row vectors in A which are not in B.

Proposition 10. *For all $m \geq 4$ and $r \in \{2, \ldots, m-2\}$, the kernel of $\mathcal{RM}_0(r, m)$ of type $2^\gamma 4^\delta$ is the quaternary linear code generated by $\begin{pmatrix} \mathcal{G}_\gamma \\ 2\mathcal{G}_\delta \\ W^{m-1} \end{pmatrix}$, where $\mathcal{G}_\gamma$ and $\mathcal{G}_\delta$ are the γ and δ generators of order two and four of $\mathcal{RM}_0(r, m)$, respectively.*

Proof. For $m = 4$, there is only the code $\mathcal{RM}_0(2, 4)$. By Proposition 9, the corresponding $\mathbb{Z}_4$-linear code of $\mathcal{RM}_0(2, m)$ is a binary linear code. Since $W^{m-1} \subseteq \mathcal{RM}_0(2, m)$ and $\delta = m$, the preposition is true for all the codes $\mathcal{RM}_0(2, m)$.

For $m = 5$, the code $\mathcal{RM}_0(3,5)$ is the first one under the Gray map, the binary code is nonlinear. In this case, we can compute its kernel and see that can be generated by $\begin{pmatrix} \mathcal{G}_\gamma \\ 2\mathcal{G}_\delta \\ W^4 \end{pmatrix}$.

By Lemma 7, there is a generator matrix for any $\mathcal{RM}_0(r,m)$ with $r \geq 2$, which can be written as follows:

$$\begin{pmatrix} \mathcal{G}_\gamma \\ 2\mathcal{G}_\delta \\ \mathcal{G}_\delta \setminus W^{m-1} \\ W^{m-1} \end{pmatrix}.$$

For $m > 5$, assume that the lemma is true for $m-1$. Let $\mathcal{C}_1 = \mathcal{RM}_0(r, m-1)$ and $\mathcal{C}_2 = \mathcal{RM}_0(r-1, m-1)$ of types $2^\gamma 4^\delta$ and $2^{\gamma'} 4^{\delta'}$, respectively. Let $\mathcal{C} = \mathcal{RM}_0(r,m) = \mathcal{PC}(\mathcal{C}_1, \mathcal{C}_2)$ be the new code with a generator matrix of the form

$$\begin{pmatrix} \mathcal{G}_\gamma & \mathcal{G}_\gamma \\ 2\mathcal{G}_\delta & 2\mathcal{G}_\delta \\ \mathcal{G}_\delta \setminus W^{m-2} & \mathcal{G}_\delta \setminus W^{m-2} \\ W^{m-2} & W^{m-2} \\ 0 & \mathcal{G}_{\gamma'} \\ 0 & 2\mathcal{G}_{\delta'} \\ 0 & \mathcal{G}_{\delta'} \setminus W^{m-2} \\ 0 & W^{m-2} \end{pmatrix}$$

The vectors of order two are always in the kernel. By Lemma 8, the vectors that are not in the kernels of $\mathcal{C}_1$ and $\mathcal{C}_2$ can not be in the kernel of $\mathcal{C}$. This excludes the row vectors in $(\mathcal{G}_\delta \setminus W^{m-2} \mid \mathcal{G}_\delta \setminus W^{m-2})$ and $(0 \mid \mathcal{G}_{\delta'} \setminus W^{m-2})$, and their linear combinations with the kernel of $\mathcal{C}$. Since $W^{m-2} \subseteq \mathcal{K}(\mathcal{C}_1)$ and $W^{m-2} \subseteq \mathcal{K}(\mathcal{C}_2)$, the row vectors of the form $(W^{m-2} \mid W^{m-2})$ are in $\mathcal{K}(\mathcal{C})$. For the vectors of the form $(0 \mid W^{m-2})$, we have two cases. By Lemmas 6 and 8, $(\mathbf{0}|\mathbf{1}) \in \mathcal{K}(\mathcal{C})$. On the other hand, the vectors $w_i \in W^{m-2}$, $2 \leq i \leq m-1$, have weight 2^{m-3}. By Proposition 5, $w_{min}(\mathcal{C}) = w_{min}(\mathcal{C}_2)$ and $2w_{min}(\mathcal{C}) = w_{min}(\mathcal{C}_1)$. For every vector y in the space generated by $W^{m-2} \setminus \mathbf{1}$, there is another vector of order four, $u \in \mathcal{G}_1$, such that the weight of $2y * u$ is less than $w_{min}(\mathcal{C})$. Thus $y \notin \mathcal{K}(\mathcal{C})$. Finally, $(W^{m-2} \mid W^{m-2}) \cup (\mathbf{0}|\mathbf{1}) = W^{m-1}$. □

Note that the case $r = 2$ is included in both Propositions 9 and 10. That is, the corresponding $\mathbb{Z}_4$-linear code of any $\mathcal{RM}_0(2,m)$ is always a binary linear code and $\mathcal{RM}_0(2,m)$ can be generated by a matrix of the form (2).

Corollary 11. *For all $m \geq 1$ and $0 \leq r \leq m$, the dimension of the kernel of $\mathcal{RM}_0(r,m)$ of type $2^\gamma 4^\delta$ is*

$$k_{0(r,m)} = \begin{cases} \gamma + 2\delta & \text{if } r \in \{0, 1, m-1, m\} \\ \gamma + \delta + m & \text{if } r \in \{2, \ldots, m-2\}. \end{cases}$$

Proof. Straightforward from Propositions 9 and 10. □

Note that, the kernel, as a binary linear code, is generated by

$$\begin{pmatrix} \phi(\mathcal{G}_\gamma) \\ \phi(2\mathcal{G}_\delta) \\ \phi(W^{m-1}) \end{pmatrix},$$

where all these vectors are linear independent over $\mathbb{Z}_2^m$.

4 Kernel Dimensions for the $\mathcal{RM}_s$ Families

In this section, the general case when $s > 0$ is studied. We will establish the dimension of the kernel for any quaternary linear Reed-Muller code in these $\mathcal{RM}_s$ families. This invariant, the kernel dimension, will help us to the classification of these codes.

As we have shown in Subsection 2.2, these quaternary linear Reed-Muller codes $\mathcal{RM}_s(r,m)$ can be obtained using the Plotkin construction, except when m is odd and $s = \frac{m-1}{2}$. In this case, they are obtained using the BQ-Plotkin construction. Note that some of these codes could be constructed using any of these two constructions.

Theorem 12. *For all $m \geq 1$, $0 \leq r \leq m$, and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$, the dimension of the kernel of $\mathcal{RM}_s(r,m)$ of type $2^\gamma 4^\delta$ is*

1. $k_{s(0,m)} = 1$, $k_{s(m-1,m)} = 2^m - 1$, $k_{s(m,m)} = 2^m$.
2. *If $s = 0$,*
$$k_{0(r,m)} = \begin{cases} \gamma + 2\delta & \text{if } \; r = 1 \\ \gamma + \delta + m & \text{if } \; r \in \{2, \ldots, m-2\}. \end{cases}$$
3. *If $s = 1$, $k_{1(r,m)} = \gamma + \delta + 2$ for all $r \in \{1, 2, \ldots, m-2\}$.*
4. *If $s \geq 2$, $k_{s(r,m)} = \gamma + \delta + 1$ for all $r \in \{1, 2, \ldots, m-2\}$, except the case $k_{2(2,5)} = \gamma + \delta + 2 = 11$.*

Proof. It is straightforward to see that $k_{s(0,m)} = 1$, $k_{s(m-1,m)} = 2^m - 1$, and $k_{s(m,m)} = 2^m$, because $\phi(\mathcal{RM}_s(0,m))$, $\phi(\mathcal{RM}_s(m-1,m))$, and $\phi(\mathcal{RM}_s(m,m))$ are the repetition, the even weight, and the universe codes, respectively.

The case $s = 0$ is proved in Corollary 11. The cases $s = 1$ and $s \geq 2$ can be proved using similar arguments to that for the case $s = 0$. When $s = 1$ there are only two generators of order four in the kernel of $\mathcal{RM}_1(r,m)$, $w_1^{m-1} = \mathbf{1}$ and w_2^{m-1}. When $s \geq 2$ there is only one generator of order four $w_1^{m-1} = \mathbf{1}$ in the kernel of $\mathcal{RM}_s(r,m)$, except for the code $\mathcal{RM}_2(2,5)$. Since $\phi(\mathcal{RM}_2(2,5))$ and $\phi(\mathcal{RM}_2(1,5))$ are equivalent $k_{2(2,5)} = 11 = \gamma + \delta + 2$. □

Note that Theorem 12 includes the previous results about the kernel dimension for $\mathbb{Z}_4$-linear Hadamard and $\mathbb{Z}_4$-linear extended 1-perfect codes [6],[13],[15] or (1). Table 1 shows the type $2^\gamma 4^\delta$ and the dimension of the kernel of all these $\mathcal{RM}_s(r,m)$ codes for $m \leq 7$.

Table 1. Type $2^\gamma 4^\delta$ and kernel dimension $k_{s(r,m)}$ for all $\mathcal{RM}_s(r,m)$ codes with $m \leq 7$, showing them in the form (γ,δ) $k_{s(r,m)}$

m	$s \backslash r$	0	1	2	3	4	5	6	7
1	0	(1,0) 1	(0,1) 2						
2	0	(1,0) 1	(1,1) 3	(0,2) 4					
3	0	(1,0) 1	(2,1) 4	(1,3) 7	(0,4) 8				
	1	(1,0) 1	(0,2) 4	(1,3) 7	(0,4) 8				
4	0	(1,0) 1	(3,1) 5	(3,4) 11	(1,7) 15	(0,8) 16			
	1	(1,0) 1	(1,2) 5	(1,5) 8	(1,7) 15	(0,8) 16			
5	0	(1,0) 1	(4,1) 6	(6,5) 16	(4,11) 20	(1,15) 31	(0,16) 32		
	1	(1,0) 1	(2,2) 6	(2,7) 11	(2,12) 16	(1,15) 31	(0,16) 32		
	2	(1,0) 1	(0,3) 4	(2,7) 11	(0,13) 14	(1,15) 31	(0,16) 32		
6	0	(1,0) 1	(5,1) 7	(10,6) 22	(10,16) 32	(5,26) 37	(1,31) 63	(0,32) 64	
	1	(1,0) 1	(3,2) 7	(4,9) 15	(4,19) 25	(3,27) 32	(1,31) 63	(0,32) 64	
	2	(1,0) 1	(1,3) 5	(2,10) 13	(2,20) 23	(1,28) 30	(1,31) 63	(0,32) 64	
7	0	(1,0) 1	(6,1) 8	(15,7) 29	(20,22) 49	(15,42) 64	(6,57) 70	(1,63) 127	(0,64) 128
	1	(1,0) 1	(4,2) 8	(7,11) 20	(8,28) 38	(7,46) 55	(4,58) 64	(1,63) 127	(0,64) 128
	2	(1,0) 1	(2,3) 6	(3,13) 17	(4,30) 35	(3,48) 52	(2,59) 62	(1,63) 127	(0,64) 128
	3	(1,0) 1	(0,4) 5	(3,13) 17	(0,32) 33	(3,48) 52	(0,60) 61	(1,63) 127	(0,64) 128

The next theorem proves that there are at least $\lfloor \frac{m-1}{2} \rfloor$ nonequivalent binary codes with the same parameters as the code $RM(r,m)$.

Lemma 13. *Given two codes $\mathcal{RM}_s(r,m)$ and $\mathcal{RM}_{s'}(r,m)$ of type $2^\gamma 4^\delta$ and $2^{\gamma'} 4^{\delta'}$ respectively, such that $s < s'$, we have that $\gamma + \delta > \gamma' + \delta'$, except one case: if m is odd, r even, $s = \frac{m-3}{2}$, and $s' = \frac{m-1}{2}$, then $\gamma + \delta = \gamma' + \delta'$.*

Proof. When $\mathcal{RM}_s(r,m)$ and $\mathcal{RM}_{s'}(r,m)$ are obtained using the Plotkin construction, it is easy to see that $\gamma + \delta > \gamma' + \delta'$.

If m is odd and $s' = \frac{m-1}{2}$, the code $\mathcal{RM}_{s'}(r,m)$ is obtained using the BQ-Plotkin construction. Without loss of generality, we can assume that $s = s' - 1$ and $\mathcal{RM}_s(r,m)$ is obtained using the Plotkin construction. Using the recursive definition of $\gamma = \gamma_{s(r,m)}$, $\delta = \delta_{s(r,m)}$, $\gamma' = \gamma_{s'(r,m)}$, and $\delta = \delta_{s'(r,m)}$, we have that $\gamma_{s(r,m)} + \delta_{s(r,m)} - \gamma_{s'(r,m)} - \delta_{s'(r,m)} = \gamma_{s'-1(r-1,m-2)}$. Hence, if $\gamma_{s'-1(r-1,m-2)} \neq 0$ then $\gamma_{s(r,m)} + \delta_{s(r,m)} > \gamma_{s'(r,m)} + \delta_{s'(r,m)}$, and if $\gamma_{s'-1(r-1,m-2)} = 0$ then $\gamma_{s(r,m)} + \delta_{s(r,m)} = \gamma_{s'(r,m)} + \delta_{s'(r,m)}$, which is when r is even. □

Theorem 14. *For all $m \geq 4$ and $r = 1$, there are at least $\lfloor \frac{m-1}{2} \rfloor$ nonequivalent binary codes with the same parameters as the code $RM(1,m)$.*

For all $m \geq 4$ and $2 \leq r \leq m-2$, there are at least $\lfloor \frac{m+1}{2} \rfloor$ nonequivalent binary codes with the same parameters as the code $RM(r,m)$, except when m is odd, and r is even. In this case, there are at least $\frac{m-1}{2}$ nonequivalent binary codes with the same parameters as the code $RM(r,m)$.

Proof. For $r = 1$, the result was proved in [13]. For $2 \leq r \leq m - 2$, the proof is consequence of Theorem 12 and Lemma 13. □

5 Conclusions

In a recent paper [17], new families of quaternary linear codes, the $\mathcal{RM}_s(r, m)$ codes, are constructed in such a way that, after the Gray map, the $\mathbb{Z}_4$-linear codes fulfill the same properties and fundamental characteristics as the binary linear Reed-Muller codes. In this paper, a structural invariant for binary codes, the kernel dimension, is used to classify these new families of codes. Using a recursive construction, we give the generator matrices of the kernel and compute the exact values of the kernel dimension for all the feasible values of s, r and m. This invariant allows us to classify all the codes except when m is odd, $m \geq 5$, and r is even. In a further research we will also compute the rank, another structural invariant for binary codes, and give a complete classification of these families of codes.

References

1. Bauer, H., Ganter, B., Hergert, F.: Algebraic techniques for nonlinear codes. Combinatorica 3, 21–33 (1983)
2. Borges, J., Fernández, C., Phelps, K.T.: Quaternary Reed-Muller codes. IEEE Trans. Inform. Theory 51(7), 2686–2691 (2005)
3. Borges, J., Fernández-Córdoba, C., Phelps, K.T.: ZRM codes. IEEE Trans. Inform. Theory 54(1), 380–386 (2008)
4. Pernas, J., Pujol, J., Villanueva, M.: Codes over $\mathbb{Z}_4$. A Magma package. Universitat Autònoma de Barcelona (2008), `http://www.ccg.uab.cat`
5. Borges, J., Phelps, K.T., Rifà, J., Zinoviev, V.A.: On $\mathbb{Z}_4$-linear Preparata-like and Kerdock-like codes. IEEE Trans. Inform. Theory 49(11), 2834–2843 (2003)
6. Borges, J., Phelps, K.T., Rifà, J.: The rank and kernel of extended 1-perfect $\mathbb{Z}_4$-linear and additive non-$\mathbb{Z}_4$-linear codes. IEEE Trans. Inform. Theory 49(8), 2028–2034 (2003)
7. Cannon, J.J., Bosma, W. (eds.): Handbook of Magma Functions, Edition 2.13, 4350 p. (2006)
8. Fernández-Córdoba, C., Pujol, J., Villanueva, M.: On rank and kernel of $\mathbb{Z}_4$-linear codes. In: Barbero, A. (ed.) ICMCTA 2008. LNCS, vol. 5228, pp. 46–55. Springer, Heidelberg (2008)
9. Fernández-Córdoba, C., Pujol, J., Villanueva, M.: $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel. Discrete Applied Mathematics (submitted, 2008) (arXiv:0807.4247)
10. Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The Z_4-linearity of Kerdock, Preparata, Goethals and related codes. IEEE Trans. Inform. Theory 40, 301–319 (1994)
11. Hou, X.-D., Lahtonen, J.T., Koponen, S.: The Reed-Muller code $R(r, m)$ is not $\mathbb{Z}_4$-linear for $3 \leq r \leq m - 2$. IEEE Trans. Inform. Theory 44, 798–799 (1998)
12. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)

13. Krotov, D.S.: $\mathbb{Z}_4$-linearHadamard and extended perfect codes. In: International Workshop on Coding and Cryptography, Paris, France, January 8-12, pp. 329–334 (2001)
14. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, Amsterdam (1977)
15. Phelps, K.T., Rifà, J., Villanueva, M.: On the additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes: rank and kernel. IEEE Trans. Inform. Theory 52(1), 316–319 (2006)
16. Pujol, J., Rifà, J., Solov'eva, F.I.: Quaternary plotkin constructions and quaternary reed-muller codes. In: Boztaş, S., Lu, H.-F(F.) (eds.) AAECC 2007. LNCS, vol. 4851, pp. 148–157. Springer, Heidelberg (2007)
17. Pujol, J., Rifà, J., Solov'eva, F.I.: Construction of $\mathbb{Z}_4$-linear Reed-Muller codes. IEEE Trans. Inform. Theory (to appear, 2008)
18. Solov'eva, F.I.: On Z4-linear codes with parameters of Reed-Muller codes. Problems of Inform. Trans. 43(1), 26–32 (2007)
19. Wan, Z.-X.: Quaternary codes. World Scientific Publishing Co. Pte. Ltd., Singapore (1997)

Appendix B

Rank for Some Families of Quaternary Reed-Muller codes

Rank for Some Families of Quaternary Reed-Muller Codes[⋆]

Jaume Pernas, Jaume Pujol, and Mercè Villanueva

Dept. of Information and Communications Engineering,
Universitat Autònoma de Barcelona, Spain
{jaume.pernas,jaume.pujol,merce.villanueva}@autonoma.edu

Abstract. Recently, new families of quaternary linear Reed-Muller codes such that, after the Gray map, the corresponding $\mathbb{Z}_4$-linear codes have the same parameters and properties as the codes in the usual binary linear Reed-Muller family have been introduced. A structural invariant, the rank, for binary codes is used to classify some of these $\mathbb{Z}_4$-linear codes. The rank is established generalizing the known results about the rank for $\mathbb{Z}_4$-linear Hadamard and $\mathbb{Z}_4$-linear extended 1-perfect codes.

Keywords: Rank, quaternary codes, Reed-Muller codes, $\mathbb{Z}_4$-linear codes.

1 Introduction

Let $\mathbb{Z}_2$ and $\mathbb{Z}_4$ be the ring of integers modulo 2 and modulo 4, respectively. Let $\mathbb{Z}_2^n$ be the set of all binary vectors of length n and let $\mathbb{Z}_4^n$ be the set of all quaternary vectors of length n. Any nonempty subset C of $\mathbb{Z}_2^n$ is a binary code and a subgroup of $\mathbb{Z}_2^n$ is called a *binary linear code* or a $\mathbb{Z}_2$*-linear code*. Equivalently, any nonempty subset $\mathcal{C}$ of $\mathbb{Z}_4^n$ is a quaternary code and a subgroup of $\mathbb{Z}_4^n$ is called a *quaternary linear code*. Some authors also use the term "quaternary codes" to refer to additive codes over $GF(4)$ [1], but note that these are not the codes we are considering in this paper.

The *Hamming distance* $d_H(u,v)$ between two vectors $u, v \in \mathbb{Z}_2^n$ is the number of coordinates in which u and v differ. The *Hamming weight* of a vector $u \in \mathbb{Z}_2^n$, denoted by $w_H(u)$, is the number of nonzero coordinates of u. The *minimum Hamming distance* of a binary code C is the minimum value of $d_H(u,v)$ for $u, v \in C$ satisfying $u \neq v$.

The Gray map, $\phi : \mathbb{Z}_4^n \longrightarrow \mathbb{Z}_2^{2n}$ given by $\phi(v_1, \ldots, v_n) = (\varphi(v_1), \ldots, \varphi(v_n))$ where $\varphi(0) = (0,0)$, $\varphi(1) = (0,1)$, $\varphi(2) = (1,1)$, $\varphi(3) = (1,0)$, is an isometry which transforms Lee distances over $\mathbb{Z}_4^n$ into Hamming distances over $\mathbb{Z}_2^{2n}$.

Let $\mathcal{C}$ be a quaternary linear code. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$, it is isomorphic to an abelian structure $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, $\mathcal{C}$ is of type $2^\gamma 4^\delta$ as a group, it has $|\mathcal{C}| = 2^{\gamma+2\delta}$ codewords and $2^{\gamma+\delta}$ codewords of order two. The binary image

[⋆] This work was supported in part by the Spanish MEC and the European FEDER under Grant MTM2006-03250.

M. Bras-Amorós and T. Høholdt (Eds.): AAECC 2009, LNCS 5527, pp. 43–52, 2009.

$C = \phi(\mathcal{C})$ of any quaternary linear code $\mathcal{C}$ of length n and type $2^\gamma 4^\delta$ is called a $\mathbb{Z}_4$-*linear code* of binary length $N = 2n$ and type $2^\gamma 4^\delta$.

Two binary codes C_1 and C_2 of length n are said to be *isomorphic* if there is a coordinate permutation π such that $C_2 = \{\pi(c) \ : \ c \in C_1\}$. They are said to be *equivalent* if there is a vector $a \in \mathbb{Z}_2^n$ and a coordinate permutation π such that $C_2 = \{a + \pi(c) \ : \ c \in C_1\}$ [11]. Two quaternary linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ both of length n and type $2^\gamma 4^\delta$ are said to be *monomially equivalent*, if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. They are said to be *permutation equivalent* if they differ only by a permutation of coordinates [9]. Note that if two quaternary linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are monomially equivalent, then the corresponding $\mathbb{Z}_4$-linear codes $C_1 = \phi(\mathcal{C}_1)$ and $C_2 = \phi(\mathcal{C}_2)$ are isomorphic.

Two structural invariants for binary codes are the rank and dimension of the kernel. The *rank* of a binary code C, denoted by r_C, is simply the dimension of $\langle C \rangle$, which is the linear span of the codewords of C. The *kernel* of a binary code C, denoted by $K(C)$, is the set of vectors that leave C invariant under translation, i.e. $K(C) = \{x \in \mathbb{Z}_2^n \ : \ C + x = C\}$. If C contains the all-zero vector, then $K(C)$ is a binary linear subcode of C. The dimension of the kernel of C will be denoted by k_C. These two invariants do not give a full classification of binary codes, since two nonisomorphic binary codes could have the same rank and dimension of the kernel. In spite of that, they can help in classification, since if two binary codes have different ranks or dimensions of the kernel, they are nonisomorphic.

It is well-known that an easy way to built the binary linear Reed-Muller family of codes, denoted by RM, is using the Plotkin construction [11]. In [14],[15], Pujol et al. introduced new quaternary Plotkin constructions to build new families of quaternary linear Reed-Muller codes, denoted by $\mathcal{RM}_s$. The quaternary linear Reed-Muller codes $\mathcal{RM}_s(r,m)$ of length 2^{m-1}, for $m \geq 1$, $0 \leq r \leq m$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$, in these new families satisfy that the corresponding $\mathbb{Z}_4$-linear codes have the same parameters and properties (length, dimension, minimum distance, inclusion and duality relationship) as the binary linear codes in the well-known RM family. In the binary case, there is only one family. In contrast, in the quaternary case, for each m there are $\lfloor \frac{m+1}{2} \rfloor$ families, which will be distinguished using subindexes s from the set $\{0, \ldots, \lfloor \frac{m-1}{2} \rfloor\}$.

The dimension of the kernel and rank have been studied for some families of $\mathbb{Z}_4$-linear codes [2], [4], [5], [10], [12]. In the RM family, the $RM(1,m)$ and $RM(m-2,m)$ binary codes are a linear Hadamard and extended 1-perfect code, respectively. Recall that a Hadamard code of length $n = 2^m$ is a binary code with $2n$ codewords and minimum Hamming distance $n/2$, and an extended 1-perfect code of length $n = 2^m$ is a binary code with 2^{n-m} codewords and minimum Hamming distance 4. Equivalently, in the $\mathcal{RM}_s$ families, the corresponding $\mathbb{Z}_4$-linear code of any $\mathcal{RM}_s(1,m)$ and $\mathcal{RM}_s(m-2,m)$ is a Hadamard and extended 1-perfect code, respectively [14],[15]. For the corresponding $\mathbb{Z}_4$-linear codes of $\mathcal{RM}_s(1,m)$ and $\mathcal{RM}_s(m-2,m)$, the rank were studied and computed in [5],[10].

Specifically,

$$r_H = \begin{cases} \gamma + 2\delta & \text{if } s = 0,1 \\ \gamma + 2\delta + \binom{\delta-1}{2} & \text{if } s \geq 2 \end{cases} \quad \text{and} \tag{1}$$

$r_P = \bar{\gamma} + 2\bar{\delta} + \delta = 2^{m-1} + \bar{\delta}$ (except $r_P = 11$, if $m = 4$ and $s = 0$), where $H = \phi(\mathcal{RM}_s(1,m))$ of type $2^{\gamma}4^{\delta}$ and $P = \phi(\mathcal{RM}_s(m-2,m))$ of type $2^{\bar{\gamma}}4^{\bar{\delta}}$.

The dimension of the kernel was computed for all $\mathcal{RM}_s(r,m)$ codes in [13]. The aim of this paper is the study of the rank for these codes, generalizing the known results about the rank for the $\mathcal{RM}_s(r,m)$ codes with $r \in \{0, 1, m-2, m-1, m\}$ [5],[10]. The paper is organized as follows. In Section 2, we recall some properties related to quaternary linear codes and the rank of these codes. Moreover, we describe the construction of the $\mathcal{RM}_s$ families of codes. In Section 3, we establish the rank for all codes in the $\mathcal{RM}_s$ families with $s \in \{0,1\}$. Furthermore, we establish the rank for the $\mathcal{RM}_s(r,m)$ codes with $r \in \{2, m-3\}$. In Section 4, we show that the rank allows us to classify the $\mathcal{RM}_s(r,m)$ codes with $r \in \{2, m-3\}$. Finally, the conclusions are given in Section 5.

2 Preliminaries

2.1 Quaternary Linear Codes

Let $\mathcal{C}$ be a quaternary linear code of length n and type $2^{\gamma}4^{\delta}$. Although $\mathcal{C}$ is not a free module, every codeword is uniquely expressible in the form

$$\sum_{i=1}^{\gamma} \lambda_i u_i + \sum_{j=1}^{\delta} \mu_j v_j,$$

where $\lambda_i \in \mathbb{Z}_2$ for $1 \leq i \leq \gamma$, $\mu_j \in \mathbb{Z}_4$ for $1 \leq j \leq \delta$ and u_i, v_j are vectors in $\mathbb{Z}_4^n$ of order two and four, respectively. The vectors u_i, v_j give us a generator matrix $\mathcal{G}$ of size $(\gamma + \delta) \times n$ for the code $\mathcal{C}$. In [8], it was shown that any quaternary linear code of type $2^{\gamma}4^{\delta}$ is permutation equivalent to a quaternary linear code with a canonical generator matrix of the form

$$\begin{pmatrix} 2T & 2I_{\gamma} & \mathbf{0} \\ S & R & I_{\delta} \end{pmatrix}, \tag{2}$$

where R, T are matrices over $\mathbb{Z}_2$ of size $\delta \times \gamma$ and $\gamma \times (n - \gamma - \delta)$, respectively; and S is a matrix over $\mathbb{Z}_4$ of size $\delta \times (n - \gamma - \delta)$.

The concepts of duality for quaternary linear codes were also studied in [8], where the inner product for any two vectors $u, v \in \mathbb{Z}_4^n$ is defined as $u \cdot v = \sum_{i=1}^{n} u_i v_i \in \mathbb{Z}_4$. Then, the *dual code* of $\mathcal{C}$, denoted by $\mathcal{C}^{\perp}$, is defined in the standard way $\mathcal{C}^{\perp} = \{v \in \mathbb{Z}_4^n : u \cdot v = 0 \text{ for all } u \in \mathcal{C}\}$. The corresponding binary code $\phi(\mathcal{C}^{\perp})$ is denoted by $C_{\perp}$ and called the $\mathbb{Z}_4$-*dual code* of $C = \phi(\mathcal{C})$. Moreover, the dual code $\mathcal{C}^{\perp}$, which is also a quaternary linear code, is of type $2^{\gamma}4^{n-\gamma-\delta}$.

Let $u * v$ denote the component-wise product for any $u, v \in \mathbb{Z}_4^n$.

Lemma 1 ([6],[7]). *Let $\mathcal{C}$ be a quaternary linear code of type $2^{\gamma}4^{\delta}$ and let $C = \phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_4$-linear code. Let $\mathcal{G}$ be a generator matrix of $\mathcal{C}$ and let $\{u_i\}_{i=1}^{\gamma}$ be the rows of order two and $\{v_j\}_{j=0}^{\delta}$ the rows of order four in $\mathcal{G}$. Then, $\langle C \rangle$ is generated by $\{\phi(u_i)\}_{i=1}^{\gamma}$, $\{\phi(v_j), \phi(2v_j)\}_{j=1}^{\delta}$ and $\{\phi(2v_j * v_k)\}_{1 \leq j < k \leq \delta}$.*

2.2 Quaternary Linear Reed-Muller Codes

Recall that a binary linear rth-order Reed-Muller code $RM(r,m)$ with $0 \leq r \leq m$ and $m \geq 2$ can be described using the Plotkin construction as follows [11]:

$$RM(r,m) = \{(u|u+v) \; : \; u \in RM(r,m-1), \, v \in RM(r-1,m-1)\},$$

where $RM(0,m)$ is the repetition code $\{\mathbf{0},\mathbf{1}\}$, $RM(m,m)$ is the universe code, and "|" denotes concatenation. For $m=1$, there are only two codes: the repetition code $RM(0,1)$ and the universe code $RM(1,1)$. This RM family of codes has length 2^m, minimum distance 2^{m-r} and dimension $\displaystyle\sum_{i=0}^{r}\binom{m}{i}$. Moreover, the code $RM(r-1,m)$ is a subcode of $RM(r,m)$ and the code $RM(r,m)$ is the dual code of $RM(m-1-r,m)$ for $0 \leq r < m$.

In the recent literature [2],[3],[8],[16],[17] several families of quaternary linear codes have been proposed and studied trying to generalize the RM family. However, when the corresponding $\mathbb{Z}_4$-linear codes are taken, they do not satisfy all the same properties as the RM family. In [14],[15], new quaternary linear Reed-Muller families, $\mathcal{RM}_s$, such that the corresponding $\mathbb{Z}_4$-linear codes have the parameters and properties of RM family of codes, were proposed. The following two constructions are necessary to generate these new $\mathcal{RM}_s$ families.

Definition 2 (Plotkin Construction). *Let $\mathcal{A}$ and $\mathcal{B}$ be two quaternary linear codes of length n, types $2^{\gamma_\mathcal{A}}4^{\delta_\mathcal{A}}$ and $2^{\gamma_\mathcal{B}}4^{\delta_\mathcal{B}}$, and minimum distances $d_\mathcal{A}$ and $d_\mathcal{B}$, respectively. A new quaternary linear code $\mathcal{PC}(\mathcal{A},\mathcal{B})$ is defined as*

$$\mathcal{PC}(\mathcal{A},\mathcal{B}) = \{(u|u+v) \; : \; u \in \mathcal{A}, v \in \mathcal{B}\}.$$

It is easy to see that if $\mathcal{G}_\mathcal{A}$ and $\mathcal{G}_\mathcal{B}$ are generator matrices of $\mathcal{A}$ and $\mathcal{B}$, respectively, then the matrix

$$\mathcal{G}_{PC} = \begin{pmatrix} \mathcal{G}_\mathcal{A} & \mathcal{G}_\mathcal{A} \\ 0 & \mathcal{G}_\mathcal{B} \end{pmatrix}$$

is a generator matrix of the code $\mathcal{PC}(\mathcal{A},\mathcal{B})$. Moreover, the code $\mathcal{PC}(\mathcal{A},\mathcal{B})$ is of length $2n$, type $2^{\gamma_\mathcal{A}+\gamma_\mathcal{B}}4^{\delta_\mathcal{A}+\delta_\mathcal{B}}$, and minimum distance $d = min\{2d_\mathcal{A}, d_\mathcal{B}\}$ [14],[15].

Definition 3 (BQ-Plotkin Construction). *Let $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ be three quaternary linear codes of length n; types $2^{\gamma_\mathcal{A}}4^{\delta_\mathcal{A}}$, $2^{\gamma_\mathcal{B}}4^{\delta_\mathcal{B}}$, and $2^{\gamma_\mathcal{C}}4^{\delta_\mathcal{C}}$; and minimum distances $d_\mathcal{A}$, $d_\mathcal{B}$, and $d_\mathcal{C}$, respectively. Let $\mathcal{G}_\mathcal{A}$, $\mathcal{G}_\mathcal{B}$, and $\mathcal{G}_\mathcal{C}$ be generator matrices of the codes $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$, respectively. A new code $\mathcal{BQ}(\mathcal{A},\mathcal{B},\mathcal{C})$ is defined as the quaternary linear code generated by*

$$\mathcal{G}_{BQ} = \begin{pmatrix} \mathcal{G}_\mathcal{A} & \mathcal{G}_\mathcal{A} & \mathcal{G}_\mathcal{A} & \mathcal{G}_\mathcal{A} \\ 0 & \mathcal{G}'_\mathcal{B} & 2\mathcal{G}'_\mathcal{B} & 3\mathcal{G}'_\mathcal{B} \\ 0 & 0 & \hat{\mathcal{G}}_\mathcal{B} & \hat{\mathcal{G}}_\mathcal{B} \\ 0 & 0 & 0 & \mathcal{G}_C \end{pmatrix},$$

where $\mathcal{G}'_\mathcal{B}$ is the matrix obtained from $\mathcal{G}_\mathcal{B}$ after switching twos by ones in their $\gamma_\mathcal{B}$ rows of order two, and $\hat{\mathcal{G}}_\mathcal{B}$ is the matrix obtained from $\mathcal{G}_\mathcal{B}$ after removing their $\gamma_\mathcal{B}$ rows of order two.

The code $\mathcal{BQ}(\mathcal{A},\mathcal{B},\mathcal{C})$ is of length $4n$, type $2^{\gamma_{\mathcal{A}}+\gamma_{\mathcal{C}}}4^{\delta_{\mathcal{A}}+\gamma_{\mathcal{B}}+2\delta_{\mathcal{B}}+\delta_{\mathcal{C}}}$, and minimum distance $d = min\{4d_{\mathcal{A}}, 2d_{\mathcal{B}}, d_{\mathcal{C}}\}$ [14],[15].

Now, the quaternary linear Reed-Muller codes $\mathcal{RM}_s(r,m)$ of length 2^{m-1}, for $m \geq 1$, $0 \leq r \leq m$, and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$, will be defined. For the recursive construction it will be convenient to define them also for $r < 0$ and $r > m$. We begin by considering the trivial cases. The code $\mathcal{RM}_s(r,m)$ with $r < 0$ is defined as the zero code. The code $\mathcal{RM}_s(0,m)$ is defined as the repetition code with only the all-zero and all-two vectors. The code $\mathcal{RM}_s(r,m)$ with $r \geq m$ is defined as the whole space $\mathbb{Z}_4^{m-1}$. For $m = 1$, there is only one family with $s = 0$, and in this family there are only the zero, repetition and universe codes for $r < 0$, $r = 0$ and $r \geq 1$, respectively. In this case, the generator matrix of $\mathcal{RM}_0(0,1)$ is $\mathcal{G}_{0(0,1)} = \begin{pmatrix} 2 \end{pmatrix}$ and the generator matrix of $\mathcal{RM}_0(1,1)$ is $\mathcal{G}_{0(1,1)} = \begin{pmatrix} 1 \end{pmatrix}$.

For any $m \geq 2$, given $\mathcal{RM}_s(r,m-1)$ and $\mathcal{RM}_s(r-1,m-1)$ codes, where $0 \leq s \leq \lfloor \frac{m-2}{2} \rfloor$, the $\mathcal{RM}_s(r,m)$ code can be constructed in a recursive way using the Plotkin construction given by Definition 2 as follows:

$$\mathcal{RM}_s(r,m) = \mathcal{PC}(\mathcal{RM}_s(r,m-1), \mathcal{RM}_s(r-1,m-1)).$$

For example, for $m = 2$, the generator matrices of $\mathcal{RM}_0(r,2)$, $0 \leq r \leq 2$, are the following:

$$\mathcal{G}_{0(0,2)} = \begin{pmatrix} 2\ 2 \end{pmatrix}; \quad \mathcal{G}_{0(1,2)} = \begin{pmatrix} 0\ 2 \\ 1\ 1 \end{pmatrix}; \quad \mathcal{G}_{0(2,2)} = \begin{pmatrix} 1\ 0 \\ 0\ 1 \end{pmatrix}.$$

Note that when m is odd, the $\mathcal{RM}_s$ family with $s = \frac{m-1}{2}$ can not be generated using the Plotkin construction. In this case, for any $m \geq 3$, m odd and $s = \frac{m-1}{2}$, given $\mathcal{RM}_{s-1}(r,m-2)$, $\mathcal{RM}_{s-1}(r-1,m-2)$ and $\mathcal{RM}_{s-1}(r-2,m-2)$, the $\mathcal{RM}_s(r,m)$ code can be constructed using the BQ-Plotkin construction given by Definition 3 as follows:

$$\mathcal{RM}_s(r,m) = \mathcal{BQ}(\mathcal{RM}_{s-1}(r,m-2), \mathcal{RM}_{s-1}(r-1,m-2), \mathcal{RM}_{s-1}(r-2,m-2)).$$

For example, for $m = 3$, there are two families. The $\mathcal{RM}_0$ family can be generated using the Plotkin construction. On the other hand, the $\mathcal{RM}_1$ family has to be generated using the BQ-Plotkin construction. The generator matrices of $\mathcal{RM}_1(r,3)$, $0 \leq r \leq 3$, are the following: $\mathcal{G}_{1(0,3)} = \begin{pmatrix} 2\ 2\ 2\ 2 \end{pmatrix}$;

$$\mathcal{G}_{1(1,3)} = \begin{pmatrix} 1\ 1\ 1\ 1 \\ 0\ 1\ 2\ 3 \end{pmatrix}; \quad \mathcal{G}_{1(2,3)} = \begin{pmatrix} 1\ 1\ 1\ 1 \\ 0\ 1\ 2\ 3 \\ 0\ 0\ 1\ 1 \\ 0\ 0\ 0\ 2 \end{pmatrix}; \quad \mathcal{G}_{1(3,3)} = \begin{pmatrix} 1\ 1\ 1\ 1 \\ 0\ 1\ 2\ 3 \\ 0\ 0\ 1\ 1 \\ 0\ 0\ 0\ 1 \end{pmatrix}.$$

Table 1 shows the type $2^\gamma 4^\delta$ of all these $\mathcal{RM}_s(r,m)$ codes for $m \leq 10$.

The following proposition summarizes the parameters and properties of these $\mathcal{RM}_s$ families of codes.

Proposition 4 ([14],[15]). *A quaternary linear Reed-Muller code $\mathcal{RM}_s(r,m)$, with $m \geq 1$, $0 \leq r \leq m$, and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$, has the following parameters and properties:*

1. *the length is* $n = 2^{m-1}$*;*
2. *the minimum distance is* $d = 2^{m-r}$*;*
3. *the number of codewords is* 2^k*, where* $k = \sum_{i=0}^{r} \binom{m}{i}$*;*
4. *the code* $\mathcal{RM}_s(r-1,m)$ *is a subcode of* $\mathcal{RM}_s(r,m)$ *for* $0 \leq r \leq m$*;*
5. *the codes* $\mathcal{RM}_s(1,m)$ *and* $\mathcal{RM}_s(m-2,m)$*, after the Gray map, are* $\mathbb{Z}_4$*-linear Hadamard and* $\mathbb{Z}_4$*-linear extended perfect codes, respectively;*
6. *the code* $\mathcal{RM}_s(r,m)$ *is the dual code of* $\mathcal{RM}_s(m-1-r,m)$ *for* $-1 \leq r \leq m$*.*

3 Rank for Some Infinite Families of $\mathcal{RM}_s(r,m)$ Codes

In this section, we will compute the rank for some infinite families of the quaternary linear Reed-Muller codes $\mathcal{RM}_s(r,m)$. The rank of $\mathcal{RM}_s(r,m)$ will be denoted by $r_{s(r,m)}$ instead of $r_{\mathcal{RM}_s(r,m)}$.

First of all, we will recall the result that gives us which of the $\mathcal{RM}_s(r,m)$ codes are binary liner codes after the Gray map. Note that if we have a quaternary linear code of type $2^\gamma 4^\delta$ which is a binary linear code after the Gray map, we can compute the rank as $\gamma + 2\delta$ [6],[7].

Proposition 5 ([13]). *For all* $m \geq 1$*, the corresponding* $\mathbb{Z}_4$*-linear code of the* $\mathcal{RM}_s(r,m)$ *code is a binary linear code if and only if*

$$\begin{cases} s = 0 \text{ and } r \in \{0,1,2,m-1,m\}, \\ s = 1 \text{ and } r \in \{0,1,m-1,m\}, \\ s \geq 2 \text{ and } r \in \{0,m-1,m\}. \end{cases}$$

Now, we will give an expression for the parameters γ and δ of a quaternary linear Reed-Muller code $\mathcal{RM}_s(r,m)$ of type $2^\gamma 4^\delta$, depending on s, r and m.

Lemma 6. *Let* $\mathcal{C}$ *be a quaternary linear Reed-Muller code* $\mathcal{RM}_s(r,m)$ *of type* $2^\gamma 4^\delta$*. Then, for* $s \geq 0$*,* $m \geq 2s+1$ *and* $0 \leq r \leq m$*,*

$$\gamma = \sum_{i=0}^{\lfloor \frac{r}{2} \rfloor} \binom{m-2s-1}{r-2i}\binom{s}{i} \quad \text{and} \quad \delta = \frac{1}{2}\sum_{i=0}^{r}\binom{m}{i} - \frac{\gamma}{2}.$$

The next proposition gives us an important result for these quaternary linear Reed-Muller codes. In some cases, we obtain two codes with the same rank, but different s. We will prove that these codes are equal. This proposition will be used for the classification of some of the $\mathcal{RM}_s(r,m)$ codes in Section 4, and it will also be used to calculate the rank of these codes as exceptions.

Proposition 7. *Given two codes* $\mathcal{RM}_s(r,m)$ *and* $\mathcal{RM}_{s-1}(r,m)$ *of type* $2^\gamma 4^\delta$ *and* $2^{\gamma'} 4^{\delta'}$*, respectively, such that* $m \geq 3$ *is odd,* $r \geq 2$ *is even, and* $s = \frac{m-1}{2}$*, then* $\mathcal{RM}_s(r,m) = \mathcal{RM}_{s-1}(r,m)$*.*

Proof. The generator matrix $\mathcal{G}_{s-1(r,m)}$ of $\mathcal{RM}_{s-1}(r,m)$ is obtained using the Plotkin construction from $\mathcal{RM}_{s-1}(r-1,m-1)$ and $\mathcal{RM}_{s-1}(r,m-1)$. Furthermore, the generator matrices of $\mathcal{RM}_{s-1}(r-1,m-1)$ and $\mathcal{RM}_{s-1}(r,m-1)$ can be obtained using Plotkin construction again from codes with $m-2$ value. So we can write the generator matrix $\mathcal{G}_{s-1(r,m)}$ as follows:

$$\mathcal{G}_{s-1(r,m)} = \begin{pmatrix} \mathcal{G}_{s-1(r,m-2)} & \mathcal{G}_{s-1(r,m-2)} & \mathcal{G}_{s-1(r,m-2)} & \mathcal{G}_{s-1(r,m-2)} \\ 0 & \mathcal{G}_{s-1(r-1,m-2)} & 0 & \mathcal{G}_{s-1(r-1,m-2)} \\ 0 & 0 & \mathcal{G}_{s-1(r-1,m-2)} & \mathcal{G}_{s-1(r-1,m-2)} \\ 0 & 0 & 0 & \mathcal{G}_{s-1(r-2,m-2)} \end{pmatrix}.$$

The generator matrix $\mathcal{G}_{s(r,m)}$ of $\mathcal{RM}_s(r,m)$ can be obtained using the BQ-Plotkin construction given by Definition 3. Since r is even and m is odd, $r-1$ and $m-2$ are odd. In this case any $\mathcal{RM}_{s-1}(r-1,m-2)$ code, where $s = \frac{m-1}{2}$, is of type $2^0 4^{\delta''}$. This result can be proved by induction on m and using the BQ-Plotkin construction. Since $\mathcal{G}_{s-1(r-1,m-2)}$ is of type $2^0 4^{\delta''}$, then $\mathcal{G}'_{s-1(r-1,m-2)} = \mathcal{G}_{s-1(r-1,m-2)}$ and $\hat{\mathcal{G}}_{s-1(r-1,m-2)} = \mathcal{G}_{s-1(r-1,m-2)}$. It is easy to find a linear combination of rows that transforms the matrix $\mathcal{G}_{s-1(r,m)}$ into the matrix $\mathcal{G}_{s(r,m)}$.

Now, we will give a recursive way to compute the rank for all Reed-Muller codes in the $\mathcal{RM}_0$ and $\mathcal{RM}_1$ families. Note that the first binary nonlinear code is $\mathcal{RM}_0(3,5)$. Thus, for $m < 5$ the rank is $\gamma + 2\delta$.

Proposition 8. *Let $\mathcal{C}$ be a quaternary linear Reed-Muller code $\mathcal{RM}_0(r,m)$. The rank of $\mathcal{C}$ for $m \geq 5$ is*

$$r_{0(r,m)} = r_{0(r,m-1)} + r_{0(r-1,m-1)} + \begin{cases} 0 & \text{if } r \in \{0,1,2,m-1,m\} \\ \binom{m-2}{2r-3} & \text{if } r \in \{3,\ldots,m-2\} \end{cases}$$

Proposition 9. *Let $\mathcal{C}$ be a quaternary linear Reed-Muller code $\mathcal{RM}_1(r,m)$. The rank of $\mathcal{C}$ for $m \geq 5$ is*

$$r_{1(r,m)} = r_{1(r,m-1)} + r_{1(r-1,m-1)} + \begin{cases} 0 & \text{if } r \in \{0,1,m-1,m\} \\ m-2 & \text{if } r = 2 \\ 2\binom{m-1}{2r-3} & \text{if } r \in \{3,\ldots,m-2\}. \end{cases}$$

The next proposition gives the rank for all quaternary linear Reed-Muller codes with $r \in \{0,1,m-3,m-2,m-1,m\}$ and any s.

Proposition 10. *Let $\mathcal{RM}_s(r,m)$ be a quaternary linear Reed-Muller code of type $2^\gamma 4^\delta$. The rank of $\mathcal{RM}_s(r,m)$ can be computed as*

$$r_{s(r,m)} = \begin{cases} \gamma + 2\delta & \text{if } r \in \{0,m-1,m\} \\ \gamma + 2\delta & \text{if } r = 1 \text{ and } s \in \{0,1\} \\ \gamma + 2\delta + \binom{\delta-1}{2} & \text{if } r = 1 \text{ and } s \geq 2 \\ 2^{m-1} + \delta & \text{if } r = m-3 \text{ and } m > 6 \\ 2^{m-1} + \delta & \text{if } r = m-2 \text{ and } m > 4. \end{cases}$$

Finally, the next proposition gives a recursive way to compute the rank of all quaternary linear Reed-Muller codes with $r = 2$ and any s.

Proposition 11. *Let $\mathcal{RM}_s(2,m)$ be a quaternary linear Reed-Muller code of type $2^\gamma 4^\delta$. The rank of $\mathcal{RM}_s(2,m)$ can be computed as*

$$r_{s(2,m)} = r_{s(2,m-1)} + r_{s(1,m-1)} + 2s + \binom{s+1}{2}(m-s-3),$$

except when m is odd and $s = \frac{m-1}{2}$, since the rank is $r_{s(2,m)} = r_{s-1(2,m)}$.

When m is odd and $s = \frac{m-1}{2}$, by Proposition 7, the codes $\mathcal{RM}_s(2,m)$ and $\mathcal{RM}_{s-1}(2,m)$ are equals. Thus, the rank is also the same. Note that, for $s = 0$ and $r = 2$, we have a binary linear code and the rank is $\gamma + 2\delta$.

4 Classification of Some Families of $\mathcal{RM}_s(r,m)$ Codes

In this section, we will show that this invariant, the rank, will allow us to classify these $\mathcal{RM}_s(r,m)$ codes in some cases depending on the parameter r. This classification was given for $r = 1$ and $r = m - 2$ [5], [10]. Now, we will extend this result for $r = 2$ and $r = m - 3$. We are close to generalize this result for all $0 \leq r \leq m$, but it is not easy to obtain a general form to compute the rank for all quaternary linear Reed-Muller codes $\mathcal{RM}_s(r,m)$.

Table 1 shows the type $2^\gamma 4^\delta$ and the rank of all these $\mathcal{RM}_s(r,m)$ codes for $m \leq 10$. In these examples, you can see that the rank is always different, except for the codes quoted in Proposition 7. If two codes have different rank, we can say that they are nonisomorphic. The next theorem proves that for a given $m \geq 4$, and $r \in \{2, m-3\}2$, the $\mathcal{RM}_s(r,m)$ codes have different rank, so they are nonisomorphic. In some cases, there is an exception, but we know by Proposition 7 that the codes are equal.

Theorem 12. *For all $m \geq 4$ and $r \in \{2, m-3\}$, there are at least $\lfloor \frac{m+1}{2} \rfloor$ nonisomorphic binary codes with the same parameters as the code $RM(r,m)$, except when m is odd, and r is even. In this case, there are at least $\frac{m-1}{2}$ nonisomorphic binary codes with the same parameters as the code $RM(r,m)$.*

Proof. By Proposition 11, we know that $r_{s(2,m)} = r_{s(2,m-1)} + r_{s(1,m-1)} + 2s + \binom{s+1}{2}(m-s-3)$. If $r = 1$, the code is Hadamard and $r_{s(1,m-1)}$ increases or is equal to, depending on s. For $m \geq 4$ the expression $2s + \binom{s+1}{2}(m-s-3)$ also increases, depending on s. We can suppose that $r_{s(2,m-1)}$ is crescent on s for $m = 4$ and proceed by induction on m. Therefore, $r_{s(2,m)}$ is different for every s, except when m is odd, where we have two codes with the same rank. By Proposition 7, these two codes are equal.

By Proposition 10, we know that $r_{s(m-3,m)} = 2^{m-1} + \delta$. In Proposition 6, we can see a way to compute γ. Since $r = m - 3$, then the value of γ is decreasing on s. Thus, δ is crescent and the rank is also crescent, depending on s. When m is odd and r is even, we have again the case of two equal codes, solved in Proposition 7.

Table 1. Type $2^{\gamma}4^{\delta}$ and rank $r_{s(r,m)}$ for all $\mathcal{RM}_s(r,m)$ codes with $m \leq 10$ and $r \in \{0,1,2,3\}$, showing them in the form $(\gamma,\delta)\ r_{s(r,m)}$

m	s r	0	1	2		$m-3$	$m-2$	$m-1$	m
1	0	(1,0) 1	(0,1) 2					(1,0) 1	(0,1) 2
2	0	(1,0) 1	(1,1) 3	(0,2) 4			(1,0) 1	(1,1) 3	(0,2) 4
3	0	(1,0) 1	(2,1) 4	(1,3) 7		(1,0) 1	(2,1) 4	(1,3) 7	(0,4) 8
	1	(1,0) 1	(0,2) 4	(1,3) 7		(1,0) 1	(0,2) 4	(1,3) 7	(0,4) 8
4	0	(1,0) 1	(3,1) 5	(3,4) 11		(3,1) 5	(3,4) 11	(1,7) 15	(0,8) 16
	1	(1,0) 1	(1,2) 5	(1,5) 13		(1,2) 5	(1,5) 13	(1,7) 15	(0,8) 16
5	0	(1,0) 1	(4,1) 6	(6,5) 16		(6,5) 16	(4,11) 27	(1,15) 31	(0,16) 32
	1	(1,0) 1	(2,2) 6	(2,7) 21		(2,7) 21	(2,12) 28	(1,15) 31	(0,16) 32
	2	(1,0) 1	(0,3) 7	(2,7) 21		(2,7) 21	(0,13) 29	(1,15) 31	(0,16) 32
6	0	(1,0) 1	(5,1) 7	(10,6) 22	(. . .)	(10,16) 47	(5,26) 58	(1,31) 63	(0,32) 64
	1	(1,0) 1	(3,2) 7	(4,9) 31	(. . .)	(4,19) 51	(3,27) 59	(1,31) 63	(0,32) 64
	2	(1,0) 1	(1,3) 8	(2,10) 35	(. . .)	(2,20) 52	(1,28) 60	(1,31) 63	(0,32) 64
7	0	(1,0) 1	(6,1) 8	(15,7) 29	(. . .)	(15,42) 106	(6,57) 121	(1,63) 127	(0,64) 128
	1	(1,0) 1	(4,2) 8	(7,11) 43	(. . .)	(7,46) 110	(4,58) 122	(1,63) 127	(0,64) 128
	2	(1,0) 1	(2,3) 9	(3,13) 53	(. . .)	(3,48) 112	(2,59) 123	(1,63) 127	(0,64) 128
	3	(1,0) 1	(0,4) 11	(3,13) 53	(. . .)	(3,48) 112	(0,60) 124	(1,63) 127	(0,64) 128
8	0	(1,0) 1	(7,1) 9	(21,8) 37	(. . .)	(21, 99) 227	(7,120) 248	(1,127) 255	(0,128) 256
	1	(1,0) 1	(5,2) 9	(11,13) 57	(. . .)	(11,104) 232	(5,121) 249	(1,127) 255	(0,128) 256
	2	(1,0) 1	(3,3) 10	(5,16) 75	(. . .)	(5,107) 235	(3,122) 250	(1,127) 255	(0,128) 256
	3	(1,0) 1	(1,4) 12	(3,17) 82	(. . .)	(3,108) 236	(1,123) 251	(1,127) 255	(0,128) 256
9	0	(1,0) 1	(8,1) 10	(28,9) 46	(. . .)	(28,219) 475	(8,247) 503	(1,255) 511	(0,256) 512
	1	(1,0) 1	(6,2) 10	(16,15) 73	(. . .)	(16,225) 481	(6,248) 504	(1,255) 511	(0,256) 512
	2	(1,0) 1	(4,3) 11	(8,19) 101	(. . .)	(8,229) 485	(4,249) 505	(1,255) 511	(0,256) 512
	3	(1,0) 1	(2,4) 13	(4,21) 118	(. . .)	(4,231) 487	(2,250) 506	(1,255) 511	(0,256) 512
	3	(1,0) 1	(0,5) 16	(4,21) 118	(. . .)	(4,231) 487	(0,251) 507	(1,255) 511	(0,256) 512
10	0	(1,0) 1	(7,1) 11	(36,10) 56	(. . .)	(36,466) 978	(9,502) 1014	(1,511) 1023	(0,512) 1024
	1	(1,0) 1	(5,2) 11	(22,17) 91	(. . .)	(22,473) 985	(7,503) 1015	(1,511) 1023	(0,512) 1024
	2	(1,0) 1	(3,3) 12	(12,22) 131	(. . .)	(12,478) 990	(5,504) 1016	(1,511) 1023	(0,512) 1024
	3	(1,0) 1	(1,4) 14	(6,25) 161	(. . .)	(6,481) 993	(3,505) 1017	(1,511) 1023	(0,512) 1024
	3	(1,0) 1	(1,5) 17	(4,26) 172	(. . .)	(4,482) 994	(1,506) 1018	(1,511) 1023	(0,512) 1024

5 Conclusions

In a recent paper [15], new families of quaternary linear codes, the $\mathcal{RM}_s(r,m)$ codes, are constructed in such a way that, after the Gray map, the $\mathbb{Z}_4$-linear codes fulfill the same properties and fundamental characteristics as the binary linear Reed-Muller codes. In this paper, a structural invariant for binary codes, the rank, is used to classify some of these new families of codes. Specifically, we classified the $\mathcal{RM}_s(r,m)$ codes with $r \in \{2, m-3\}$. The $\mathcal{RM}_s(r,m)$ codes with $r \in \{0,1,m-2,m-1,m\}$ were already classified using the rank [5],[10]. As a future research, it would be interesting to compute the rank for the $\mathcal{RM}_s(r,m)$ codes with $r \in \{3,\ldots,m-4\}$ and $s \geq 2$, in order to see whether it is possible to obtain a full classification of all these $\mathcal{RM}_s(r,m)$ codes using this invariant.

In this paper, we also proved that, when m is odd, $m \geq 5$, and r is even, there are two codes with the same rank, because these two codes are equal. Moreover, we also computed the rank for all codes in the $\mathcal{RM}_0$ and $\mathcal{RM}_1$ families.

References

1. Bierbrauer, J.: Introduction to coding theory. Chapman & Hall/CRC, Boca Raton (2005)
2. Borges, J., Fernández, C., Phelps, K.T.: Quaternary Reed-Muller codes. IEEE Trans. Inform. Theory 51(7), 2686–2691 (2005)
3. Borges, J., Fernández-Córdoba, C., Phelps, K.T.: "ZRM codes". IEEE Trans. Inform. Theory 54(1), 380–386 (2008)

4. Borges, J., Phelps, K.T., Rifà, J., Zinoviev, V.A.: On $\mathbb{Z}_4$-linear Preparata-like and Kerdock-like codes. IEEE Trans. Inform. Theory 49(11), 2834–2843 (2003)
5. Borges, J., Phelps, K.T., Rifà, J.: The rank and kernel of extended 1-perfect $\mathbb{Z}_4$-linear and additive non-$\mathbb{Z}_4$-linear codes. IEEE Trans. Inform. Theory 49(8), 2028–2034 (2003)
6. Fernández-Córdoba, C., Pujol, J., Villanueva, M.: On rank and kernel of $\mathbb{Z}_4$-linear codes. In: Barbero, A. (ed.) ICMCTA 2008. LNCS, vol. 5228, pp. 46–55. Springer, Heidelberg (2008)
7. Fernández-Córdoba, C., Pujol, J., Villanueva, M.: $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel. Discrete Applied Mathematics (2008) (submitted), arXiv:0807.4247
8. Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes. IEEE Trans. Inform. Theory 40, 301–319 (1994)
9. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
10. Krotov, D.S.: $\mathbb{Z}_4$-linear Hadamard and extended perfect codes. In: International Workshop on Coding and Cryptography, Paris, France, January 8-12, pp. 329–334 (2001)
11. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, Amsterdam (1977)
12. Phelps, K.T., Rifà, J., Villanueva, M.: On the additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes: rank and kernel. IEEE Trans. Inform. Theory 52(1), 316–319 (2006)
13. Pernas, J., Pujol, J., Villanueva, M.: Kernel dimension for some families of quaternary Reed-Muller codes. In: Calmet, J., Geiselmann, W., Müller-Quade, J. (eds.) Beth Festschrift. LNCS, vol. 5393, pp. 128–141. Springer, Heidelberg (2008)
14. Pujol, J., Rifà, J., Solov'eva, F.I.: Quaternary Plotkin constructions and quaternary Reed-Muller codes. In: Boztaş, S., Lu, H.-F(F.) (eds.) AAECC 2007. LNCS, vol. 4851, pp. 148–157. Springer, Heidelberg (2007)
15. Pujol, J., Rifà, J., Solov'eva, F.I.: Construction of $\mathbb{Z}_4$-linear Reed-Muller codes. IEEE Trans. Inform. Theory 55(1), 99–104 (2009)
16. Solov'eva, F.I.: On Z4-linear codes with parameters of Reed-Muller codes. Problems of Inform. Trans. 43(1), 26–32 (2007)
17. Wan, Z.-X.: Quaternary codes. World Scientific Publishing Co. Pte. Ltd., Singapore (1997)

Appendix C

Classification of Some Families of Quaternary Reed–Muller Codes

Classification of Some Families of Quaternary Reed–Muller Codes

Jaume Pernas, Jaume Pujol, and Mercè Villanueva

***Abstract*—Recently, new families of quaternary linear Reed–Muller codes have been introduced. They satisfy that, after the Gray map, the corresponding $\mathbb{Z}_4$-linear codes have the same parameters and properties as the codes of the binary linear Reed–Muller family. A structural invariant, the dimension of the kernel, for binary codes is used to classify completely these $\mathbb{Z}_4$-linear codes. The dimension of the kernel for these $\mathbb{Z}_4$-linear codes is established generalizing the known results about the dimension of the kernel for $\mathbb{Z}_4$-linear Hadamard and $\mathbb{Z}_4$-linear extended 1-perfect codes.**

***Index Terms*—$\mathbb{Z}_4$-linear codes, kernel, quaternary codes, Reed–Muller codes.**

I. Introduction

LET $\mathbb{Z}_2$ and $\mathbb{Z}_4$ be the ring of integers modulo 2 and modulo 4, respectively. Let $\mathbb{Z}_2^n$ be the set of all binary vectors of length n and let $\mathbb{Z}_4^n$ be the set of all quaternary vectors of length n. Any nonempty subset C of $\mathbb{Z}_2^n$ is a binary code and a subgroup of $\mathbb{Z}_2^n$ is called a binary linear code. Equivalently, any nonempty subset $\mathcal{C}$ of $\mathbb{Z}_4^n$ is a quaternary code and a subgroup of $\mathbb{Z}_4^n$ is called a quaternary linear code. The all-zero and all-one vector will be denoted by $\mathbf{0}$ and $\mathbf{1}$, respectively. Let $u * v$ denote the component-wise product for any $u, v \in \mathbb{Z}_2^n$ or $u, v \in \mathbb{Z}_4^n$. It will be clear by the context whether we refer to binary or quaternary vectors.

The *Hamming distance* $d_H(u, v)$ between two vectors $u, v \in \mathbb{Z}_2^n$ is the number of coordinates in which u and v differ. The *Hamming weight* of a vector $u \in \mathbb{Z}_2^n$, denoted by $w_H(u)$, is the number of nonzero coordinates of u. The minimum Hamming distance of a binary code C is the minimum value of $d_H(u, v)$ for $u, v \in C$ satisfying $u \neq v$. The minimum Hamming weight of a binary code C, denoted by $w_H(C)$, is the minimum value of $w_H(u)$ for $u \in C \setminus \{\mathbf{0}\}$. We define the *Lee weights* over the elements in $\mathbb{Z}_4$ as: $w_L(0) = 0$, $w_L(1) = w_L(3) = 1$, $w_L(2) = 2$. The *Lee weight* of a vector $u \in \mathbb{Z}_4^n$, denoted by $w_L(u)$, is the addition of the weights of its coordinates, whereas the *Lee distance* $d_L(u, v)$ between two vectors $u, v \in \mathbb{Z}_4^n$ is $d_L(u, v) = w_L(u - v)$. The minimum Lee distance of a quaternary code $\mathcal{C}$ is the minimum value of $d_L(u, v)$ for $u, v \in \mathcal{C}$ satisfying $u \neq v$. The minimum Lee weight of a quaternary code $\mathcal{C}$, denoted by $w_L(\mathcal{C})$, is the minimum value of $w_L(u)$ for $u \in \mathcal{C} \setminus \{\mathbf{0}\}$. The Gray map, $\phi : \mathbb{Z}_4^n \longrightarrow \mathbb{Z}_2^{2n}$ given by $\phi(v_1, \dots, v_n) = (\varphi(v_1), \dots, \varphi(v_n))$ where $\varphi(0) = (0, 0)$, $\varphi(1) = (0, 1)$, $\varphi(2) = (1, 1)$, $\varphi(3) = (1, 0)$, is an isometry which transforms Lee distances over $\mathbb{Z}_4^n$ into Hamming distances over $\mathbb{Z}_2^{2n}$. Therefore, the minimum Lee weight of a quaternary code $\mathcal{C}$ coincides with the minimum Hamming weight of $C = \phi(\mathcal{C})$.

Let $\mathcal{C}$ be a quaternary linear code. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$, it is isomorphic to an abelian structure $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, $\mathcal{C}$ is of type $2^\gamma 4^\delta$ as a group, it has $|\mathcal{C}| = 2^{\gamma+2\delta}$ codewords and $2^{\gamma+\delta}$ codewords of order two. The binary image $C = \phi(\mathcal{C})$ of any quaternary linear code $\mathcal{C}$ of length n and type $2^\gamma 4^\delta$ is called a $\mathbb{Z}_4$*-linear code* of length $2n$ and type $2^\gamma 4^\delta$.

Two binary codes C_1 and C_2 of length n are said to be *isomorphic* if there is a coordinate permutation π such that $C_2 = \{\pi(c) : c \in C_1\}$. They are said to be *equivalent* if there is a vector $a \in \mathbb{Z}_2^n$ and a coordinate permutation π such that $C_2 = \{a + \pi(c) : c \in C_1\}$ [2]. Two quaternary linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ both of length n and type $2^\gamma 4^\delta$ are said to be *monomially equivalent*, if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. They are said to be *permutation equivalent* if they differ only by a permutation of coordinates [3]. Note that if two quaternary linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are monomially equivalent, then the corresponding $\mathbb{Z}_4$-linear codes $C_1 = \phi(\mathcal{C}_1)$ and $C_2 = \phi(\mathcal{C}_2)$ are isomorphic. Therefore, if $\phi(\mathcal{C}_1)$ and $\phi(\mathcal{C}_2)$ are not isomorphic, then $\mathcal{C}_1$ and $\mathcal{C}_2$ are not monomially equivalent.

Two structural invariants for binary codes are the rank and dimension of the kernel. The *rank* of a binary code C is simply the dimension of $\langle C \rangle$, which is the linear span of the codewords of C. The *kernel* of a binary code C, denoted by $K(C)$, is the set of vectors that leave C invariant under translation, i.e., $K(C) = \{x \in \mathbb{Z}_2^n : C + x = C\}$. If C contains the all-zero vector, then $K(C)$ is a binary linear subcode of C. In general, C can be written as the union of cosets of $K(C)$, and $K(C)$ is the largest such linear code for which this is true [4]. These two invariants do not give a full classification of binary codes, since two nonisomorphic binary codes could have the same rank and dimension of the kernel. In spite of that, they can help in classification, since if two binary codes have different ranks or dimensions of the kernel, they are nonisomorphic.

In [5], Hammons *et al.* showed that several families of binary codes are $\mathbb{Z}_4$-linear. In particular, they considered the binary linear Reed–Muller family of codes, denoted by RM,

Manuscript received September 30, 2010; revised January 24, 2011; accepted January 24, 2011. Date of current version August 31, 2011. This work was supported in part by the Spanish MICINN under Grants PCI2006-A7-0616 and TIN2010-17358, and by the Catalan AGAUR under Grant 2009SGR1224. The material in this paper was presented in part at the Mathematical Methods in Computer Science Conference, Karlsruhe, Germany, December 2008 [1].

The authors are with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain.

Communicated by I. F. Blake, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2011.2119465

and proved that the binary linear rth-order Reed–Muller code $RM(r,m)$ of length 2^m is $\mathbb{Z}_4$-linear for $r=0,1,2,m-1,m$ and is not $\mathbb{Z}_4$-linear for $r=m-2$ $(m\geq 5)$. In a subsequent work [6], Hou *et al.* proved that $RM(r,m)$ is not $\mathbb{Z}_4$-linear for $3\leq r\leq m-2$ $(m\geq 5)$.

It is well-known that an easy way to build the RM family is using the Plotkin construction [2]. In [7], [8], Pujol *et al.* introduced new quaternary Plotkin constructions to build new families of quaternary linear Reed–Muller codes, denoted by $\mathcal{RM}_s$. The quaternary linear Reed–Muller codes $\mathcal{RM}_s(r,m)$ of length 2^{m-1}, defined for $m\geq 1$, $0\leq r\leq m$ and $0\leq s\leq\left\lfloor\frac{m-1}{2}\right\rfloor$, satisfy that the corresponding $\mathbb{Z}_4$-linear codes have the same parameters and properties (length, dimension, minimum distance, inclusion and duality relationship) as the binary linear codes in the well-known RM family. In the binary case, there is only one family. In contrast, in the quaternary case, for each m there are $\left\lfloor\frac{m+1}{2}\right\rfloor$ families, which will be distinguished using subindexes s from the set $\{0,\dots,\left\lfloor\frac{m-1}{2}\right\rfloor\}$. The dimension of $K(\Phi(\mathcal{RM}_s(r,m)))$ will be denoted by $k_{s,(r,m)}$.

The dimension of the kernel and rank have been studied for some families of $\mathbb{Z}_4$-linear codes [9]–[13]. In the RM family, the $RM(1,m)$ and $RM(m-2,m)$ is a linear Hadamard and extended 1-perfect code, respectively. Recall that a Hadamard code of length $n=2^m$ is a binary code with $2n$ codewords and minimum Hamming distance $n/2$, and an extended 1-perfect code of length $n=2^m$ is a binary code with 2^{n-m-1} codewords and minimum Hamming distance 4. Equivalently, in the $\mathcal{RM}_s$ families, the corresponding $\mathbb{Z}_4$-linear code of any $\mathcal{RM}_s(1,m)$ and $\mathcal{RM}_s(m-2,m)$ is a Hadamard and extended 1-perfect code, respectively [7], [8].

The dimension of the kernel and the rank of these codes were studied and computed in [11]–[13]. Specifically

$$k_{s,(1,m)}=\begin{cases}\gamma+\delta+1, & \text{if } s\geq 2\\ \gamma+2\delta & \text{if } s=0,1\end{cases}$$
$$\text{and}$$
$$k_{s,(m-2,m)}=\begin{cases}\bar{\gamma}+\bar{\delta}+1, & \text{if } s\geq 2\\ \bar{\gamma}+\bar{\delta}+2, & \text{if } s=1\\ \bar{\gamma}+\bar{\delta}+m, & \text{if } s=0\end{cases}\tag{1}$$

where the type of $\mathcal{RM}_s(1,m)$ and $\mathcal{RM}_s(m-2,m)$ is $2^\gamma 4^\delta$ and $2^{\bar{\gamma}}4^{\bar{\delta}}$, respectively.

The aim of this paper is to classify the quaternary linear Reed–Muller codes $\mathcal{RM}_s(r,m)$ for all r and m. In order to establish this classification, we will study the dimension of the kernel for these codes, generalizing the known results about the dimension of the kernel for the $\mathcal{RM}_s(1,m)$ and $\mathcal{RM}_s(m-2,m)$ codes. The paper is organized as follows. In Section II, we recall some properties related to quaternary linear codes and the kernel of these codes. Moreover, we describe the construction of the $\mathcal{RM}_s$ families of codes. In Section III, we establish the kernel and its dimension for all codes in the $\mathcal{RM}_0$ family. In Section IV, we give the main results about the kernel and its dimension for all codes in the $\mathcal{RM}_s$ families, with $s>0$. In Section V, we show that we can use this invariant, the dimension of the kernel, to classify completely the codes in the $\mathcal{RM}_s$ families. Finally, the conclusions are given in Section VI.

We would also like to mention that we have developed in Magma several functions that expand the current functionality for codes over $\mathbb{Z}_4$ [14], [15]. Specifically, these functions allow to construct the new $\mathcal{RM}_s$ families of codes and Plotkin constructions for quaternary linear codes. Moreover, there are also efficient functions for computing the rank and dimension of the kernel of any quaternary linear code. These functions are included in Magma distribution, since version 2.15–15, but they can also be downloaded from the web page http://ccsg.uab.cat.

II. Preliminaries

A. Quaternary Linear Codes

Let $\mathcal{C}$ be a quaternary linear code of length n and type $2^\gamma 4^\delta$. Although $\mathcal{C}$ is not a free module, every codeword is uniquely expressible in the form

$$\sum_{i=1}^{\gamma}\lambda_i u_i+\sum_{j=1}^{\delta}\mu_j v_j$$

where $\lambda_i\in\mathbb{Z}_2$ for $1\leq i\leq\gamma$, $\mu_j\in\mathbb{Z}_4$ for $1\leq j\leq\delta$ and u_i, v_j are vectors in $\mathbb{Z}_4^n$ of order two and four, respectively. The vectors u_i, v_j give us a generator matrix $\mathcal{G}$ of size $(\gamma+\delta)\times n$ for the code $\mathcal{C}$. The submatrices with only u_i and v_j vectors are denoted by $\mathcal{G}_\gamma$ and $\mathcal{G}_\delta$, respectively. Moreover, $\mathcal{G}$, $\mathcal{G}_\gamma$ and $\mathcal{G}_\delta$ will also be used to denote the sets of its row vectors.

The concepts of duality for quaternary linear codes were also studied in [5], where the inner product for any two vectors $u,v\in\mathbb{Z}_4^n$ is defined as $u\cdot v=u_1v_1+u_2v_2+\cdots+u_nv_n\in\mathbb{Z}_4$. Then, the *dual code* of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined in the standard way $\mathcal{C}^\perp=\{v\in\mathbb{Z}_4^n : u\cdot v=0 \text{ for all } u\in\mathcal{C}\}$. The corresponding binary code $\Phi(\mathcal{C}^\perp)$ is denoted by $C_\perp$ and called the $\mathbb{Z}_4$-*dual code* of $C=\Phi(\mathcal{C})$. Moreover, the dual code $\mathcal{C}^\perp$, which is also a quaternary linear code, is of type $2^\gamma 4^{n-\gamma-\delta}$.

Let $\mathcal{C}$ be a quaternary linear code and let $C=\Phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_4$-linear code with kernel $K(C)$. The kernel of $\mathcal{C}$, denoted by $\mathcal{K}(\mathcal{C})$, is defined as the inverse Gray map image of $K(C)$, that is $\mathcal{K}(\mathcal{C})=\Phi^{-1}(K(C))$. Furthermore, the dimension of $\mathcal{K}(\mathcal{C})$ is defined as the dimension of $K(C)$. The following lemma gives another way to describe $\mathcal{K}(\mathcal{C})$.

Lemma 1 ([16], [17]): Let $\mathcal{C}$ be a quaternary linear code. Then, $\mathcal{K}(\mathcal{C})=\{u : u\in\mathcal{C} \text{ and } 2u*v\in\mathcal{C},\ \forall v\in\mathcal{C}\}$.

Note that if $\mathcal{G}$ is a generator matrix of a quaternary linear code $\mathcal{C}$, then $u\in\mathcal{K}(\mathcal{C})$ if and only if $u\in\mathcal{C}$ and $2u*v\in\mathcal{C}$ for all $v\in\mathcal{G}$. Moreover, all codewords of order two in $\mathcal{C}$ belong to $\mathcal{K}(\mathcal{C})$. It is also clear that if $\mathbf{1}\in\mathcal{C}$, then $\mathbf{1}\in\mathcal{K}(\mathcal{C})$. Finally, we mention that $\mathcal{K}(\mathcal{C})$ is a quaternary linear subcode of $\mathcal{C}$ and its dimension defined as above is $\gamma+2\delta-\kappa$, where $\kappa\in\{0,2,\dots,\delta\}$, and that there exists a set $\{v_1,v_2,\dots,v_\kappa\}$ of row vectors of order four in $\mathcal{G}$, such that

$$\mathcal{C}=\bigcup_{I\subseteq\{1,\dots,\kappa\}}(\mathcal{K}(\mathcal{C})+v_I)\tag{2}$$

where $I=\{i_1,\dots,i_l\}$ and $v_I=v_{i_1}+\cdots+v_{i_l}$. If $I=\emptyset$ then $v_I=\mathbf{0}$. [16], [17].

B. Quaternary Linear Reed–Muller Codes

Recall that a binary linear rth-order Reed–Muller code $RM(r,m)$, with $m \ge 2$ and $0 \le r \le m$, can be described using the Plotkin construction as follows [2]:

$$RM(r,m) = \{(u|u+v) : u \in RM(r,m-1),\\ v \in RM(r-1,m-1)\}$$

where $RM(0,m)$ is the repetition code $\{0,1\}$, $RM(m,m)$ is the universe code, and "|" denotes concatenation. For $m=1$, there are only two codes: the repetition code $RM(0,1)$ and the universe code $RM(1,1)$. This RM family has the parameters and properties quoted in the following proposition.

Proposition 2 ([2]): A binary linear rth-order Reed–Muller code $RM(r,m)$, with $m \ge 1$ and $0 \le r \le m$, has the following parameters and properties:

1) the length is $n = 2^m$;
2) the minimum Hamming distance is $d = 2^{m-r}$;
3) the dimension is $\sum_{i=0}^{r} \binom{m}{i}$;
4) the code $RM(r-1,m)$ is a subcode of $RM(r,m)$ for $0 < r \le m$;
5) the code $RM(r,m)$ is the dual code of $RM(m-1-r,m)$ for $0 \le r < m$.

In the recent literature [5], [9], [18]–[20] several families of quaternary linear codes have been proposed and studied trying to generalize the RM family. However, when the corresponding $\mathbb{Z}_2$-linear codes are taken, they do not satisfy all the properties quoted in Proposition 2. In [7], [8], new quaternary linear Reed–Muller families, $\mathcal{RM}_s$, such that the corresponding $\mathbb{Z}_2$-linear codes have the parameters and properties described in Proposition 2, were proposed. The following two Plotkin constructions are necessary to generate these new $\mathcal{RM}_s$ families.

Definition 3 (Plotkin Construction): Let $\mathcal{A}$ and $\mathcal{B}$ be two quaternary linear codes of length n, types $2^{\gamma_A}4^{\delta_A}$ and $2^{\gamma_B}4^{\delta_B}$, and minimum Lee distances d_A and d_B, respectively. A new quaternary linear code $PC(\mathcal{A},\mathcal{B})$ is defined as

$$PC(\mathcal{A},\mathcal{B}) = \{(u|u+v) : u \in \mathcal{A}, v \in \mathcal{B}\}.$$

It is easy to see that if $\mathcal{G}_A$ and $\mathcal{G}_B$ are generator matrices of $\mathcal{A}$ and $\mathcal{B}$, respectively, then the matrix

$$\mathcal{G}_{PC} = \begin{pmatrix} \mathcal{G}_A & \mathcal{G}_A \\ 0 & \mathcal{G}_B \end{pmatrix}$$

is a generator matrix of the code $PC(\mathcal{A},\mathcal{B})$. Moreover, the code $PC(\mathcal{A},\mathcal{B})$ is of length $2n$, type $2^{\gamma_A+\gamma_B}4^{\delta_A+\delta_B}$, and minimum Lee distance $d = \min\{2d_A, d_B\}$ [7], [8].

Definition 4 (BQ-Plotkin Construction): Let $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ be three quaternary linear codes of length n; types $2^{\gamma_A}4^{\delta_A}$, $2^{\gamma_B}4^{\delta_B}$, and $2^{\gamma_C}4^{\delta_C}$; and minimum Lee distances d_A, d_B, and d_C, respectively. Let $\mathcal{G}_A$, $\mathcal{G}_B$, and $\mathcal{G}_C$ be generator matrices of the codes $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$, respectively. A new code $BQ(\mathcal{A},\mathcal{B},\mathcal{C})$ is defined as the quaternary linear code generated by

$$\mathcal{G}_{BQ} = \begin{pmatrix} \mathcal{G}_A & \mathcal{G}_A & \mathcal{G}_A & \mathcal{G}_A \\ 0 & \mathcal{G}'_B & 2\mathcal{G}'_B & 3\mathcal{G}'_B \\ 0 & 0 & \hat{\mathcal{G}}_B & \hat{\mathcal{G}}_B \\ 0 & 0 & 0 & \mathcal{G}_C \end{pmatrix}$$

where $\mathcal{G}'_B$ is the matrix obtained from $\mathcal{G}_B$ after switching twos by ones in their γ_B rows of order two, and $\hat{\mathcal{G}}_B$ is the matrix obtained from $\mathcal{G}_B$ after removing their γ_B rows of order two.

The code $BQ(\mathcal{A},\mathcal{B},\mathcal{C})$ is of type $2^{\gamma_A+\gamma_C}4^{\delta_A+\gamma_B+2\delta_B+\delta_C}$, length $4n$, and minimum Lee distance $d = \min\{4d_A, 2d_B, d_C\}$ [7], [8].

Now, the quaternary linear Reed–Muller codes $\mathcal{RM}_s(r,m)$ of length 2^{m-1}, for $m \ge 1$, $0 \le r \le m$, and $0 \le s \le \lfloor \frac{m-1}{2} \rfloor$, will be defined. For the recursive construction, it will be convenient to define them also for $r < 0$ and $r > m$. The code $\mathcal{RM}_s(r,m)$ with $r < 0$ is defined as the zero code. The code $\mathcal{RM}_s(0,m)$ is defined as the repetition code with only the all-zero and all-two vectors. The code $\mathcal{RM}_s(r,m)$ with $r \ge m$ is defined as the universe code, that is, the whole space $\mathbb{Z}_4^{2^{m-1}}$. For $m = 1$, there is only one family with $s = 0$, and in this family there are only the zero, repetition and universe codes for $r < 0$, $r = 0$ and $r \ge 1$, respectively. In this case, the generator matrix of $\mathcal{RM}_0(0,1)$ is $\mathcal{G}_{0(0,1)} = (2)$, and the generator matrix of $\mathcal{RM}_0(r,1)$ is $\mathcal{G}_{0(r,1)} = (1)$, where $r \ge 1$.

For any $m \ge 2$, given $\mathcal{RM}_s(r,m-1)$ and $\mathcal{RM}_s(r-1,m-1)$ codes, where $0 \le s \le \lfloor \frac{m-2}{2} \rfloor$, the $\mathcal{RM}_s(r,m)$ code can be constructed in a recursive way using the Plotkin construction given by Definition 3, as follows:

$$\mathcal{RM}_s(r,m) = PC(\mathcal{RM}_s(r,m-1), \mathcal{RM}_s(r-1,m-1)).$$

For example, for $m = 2$, the generator matrices of $\mathcal{RM}_0(r,2)$, $0 \le r \le 2$, are the following: $\mathcal{G}_{0(0,2)} = (2 \quad 2)$;

$$\mathcal{G}_{0(1,2)} = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}; \quad \mathcal{G}_{0(2,2)} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Note that when m is odd, the $\mathcal{RM}_s$ family with $s = \frac{m-1}{2}$ can not be generated using the Plotkin construction. In this case, for any $m \ge 3$, m odd and $s = \frac{m-1}{2}$, given $\mathcal{RM}_{s-1}(r,m-2)$, $\mathcal{RM}_{s-1}(r-1,m-2)$ and $\mathcal{RM}_{s-1}(r-2,m-2)$, the $\mathcal{RM}_s(r,m)$ code can be constructed using the BQ-Plotkin construction given by Definition 4 as follows:

$$\mathcal{RM}_s(r,m) = BQ(\mathcal{RM}_{s-1}(r,m-2),\\ \mathcal{RM}_{s-1}(r-1,m-2),\\ \mathcal{RM}_{s-1}(r-2,m-2)).$$

For example, for $m = 3$, there are two families. The $\mathcal{RM}_0$ family can be generated using the Plotkin construction. On the other hand, the $\mathcal{RM}_1$ family has to be generated using

TABLE I
TYPE $2^{\gamma}4^{\delta}$ AND DIMENSION OF THE KERNEL $k_{s(r,m)}$ FOR ALL $\mathcal{RM}_s(r,m)$ CODES WITH $m \leq 7$, SHOWING THEM IN THE FORM $(\gamma,\delta)k_{s(r,m)}$

m	s \ r	0	1	2	3	4	5	6	7
1	0	(1,0) 1	(0,1) 2						
2	0	(1,0) 1	(1,1) 3	(0,2) 4					
3	0	(1,0) 1	(2,1) 4	(1,3) 7	(0,4) 8				
	1	(1,0) 1	(0,2) 4	(1,3) 7	(0,4) 8				
4	0	(1,0) 1	(3,1) 5	(3,4) 11	(1,7) 15	(0,8) 16			
	1	(1,0) 1	(1,2) 5	(1,5) 8	(1,7) 15	(0,8) 16			
5	0	(1,0) 1	(4,1) 6	(6,5) 16	(4,11) 20	(1,15) 31	(0,16) 32		
	1	(1,0) 1	(2,2) 6	(2,7) 11	(2,12) 16	(1,15) 31	(0,16) 32		
	2	(1,0) 1	(0,3) 4	(2,7) 11	(0,12) 14	(1,15) 31	(0,16) 32		
6	0	(1,0) 1	(5,1) 7	(10,6) 22	(10,16) 32	(5,26) 37	(1,31) 63	(0,32) 64	
	1	(1,0) 1	(3,2) 7	(4,9) 15	(4,19) 25	(3,27) 32	(1,31) 63	(0,32) 64	
	2	(1,0) 1	(1,3) 5	(2,10) 13	(2,20) 23	(1,28) 30	(1,31) 63	(0,32) 64	
7	0	(1,0) 1	(6,1) 8	(15,7) 29	(20,22) 49	(15,42) 64	(6,57) 70	(1,63) 127	(0,64) 128
	1	(1,0) 1	(4,2) 8	(7,11) 20	(8,28) 38	(7,46) 55	(4,58) 64	(1,63) 127	(0,64) 128
	2	(1,0) 1	(2,3) 6	(3,13) 17	(4,30) 35	(3,48) 52	(2,59) 62	(1,63) 127	(0,64) 128
	3	(1,0) 1	(0,4) 5	(3,13) 17	(0,32) 33	(3,48) 52	(0,60) 61	(1,63) 127	(0,64) 128

the BQ-Plotkin construction. The generator matrices of $\mathcal{RM}_1(r,3)$, $0 \leq r \leq 3$, are the following:

$$\mathcal{G}_{1(0,3)} = (2\ \ 2\ \ 2\ \ 2);$$

$$\mathcal{G}_{1(1,3)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \end{pmatrix};$$

$$\mathcal{G}_{1(2,3)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix};$$

$$\mathcal{G}_{1(3,3)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The generator matrices $\mathcal{G}_{s(r,m)}$ will be exactly the matrices obtained following this construction process unless otherwise stated. The following proposition summarizes the parameters and properties of these $\mathcal{RM}_s$ families of codes.

Proposition 5 ([7], [8]): A quaternary linear Reed–Muller code $\mathcal{RM}_s(r,m)$, with $m \geq 1$, $0 \leq r \leq m$, and $0 \leq s \leq \lfloor\frac{m-1}{2}\rfloor$, has the following parameters and properties:

1) the length is $n = 2^{m-1}$;
2) the minimum Lee distance is $d = 2^{m-r}$;
3) the number of codewords is $2^{\sum_{i=0}^{r}\binom{m}{i}}$;
4) the code $\mathcal{RM}_s(r-1,m)$ is a subcode of $\mathcal{RM}_s(r,m)$ for $0 < r \leq m$;
5) the codes $\mathcal{RM}_s(1,m)$ and $\mathcal{RM}_s(m-2,m)$, after the Gray map, are $\mathbb{Z}_4$-linear Hadamard and $\mathbb{Z}_4$-linear extended 1-perfect codes, respectively;
6) the code $\mathcal{RM}_s(r,m)$ is the dual code of $\mathcal{RM}_s(m-1-r,m)$ for $-1 \leq r \leq m$.

III. KERNEL FOR THE $\mathcal{RM}_0(r,m)$ CODES

The purpose of this section is to establish the dimension of the kernel for all codes in the $\mathcal{RM}_0$ family. Moreover, we will give a generator matrix of the kernel, from a generator matrix of the code.

First of all, we will give an expression for the parameters γ and δ of a quaternary linear Reed–Muller code $\mathcal{RM}_s(r,m)$ of type $2^{\gamma}4^{\delta}$, depending on s, r and m. Table I shows the type $2^{\gamma}4^{\delta}$ of all these codes for $m \leq 7$. In order to distinguish the γ and δ of the different $\mathcal{RM}_s(r,m)$ codes, we will denote them by $\gamma_{s(r,m)}$ and $\delta_{s(r,m)}$, respectively. Moreover, the kernel of any quaternary linear Reed–Muller code $K(\mathcal{RM}_s(r,m))$ will be denoted by $K_{s(r,m)}$. For the following expressions, we will consider that $\binom{a}{b} = 0$, when $a < b$.

Lemma 6: Let $\mathcal{C}$ be a quaternary linear Reed–Muller code $\mathcal{RM}_s(r,m)$ of type $2^{\gamma}4^{\delta}$. Then, for $m \geq 1$, $0 \leq r \leq m$, and $0 \leq s \leq \lfloor\frac{m-1}{2}\rfloor$,

$$\gamma = \sum_{i=0}^{\lfloor\frac{r}{2}\rfloor}\binom{m-2s-1}{r-2i}\binom{s}{i} \quad \textit{and} \quad \delta = \frac{1}{2}\sum_{i=0}^{r}\binom{m}{i} - \frac{\gamma}{2}.$$

Proof: The code $\mathcal{C}$ can be constructed using the Plotkin and BQ-Plotkin constructions. By the results about the type of these constructions given in Section II-B, and using induction on m, for all r and s, we obtain $\gamma = \sum_{i=0}^{\lfloor\frac{r}{2}\rfloor}\binom{m-2s-1}{r-2i}\binom{s}{i}$. Since $\gamma + 2\delta = \sum_{i=0}^{r}\binom{m}{i}$ by Proposition 5, we obtain the expression for δ. □

Proposition 7: For all $m \geq 1$ and $r \in \{0,\ldots,m\}$, the dimension of the kernel of $\mathcal{RM}_0(r,m)$ of type $2^{\gamma}4^{\delta}$ is

$$k_{0(r,m)} = \begin{cases} \gamma + 2\delta & \text{if } r \in \{0,1,2,m-1,m\} \\ \gamma + \delta + m & \text{if } r \in \{3,\ldots,m-2\}. \end{cases}$$

Proof: In [21], it was proved that $\mathcal{RM}_0(r,m) = \mathcal{ZRM}^-(r,m-1)$. The $\mathcal{ZRM}^-(r,m-1)$ codes, defined for all $m \geq 1$ and $r \in \{0,\ldots,m\}$, were introduced in [18]. Since $\Phi(\mathcal{ZRM}^-(r,m-1))$ is a binary linear code for $r \in \{0,1,2,m-1,m\}$ [18], in these cases, the dimension of the kernel is $k_{0(r,m)} = \gamma + 2\delta$. On the other hand, for $r \in \{3,\ldots,m-2\}$, we know that the dimension of $K_{0(r,m)}$ is equal to the dimension of $K(\mathcal{ZRM}^-(r,m-1))$, which is $\sum_{i=0}^{r}\binom{m-1}{i} + m$ [18], [21]. By Lemma 6, and due to the fact that $s = 0$, we have $\gamma = \binom{m-1}{r}$ and $\delta = \frac{1}{2}\left[\sum_{i=0}^{r}\binom{m}{i} - \gamma\right]$. It is easy to check that

$\gamma + \delta = \frac{1}{2}\left[\sum_{i=0}^{r}\binom{m}{i} + \binom{m-1}{r}\right] = \sum_{i=0}^{r}\binom{m-1}{i}$. Therefore, the equality $k_{0,(r,m)} = \gamma + \delta + m$ holds. □

Lemma 8: Let $\mathcal{A}$ and $\mathcal{B}$ be two quaternary linear codes of length n with generator matrices $\mathcal{G}_A$ and $\mathcal{G}_B$, respectively, such that $\mathcal{B} \subset \mathcal{A}$. Let $\mathcal{C} = PC(\mathcal{A}, \mathcal{B})$ of length $2n$. If $u \in \mathcal{A}$ and $v \in \mathcal{B}$, then $(u|u+v) \in K(\mathcal{C})$ if and only if $u \in K(\mathcal{A})$, $2v * w \in \mathcal{B}$, and $2u * z \in \mathcal{B}$ for all $w \in \mathcal{G}_A$ and $z \in \mathcal{G}_B$.

Proof: The codeword $(u|u+v) \in K(\mathcal{C})$ if and only if $2(u|u+v) * (w|w) \in \mathcal{C}$ and $2(u|u+v) * (0|z) \in \mathcal{C}$ for all w, z in $\mathcal{G}_A$, $\mathcal{G}_B$, respectively. That means $(2u * w|2u * w + 2v * w) \in \mathcal{C}$ for all $w \in \mathcal{G}_A$, and $(0|2u * z + 2v * z) \in \mathcal{C}$ for all $z \in \mathcal{G}_B$. That is, $u \in K(\mathcal{A})$ and $2v * w \in \mathcal{B}$ for all $w \in \mathcal{G}_A$, and $2u * z + 2v * z \in \mathcal{B}$ for all $z \in \mathcal{G}_B$. Note that since $\mathcal{B} \subset \mathcal{A}$, the condition $2v * w \in \mathcal{B}$ for all $w \in \mathcal{G}_A$ implies that $2v * z \in \mathcal{B}$ for all $z \in \mathcal{G}_B$. Therefore, $2u * z + 2v * z \in \mathcal{B}$ for all $z \in \mathcal{G}_B$ is simplified to $2u * z \in \mathcal{B}$ for all $z \in \mathcal{G}_B$. □

Corollary 9: Let $\mathcal{A}$ and $\mathcal{B}$ be two quaternary linear codes of length n, such that $\mathcal{B} \subset \mathcal{A}$. Let $\mathcal{C} = PC(\mathcal{A}, \mathcal{B})$ of length $2n$. If $(u|u+v) \in K(\mathcal{C})$, where $u \in \mathcal{A}$ and $v \in \mathcal{B}$, then $u \in K(\mathcal{A})$ and $v \in K(\mathcal{B})$. That is, $K(PC(\mathcal{A}, \mathcal{B})) \subset PC(K(\mathcal{A}), K(\mathcal{B}))$.

Proof: Straightforward from Lemma 8. □

Let $\mathcal{C}$ be a quaternary linear code. The code $2\mathcal{C}$ is obtained from $\mathcal{C}$ by multiplying by two all codewords of $\mathcal{C}$. Note that if $\mathcal{G}$ is a generator matrix of $\mathcal{C}$, then $2\mathcal{G}$ is a generator matrix of $2\mathcal{C}$.

Lemma 10: For all $m \geq 1$ and $r \in \{0, \ldots, m-1\}$, $2\mathcal{RM}_0(r+1, m) \subset \mathcal{RM}_0(r, m)$.

Proof: Let $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ be three quaternary linear codes such that $2\mathcal{A} \subset \mathcal{B}$ and $2\mathcal{B} \subset \mathcal{C}$. It is easy to see that $2PC(\mathcal{A}, \mathcal{B}) \subset PC(\mathcal{B}, \mathcal{C})$. Since the codes $\mathcal{RM}_0(r, 1)$ satisfy this relationship for all $r \in \mathbb{Z}$, and the codes $\mathcal{RM}_0(r, m)$ for $m > 1$ and $r \in \mathbb{Z}$ can be obtained using the Plotkin construction, the result follows. □

Since $K(\mathcal{C})$ is a linear subcode of $\mathcal{C}$, now we will give a generator matrix of $K_{0,(r,m)}$ for all $m \geq 5$ and $r \in \{3, \ldots, m-2\}$ from $\mathcal{G}_{0,(r,m)}$. Note that for all $m \geq 1$ and $r \in \{0, 1, 2, m-1, m\}$, $\Phi(\mathcal{RM}_0(r, m))$ is a binary linear code, so $K_{0,(r,m)} = \mathcal{RM}_0(r, m)$ and it is generated by $\mathcal{G}_{0,(r,m)}$.

Let define the set of vectors $V_1 = \{1\}$ and $V_m = \{(v|v) : v \in V_{m-1}\} \cup \{(0|1)\}$ for $m \geq 2$. Clearly, the length of the vectors in V_m is 2^{m-1}, and $|V_m| = m$ follows from $|V_m| = |V_{m-1}| + 1$. Moreover, by construction $V_m \subset \mathcal{G}_{0,(r,m)}$ for all $r \geq 2$.

Proposition 11: For all $m \geq 5$ and $r \in \{3, \ldots, m-2\}$, the kernel of $\mathcal{RM}_0(r, m)$ of type $2^\gamma 4^\delta$ is a linear subcode of type $2^{\gamma+\delta-m} 4^m$ generated by

$$\mathcal{M}_{0,(r,m)} = \begin{pmatrix} \mathcal{G}_S \\ 2\mathcal{G}_Q \\ V_m \end{pmatrix}.$$

Proof: By Lemma 1, $\mathcal{G}_S \cup 2\mathcal{G}_Q \subset K_{0,(r,m)}$. In the next paragraph, we will show that $V_m \subset K_{0,(r,m)}$. Applying the Gray map to all row vectors of $\mathcal{M}_{0,(r,m)}$, we obtain $\gamma + \delta + m$ linear independent binary vectors. Therefore, by Proposition 7, once we prove that $V_m \subset K_{0,(r,m)}$, we will have that $K_{0,(r,m)}$ is generated by $\mathcal{M}_{0,(r,m)}$.

We said before that $V_m \subset \mathcal{G}_{0,(r,m)} \subset \mathcal{RM}_0(r, m)$ for all $r \geq 2$. By Proposition 7, for all $m \geq 2$, $\mathcal{RM}_0(2, m)$ is a binary linear code after the Gray map, so $V_m \subset \mathcal{RM}_0(2, m) = K_{0,(2,m)}$. For the same reason, we also have that $V_4 \subset \mathcal{RM}_0(r, 4) = K_{0,(r,4)}$ for all $r \geq 2$. Assume the result is true for $m \geq 4$ and $r \geq 2$. By Lemma 8, it follows that $v \in K_{0,(r-1,m)}$ and $v \in K_{0,(r,m)}$ implies that $(v|v) \in K_{0,(r,m+1)}$. Thus, $V_{m+1} \setminus \{(0|1)\} \subset K_{0,(r,m+1)}$ for all $r \geq 3$. Again by Lemma 8, it follows that $(0|1) \in K_{0,(r,m+1)}$ if and only if $2\mathcal{RM}_0(r, m) \subset \mathcal{RM}_0(r-1, m)$, which it holds by Lemma 10. Therefore, $V_{m+1} \subset K_{0,(r,m+1)}$ for all $r \geq 2$, as we wanted to show. □

IV. Kernel for the $\mathcal{RM}_s(r, m)$ Codes, $s > 0$

In this section, we will establish the dimension of the kernel for all the $\mathcal{RM}_s(r, m)$ codes with $s > 0$. At the same time, we will give a generator matrix of the kernel, from a generator matrix of the code. In order to do that, first we will prove some results concerning the constructions and properties of these codes.

Lemma 12: For all $m \geq 3$, $1 \leq s \leq \left\lfloor \frac{m-1}{2} \right\rfloor$ and $r \in \{0, \ldots, m-2\}$, $2\mathcal{RM}_s(r+1, m) \not\subseteq \mathcal{RM}_s(r, m)$.

Proof: Assume that $2\mathcal{RM}_s(r+1, m) \subseteq \mathcal{RM}_s(r, m)$. Hence, $\mathcal{X} = 2\mathcal{RM}_s(r+1, m)$ is a subcode of the subcode $\mathcal{Y}$ of $\mathcal{RM}_s(r, m)$ that contains all codewords of order two. After the Gray map, $\mathcal{X}$ and $\mathcal{Y}$ are binary linear codes of dimension $\delta_{s,(r+1,m)}$ and $\gamma_{s,(r,m)} + \delta_{s,(r,m)}$, respectively. Because of the former is a subcode of the latter follows $\delta_{s,(r+1,m)} \leq \gamma_{s,(r,m)} + \delta_{s,(r,m)}$. Now, we are going to prove that $\delta_{s,(r+1,m)} > \gamma_{s,(r,m)} + \delta_{s,(r,m)}$, so the initial assumption is false.

It is easy to check the trivial cases where $\delta_{s,(r+1,m)} = \gamma_{s,(r,m)} + \delta_{s,(r,m)} = 0$ for all $r < 0$, and $\delta_{s,(r+1,m)} = \gamma_{s,(r,m)} + \delta_{s,(r,m)} = 2^m$ for all $r > m-2$. Now, we proceed by induction to prove the result for all $s \geq 1$ and $m = 2s+1 \geq 3$. For $s = 1$, $m = 2s+1 = 3$ and $r \in \{0, 1\}$, it is clear that $\delta_{s,(r+1,m)} > \gamma_{s,(r,m)} + \delta_{s,(r,m)}$ (see Table I). For any $s \geq 1$ and $m = 2s+1$, assume that $\delta_{s,(r+1,m)} > \gamma_{s,(r,m)} + \delta_{s,(r,m)}$ for all $r \in \{0, \ldots, m-2\}$, and $\delta_{s,(r+1,m)} = \gamma_{s,(r,m)} + \delta_{s,(r,m)}$ for all $r \notin \{0, \ldots, m-2\}$. By the result on the parameters γ and δ for the $\mathcal{RM}_{s+1}(r, m+2)$ codes obtained using the BQ-Plotkin construction, we have that

$$\begin{aligned}
&\gamma_{s+1,(r,m+2)} + \delta_{s+1,(r,m+2)} \\
&\quad = \gamma_{s,(r-2,m)} + \gamma_{s,(r,m)} + \delta_{s,(r,m)} \\
&\qquad + \gamma_{s,(r-1,m)} + 2\delta_{s,(r-1,m)} + \delta_{s,(r-2,m)} \\
&\quad \leq \delta_{s,(r-1,m)} + \delta_{s,(r+2,m)} + \delta_{s,(r,m)} + \delta_{s,(r-1,m)}.
\end{aligned}$$

Moreover, since $\gamma_{s,(r-1,m)} + \delta_{s,(r-1,m)} \leq \delta_{s,(r,m)}$, we have that $\delta_{s,(r-1,m)} \leq \delta_{s,(r,m)} \leq \gamma_{s,(r,m)} + \delta_{s,(r,m)}$, and

$$\begin{aligned}
&\delta_{s,(r-1,m)} + \delta_{s,(r+1,m)} + \delta_{s,(r,m)} + \delta_{s,(r-1,m)} \\
&\quad \leq \delta_{s,(r-1,m)} + \delta_{s,(r+1,m)} + 2\delta_{s,(r,m)} + \gamma_{s,(r,m)} \\
&\quad = \delta_{s+1,(r+1,m+2)}.
\end{aligned}$$

In fact, by the induction hypothesis, we have $\delta_{s+1,(r+1,m+2)} > \gamma_{s+1,(r,m+2)} + \delta_{s+1,(r,m+2)}$, $\forall r \in \{0, \ldots, m\}$. Finally, we finish the induction for any $s \geq 1$ and $m \geq 2s+1$. Now, by the result on the parameters γ and δ for the codes obtained using the Plotkin construction we have that

$$\begin{aligned}\gamma_{s,r,m+1}&+\delta_{s,r,m+1}\\ &=\gamma_{s,r,m}+\gamma_{s,r-1,m}+\delta_{s,r,m}+\delta_{s,r-1,m}\\ &\leq\delta_{s,r,m}+\delta_{s,r+1,m}=\delta_{s,r+1,m+1}.\end{aligned}$$

Again, by the induction hypothesis, it follows that $\delta_{s,r+1,m+1}\geq\gamma_{s,r,m+1}+\delta_{s,r,m+1}$, $\forall r\in\{0,\ldots,m-1\}$. □

Lemma 13 ([7], [8]): Let $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ be the quaternary linear Reed–Muller codes $\mathcal{RM}_s(r+1,m)$, $\mathcal{RM}_s(r,m)$ and $\mathcal{RM}_s(r-1,m)$, with generator matrices $\mathcal{G}_\mathcal{A}$, $\mathcal{G}_\mathcal{B}$ and $\mathcal{G}_\mathcal{C}$, respectively. Then, $\mathcal{C}\subset\mathcal{B}\subset\mathcal{A}$ and $\hat{\mathcal{B}}\subset\mathcal{B}\subset\mathcal{B}'\subset\mathcal{A}$, where $\hat{\mathcal{B}}$ and $\mathcal{B}'$ are the codes generated by $\mathcal{G}_{\hat{\mathcal{B}}}$ and $\mathcal{G}_{\mathcal{B}'}$, respectively.

Lemma 14: Let $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ be the quaternary linear Reed–Muller codes $\mathcal{RM}_s(r+1,m)$, $\mathcal{RM}_s(r,m)$ and $\mathcal{RM}_s(r-1,m)$, with generator matrices $\mathcal{G}_\mathcal{A}$, $\mathcal{G}_\mathcal{B}$ and $\mathcal{G}_\mathcal{C}$, respectively. Let $\mathcal{D}=BQ(\mathcal{A},\mathcal{B},\mathcal{C})$. If $x\in\mathcal{A}$, $y'\in\mathcal{B}'$, $\hat{y}\in\hat{\mathcal{B}}$ and $z\in\mathcal{C}$, then $(x|x+y'|x+2y'+\hat{y}|x+3y'+\hat{y}+z)\in K(\mathcal{D})$ if and only if $2x*v\in\mathcal{A}$, $2y'*v\in\mathcal{B}'$, $2\hat{y}*v\in\hat{\mathcal{B}}$, $2z*v\in\mathcal{C}$, $2x*v'\in\mathcal{B}'$, $2\hat{y}*v'\in\mathcal{C}$, $2x*\hat{v}\in\hat{\mathcal{B}}$, $2y'*\hat{v}\in\mathcal{C}$, and $2x*\bar{v}+2y'*\bar{v}\in\mathcal{C}$ for all $v\in\mathcal{G}_\mathcal{A}$, $v'\in\mathcal{G}_{\mathcal{B}'}$, $\hat{v}\in\mathcal{G}_{\hat{\mathcal{B}}}$ and $\bar{v}\in\mathcal{G}_\mathcal{C}$.

Proof: The codeword $t=(x|x+y'|x+2y'+\hat{y}|x+3y'+\hat{y}+z)\in K(\mathcal{D})$ if and only if $2t*(v|v|v|v)\in\mathcal{D}$, $2t*(0|v'|2v'|3v')\in\mathcal{D}$, $2t*(0|0|\hat{v}|\hat{v})\in\mathcal{D}$ and $2t*(0|0|0|\bar{v})\in\mathcal{D}$ for all $v\in\mathcal{G}_\mathcal{A}$, $v'\in\mathcal{G}_{\mathcal{B}'}$, $\hat{v}\in\mathcal{G}_{\hat{\mathcal{B}}}$ and $\bar{v}\in\mathcal{G}_\mathcal{C}$. That is, $2x*v\in\mathcal{A}$, $2y'*v\in\mathcal{B}'$, $2\hat{y}*v\in\hat{\mathcal{B}}$, $2z*v\in\mathcal{C}$, $2x*v'+2y'*v'\in\mathcal{B}'$, $2\hat{y}*v'+2z*v'\in\mathcal{C}$, $2x*\hat{v}+2\hat{y}*\hat{v}\in\hat{\mathcal{B}}$, $2y'*\hat{v}+2z*\hat{v}\in\mathcal{C}$, and $2x*\bar{v}+2y'*\bar{v}+2\hat{y}*\bar{v}+2z*\bar{v}\in\mathcal{C}$ for all $v\in\mathcal{G}_\mathcal{A}$, $v'\in\mathcal{G}_{\mathcal{B}'}$, $\hat{v}\in\mathcal{G}_{\hat{\mathcal{B}}}$ and $\bar{v}\in\mathcal{G}_\mathcal{C}$. Finally, we can simplify these conditions using Lemma 13. □

Corollary 15: Let $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ be the quaternary linear Reed–Muller codes $\mathcal{RM}_s(r+1,m)$, $\mathcal{RM}_s(r,m)$ and $\mathcal{RM}_s(r-1,m)$, respectively. Let $\mathcal{D}=BQ(\mathcal{A},\mathcal{B},\mathcal{C})$. If $(x|x+y'|x+2y'+\hat{y}|x+3y'+\hat{y}+z)\in K(\mathcal{D})$, where $x\in\mathcal{A}$, $y'\in\mathcal{B}'$, $\hat{y}\in\hat{\mathcal{B}}$ and $z\in\mathcal{C}$, then $x\in K(\mathcal{A})$, $y'\in K(\mathcal{B}')\subset K(\mathcal{A})$, $\hat{y}\in K(\hat{\mathcal{B}})\subset K(\mathcal{B})$ and $z\in K(\mathcal{C})$.

Proof: If $(x|x+y'|x+2y'+\hat{y}|x+3y'+\hat{y}+z)\in K(\mathcal{D})$, then $2(x|x+y'|x+2y'+\hat{y}|x+3y'+\hat{y}+z)*(v|v|v|v)\in\mathcal{D}$ for all $v\in\mathcal{G}_\mathcal{A}$. That is, $2x*v\in\mathcal{A}$, $2y'*v\in\mathcal{B}'$, $2\hat{y}*v\in\hat{\mathcal{B}}$ and $2z*v\in\mathcal{C}$. By Lemma 13, we know that $\mathcal{G}_\mathcal{C}$, $\mathcal{G}_{\mathcal{B}'}$, and $\mathcal{G}_{\hat{\mathcal{B}}}$ are submatrices of $\mathcal{G}_\mathcal{A}$. Thus, we can say that $x\in K(\mathcal{A})$, $y'\in K(\mathcal{B}')$, $\hat{y}\in K(\hat{\mathcal{B}})$, and $z\in K(\mathcal{C})$. Since $\hat{\mathcal{B}}$ is the code generated by $\mathcal{G}_{\hat{\mathcal{B}}}$ and $\mathcal{G}_{\hat{\mathcal{B}}}$ is the matrix $\mathcal{G}_\mathcal{B}$ after removing the rows of order two, we can say that $K(\hat{\mathcal{B}})\subset K(\mathcal{B})$. Moreover, $2y'*v\in\mathcal{B}'\subset\mathcal{A}$ for all $v\in\mathcal{G}_\mathcal{A}$, so $y'\in K(\mathcal{A})$. □

Proposition 16: For all $m\geq 3$, $1\leq s\leq\lfloor\frac{m-1}{2}\rfloor$ and $r\in\{0,m-1,m\}$, the corresponding $\mathbb{Z}_2$-linear codes of $\mathcal{RM}_s(r,m)$ and $\mathcal{RM}_1(1,m)$ are binary linear codes.

Proof: For $r=0$, $r=m-1$ and $r=m$, the corresponding $\mathbb{Z}_2$-linear codes of $\mathcal{RM}_s(r,m)$ are the repetition, the even weight and the universe codes, respectively, which are binary linear codes. For $r=1$, the corresponding $\mathbb{Z}_2$-linear code of $\mathcal{RM}_1(1,m)$ is the binary linear Hadamard code [7], [8]. □

Note that for all $m\geq 3$ and $r\in\{0,1,m-1,m\}$, $\Phi(\mathcal{RM}_1(r,m))$ is a binary linear code, so $K_{1,r,m}=\mathcal{RM}_1(r,m)$ and it is generated by $\mathcal{G}_{1,r,m}$. Now, we will show that $K_{1,r,m}$, for all $m\geq 4$ and $r\in\{2,\ldots,m-2\}$, is generated by

$$\mathcal{M}_{1,r,m}=\begin{pmatrix}\mathcal{G}_T\\ 2\mathcal{G}_Q\\ \mathbf{1}\\ v\end{pmatrix}$$

where $v=(0,1,0,1,\ldots,0,1)$.

Proposition 17: For all $m\geq 4$ and $r\in\{2,\ldots,m-2\}$, the kernel of $\mathcal{RM}_1(r,m)$ of type $2^\gamma 4^\delta$ is a linear subcode of type $2^{\gamma+\delta-2}4^2$ generated by $\mathcal{M}_{1,r,m}$, and $\kappa_{1,r,m}=\gamma+\delta+2$.

Proof: By (1), we know that $\kappa_{1,1,m}=\kappa_{1,m-2,m}=\gamma+\delta+2$. Note that $\kappa_{1,1,m}=\gamma+2\delta$, since $\delta=2$. For these two cases, it is easy to check that the kernel is generated by $\mathcal{M}_{1,r,m}$. Hence, the result is true for $m=4$, and we just need to prove it for every $m\geq 5$ and $r\in\{2,\ldots,m-3\}$. We proceed by induction on $m\geq 5$. The known cases $r\in\{1,m-2\}$ will be used to complete each induction step.

Let $\mathcal{S}_{1,r,m}$ be the code generated by $\mathcal{M}_{1,r,m}$. Assume that $\mathcal{S}_{1,r,m-1}=K_{1,r,m-1}$ for all $r\in\{1,\ldots,m-3\}$. By Lemma 8, since $v\in\mathcal{S}_{1,r,m-1}=K_{1,r,m-1}$, then $(v|v)\in K_{1,r,m}$ for all $r\in\{2,\ldots,m-3\}$. Moreover, it is clear that $\mathbf{1}\in K_{1,r,m}$. Therefore, $\mathcal{S}_{1,r,m}\subset K_{1,r,m}$ for all $r\in\{2,\ldots,m-3\}$.

By Corollary 9, we have that $\mathcal{S}_{1,r,m}\subset K_{1,r,m}\subset PC(\mathcal{S}_{1,r,m-1},\mathcal{S}_{1,r-1,m-1})\subset\mathcal{RM}_1(r,m)$. Since $\mathbf{1}$ and v are the unique vectors of order four in $\mathcal{M}_{1,r,m-1}$ for all $r\in\{1,\ldots,m-3\}$, we have that $\mathbf{1}$, v, $(\mathbf{0}|\mathbf{1})$, $(\mathbf{0}|v)$ are the only vectors of order four in the generator matrix of $PC(\mathcal{S}_{1,r,m-1},\mathcal{S}_{1,r-1,m-1})$ for all $r\in\{2,\ldots,m-3\}$. Moreover, since $\mathcal{S}_{1,r,m}$ is a subcode of $K_{1,r,m}$, $K_{1,r,m}$ and $\mathcal{RM}_1(r,m)$ can be written as a union of cosets of $\mathcal{S}_{1,r,m}$ [16], [17]. Actually, looking at their types, the code $PC(\mathcal{S}_{1,r,m-1},\mathcal{S}_{1,r-1,m-1})$ is the union of four cosets of $\mathcal{S}_{1,r,m}$ with leaders given by the vectors $\mathbf{0}$, $(\mathbf{0}|\mathbf{1})$, $(\mathbf{0}|v)$, $(\mathbf{0}|\mathbf{1}+v)$. Now, we are going to see that the three nonzero leaders are not in $K_{1,r,m}$, which will give us that $\mathcal{S}_{1,r,m}=K_{1,r,m}$.

By Lemma 8, $(\mathbf{0}|\mathbf{1})\in K_{1,r,m}$ if and only if $2\mathcal{RM}_1(r,m-1)\subset\mathcal{RM}_1(r-1,m-1)$, which is not true by Lemma 12. Hence, $(\mathbf{0}|\mathbf{1})\notin K_{1,r,m}$. For the other two leaders, we need the vector $x=(0,\ldots,0,\ldots,1)\in\mathcal{RM}_1(r,m-1)$ of minimum weight 2^{m-r-1}. By Lemma 1, $(\mathbf{0}|v)\in K_{1,r,m}$ if and only if $2(\mathbf{0}|v)*x\in\mathcal{RM}_1(r,m)$ for all $x\in\mathcal{RM}_1(r,m)$. By Plotkin construction, $(x|x)\in\mathcal{RM}_1(r,m)$. Therefore, since $2(\mathbf{0}|v)*(x|x)$ is of weight 2^{m-r-1} and $\mathcal{RM}_1(r,m)$ have minimum weight 2^{m-r}, $(\mathbf{0}|v)\notin K_{1,r,m}$. Likewise $(\mathbf{0}|\mathbf{1}+v)\notin K_{1,r,m}$. □

Finally, we will focus on the codes with $s\geq 2$. Note that for all $m\geq 3$, $s\geq 2$ and $r\in\{0,m-1,m\}$, $\Phi(\mathcal{RM}_s(r,m))$ is a binary linear code, so $K_{s,r,m}=\mathcal{RM}_s(r,m)$ and it is generated by $\mathcal{G}_{s,r,m}$. Now, we will show that $K_{s,r,m}$, for all $m\geq 5$, $s\geq 2$ and $r\in\{1,\ldots,m-2\}$, is generated by

$$\mathcal{M}_{s,r,m}=\begin{pmatrix}\mathcal{G}_T\\ 2\mathcal{G}_Q\\ \mathbf{1}\end{pmatrix}$$

except $K_{2,2,5}$, which is generated by $\mathcal{M}_{1,2,5}$.

Proposition 18: For all $m \geq 5$, $2 \leq s \leq \lfloor\frac{m-1}{2}\rfloor$ and $r \in \{1,\dots,m-2\}$, the kernel of $RM_s(r,m)$ of type $2^\gamma 4^\delta$ is a linear subcode of type $2^{\gamma+\delta-1}4$ generated by $M_{s}(r,m)$, and $k_{s}(r,m) = \gamma+\delta+1$. There is an exception, the kernel of $RM_2(2,5)$ is generated by $M_1(2,5)$ and $k_2(2,5) = \gamma+\delta+2 = 11$.

Proof: By (1), we know that $k_{s}(1,m) = k_{s}(m-2,m) = \gamma+\delta+1$ when $s \geq 2$. For these cases, it is easy to check that the kernel is generated by $M_{s}(1,m)$ and $M_{s}(m-2,m)$ with $s \geq 2$, respectively. By Propositions 20 and 17, $RM_2(2,5) = RM_1(2,5)$ and $k_2(2,5) = k_1(2,5) = \gamma+\delta+2$. Therefore, the result holds for $m = 5$, $s = 2$ and $r \in \{1,2,3\}$.

Now, we will proceed by induction on $m \geq 6$ and $2 \leq s < \frac{m-1}{2}$ (when the codes can be constructed using the Plotkin construction), and by induction on $m \geq 7$ odd and $s = \frac{m-1}{2}$, or equivalently on $s \geq 3$ and $m = 2s+1$ (when the codes are constructed using the BQ-Plotkin construction).

In the former, in order to begin the induction on m without any exception, we will compute the kernel for $m = 6$, $s = 2$ and $r \in \{2,3\}$. It is easy to check that in these cases the proposition is true (see Table I). Hence, we will proceed by induction on $m \geq 7$ for every $2 \leq s < \frac{m-1}{2}$ and $r \in \{1,\dots,m-2\}$. Since all these cases can be constructed using the Plotkin construction, using similar arguments as in the proof of Proposition 17, and the induction hypothesis, the result is true for all these codes.

In the latter, in order to begin the induction on s without any exception, we will compute the kernel for $s = 3$, $m = 7$ and $r = 3$. It is also easy to check that in this case the proposition is true (see Table I). Moreover, by Proposition 20, $RM_s(2,m) = RM_{s-1}(2,m)$ and $RM_s(m-3,m) = RM_{s-1}(m-3,m)$ for all $s \geq 2$ and $m = 2s+1$. Hence, the result is true for $s = 3$ and $m = 7$. In the next paragraph, we will proceed by induction on $s \geq 4$ for every $m = 2s+1$ and $r \in \{3,\dots,m-4\}$. The known cases for $r \in \{1,2,m-3,m-2\}$ will be used to complete each induction step.

Let $C_{s}(r,m)$ be the code generated by $M_{s}(r,m)$. Since G_γ, $2G_\delta \subset K_{s}(r,m)$ by Lemma 1, and $\mathbf{1} \in K_{s}(r,m)$, it is clear that $C_{s}(r,m) \subset K_{s}(r,m)$ for all $r \in \{3,\dots,m-4\}$. Moreover, since $C_{s}(r,m)$ is a subcode of $K_{s}(r,m)$, the code $RM_s(r,m)$ can be written as a union of cosets of $C_{s}(r,m)$ [16], [17]. Actually, looking at their types, $RM_s(r,m)$ is the union of $2^{\delta-1}$ cosets of $C_{s}(r,m)$. The set of leaders is $\left\{\sum_{i=1}^{\delta-1}\lambda_i v_i : \lambda_i \in \{0,1\}\right\}$, where $v_i \in G_\delta$ with $v_i \neq \mathbf{1}$. Now, we are going to see that the nonzero leaders are not in $K_{s}(r,m)$, which will give us that $C_{s}(r,m) = K_{s}(r,m)$.

Assume that $C_{s-1}(r,m-2) = K_{s-1}(r,m-2)$ for all $r \in \{1,\dots,m-4\}$. Thus, by Corollary 15 only the subset of leaders $\{\sum_{i=1}^{3}\lambda_i v_i : \lambda_i \in \{0,1\}\}$, where $v_1 = (0|1|2|3)$, $v_2 = (0|0|1|1)$ and $v_3 = (0|0|0|1)$, could be in $K_{s}(r,m)$ for all $r \in \{3,\dots,m-4\}$. Now, we will see that $v_1, v_2, v_3 \notin K_{s}(r,m)$. By Lemma 14, if $v_1 \in K_{s}(r,m)$ or $v_3 \in K_{s}(r,m)$, then $2w \in RM_{s-1}(r-2,m-2)$, $\forall w \in RM_{s-1}(r-1,m-2)$. This is a not true, since $2RM_{s-1}(r-1,m-2) = 2RM_{s-1}(r-1,m-2) \not\subseteq RM_{s-1}(r-2,m-2)$, by Lemma 12. Again by Lemma 14, if $v_2 \in K_{s}(r,m)$, then $2w \in RM_{s-1}(r-2,m-2)$, $\forall w \in RM'_{s-1}(r-1,m-2)$. This is not true, since $RM_{s-1}(r-1,m-2) \subset RM'_{s-1}(r-1,m-2)$ by Lemma 13, and $2RM_{s-1}(r-1,m-2) \not\subseteq RM_{s-1}(r-2,m-2)$ by Lemma 12. Using the same arguments, it is easy to see that the other nonzero leaders are not in $K_{s}(r,m)$. Hence $C_{s}(r,m) = K_{s}(r,m)$ for all $r \in \{3,\dots,m-4\}$. □

V. Classification of the RM_s Families

In this section, we will show that this invariant, the dimension of the kernel, will allow us to classify completely the codes in the RM_s families for all r and m.

As we have shown in Section II-B, the quaternary linear Reed–Muller codes $RM_s(r,m)$ can be obtained using the Plotkin construction, except when m is odd and $s = \frac{m-1}{2}$. In this case, they are obtained using the BQ-Plotkin construction. Note that some of these codes could be constructed using any of these two constructions.

Theorem 19: For all $m \geq 1$, $0 \leq s \leq \lfloor\frac{m-1}{2}\rfloor$ and $r \in \{0,\dots,m\}$, the dimension of the kernel of $RM_s(r,m)$ of type $2^\gamma 4^\delta$ is

1) $k_{s}(0,m) = 1$, $k_{s}(m-1,m) = 2^m - 1$, $k_{s}(m,m) = 2^m$.

2) If $s = 0$,

$$k_0(r,m) = \begin{cases} \gamma+2\delta & \text{for } r = 1\\ \gamma+\delta+m & \text{for } r \in \{2,\dots,m-2\}.\end{cases}$$

3) If $s = 1$, $k_1(r,m) = \gamma+\delta+2$, for $r \in \{1,2,\dots,m-2\}$.

4) If $s \geq 2$, $k_{s}(r,m) = \gamma+\delta+1$, for $r \in \{1,2,\dots,m-2\}$, except $k_2(2,5) = \gamma+\delta+2 = 11$.

Proof: It is straightforward to see that $k_{s}(0,m) = 1$, $k_{s}(m-1,m) = 2^m - 1$, and $k_{s}(m,m) = 2^m$, because $\Phi(RM_s(0,m))$, $\Phi(RM_s(m-1,m))$, and $\Phi(RM_s(m,m))$ are the repetition, the even weight, and the universe codes, respectively. The cases $s = 0$, $s = 1$ and $s \geq 2$ are proved in Propositions 7, 17, and 18, respectively. □

Note that Theorem 19 includes the previous results about the dimension of the kernel for $\mathbb{Z}_4$-linear Hadamard and $\mathbb{Z}_4$-linear extended 1-perfect codes [11]–[13] or (1). Table I shows the type $2^\gamma 4^\delta$ and the dimension of the kernel of all these $RM_s(r,m)$ codes for $m \leq 7$.

Proposition 20: For all $m \geq 3$, $1 \leq s \leq \lfloor\frac{m-1}{2}\rfloor$, and $r \in \{1\dots m-2\}$ we have $\gamma_{s-1}(r,m) + \delta_{s-1}(r,m) > \gamma_{s}(r,m) + \delta_{s}(r,m)$, except one case: if m is odd, r even and $s = \frac{m-1}{2}$, then $\gamma_{s-1}(r,m) + \delta_{s-1}(r,m) = \gamma_{s}(r,m) + \delta_{s}(r,m)$ and $RM_s(r,m) = RM_{s-1}(r,m)$.

Proof: First of all, note that $\gamma_{s-1}(r,m) + \delta_{s-1}(r,m) = \gamma_{s}(r,m) + \delta_{s}(r,m)$ when $r \notin \{1,\dots,m-2\}$, since in these cases the codes are equal for any $1 \leq s \leq \lfloor\frac{m-1}{2}\rfloor$. Now, we will proceed by induction on $m \geq 3$. Except when $m \geq 3$ odd and $s = \frac{m-1}{2}$, the $RM_s(r,m)$ codes are obtained using the Plotkin construction. In these cases it is easy to see that $\gamma_{s-1}(r,m) + \delta_{s-1}(r,m) > \gamma_{s}(r,m) + \delta_{s}(r,m)$, by Definition 3.

On the other hand, when $m \geq 3$ odd and $s = \frac{m-1}{2}$, the $RM_s(r,m)$ and $RM_{s-1}(r,m)$ codes are obtained using the

BQ-Plotkin and Plotkin construction, respectively. Therefore, the generator matrices can be constructed as

$$\bar{G}_{s-1(r,m)} = PC\big(PC(\bar{G}_{s-1(r,m-2)}, \bar{G}_{s-1(r-1,m-2)}),\\ PC(\bar{G}_{s-1(r-1,m-2)}, \bar{G}_{s-1(r-2,m-2)})\big)$$

and

$$\bar{G}_{s(r,m)} = BQ(\bar{G}_{s-1(r,m-2)}, \bar{G}_{s-1(r-1,m-2)}, \bar{G}_{s-1(r-2,m-2)}).$$

By Definitions 3 and 4, we have that $\gamma_{s-1(r,m)} + \delta_{s-1(r,m)} - \gamma_{s(r,m)} - \delta_{s(r,m)} = \gamma_{s-1(r-1,m-2)}$. By Lemma 6, $\gamma_{s-1(r-1,m-2)} = 0$ if and only if r is even. Hence, if r is even, then $\gamma_{s-1(r,m)} + \delta_{s-1(r,m)} = \gamma_{s(r,m)} + \delta_{s(r,m)}$, otherwise $\gamma_{s-1(r,m)} + \delta_{s-1(r,m)} > \gamma_{s(r,m)} + \delta_{s(r,m)}$. Moreover, if r is even, since $\gamma_{s-1(r-1,m-2)} = 0$, then the generator matrices satisfy that $\bar{G}'_{s-1(r-1,m-2)} = \hat{G}_{s-1(r-1,m-2)} = \bar{G}_{s-1(r-1,m-2)}$. In this case, it is easy to find a linear combination of rows that transforms the matrix $\bar{G}_{s-1(r,m)}$ into the matrix $\bar{G}_{s(r,m)}$, and then the codes are equals. □

Theorem 21: For all $m \geq 3$ and $r = 1$, there are at least $\lfloor \frac{m-1}{2} \rfloor$ nonisomorphic binary codes with the same parameters as the code $RM(1,m)$.

For all $m \geq 4$ and $2 \leq r \leq m-2$, there are at least $\lfloor \frac{m+1}{2} \rfloor$ nonisomorphic binary codes with the same parameters as the code $RM(r,m)$, except when m is odd, and r is even. In this case, there are at least $\frac{m-1}{2}$ nonisomorphic binary codes with the same parameters as the code $RM(r,m)$.

Proof: For $r = 1$, the result was proved in [12]. For $2 \leq r \leq m-2$, the proof is consequence of Theorem 19 and Proposition 20. □

VI. Conclusions

In a recent paper [8], new families of quaternary linear codes, the $\mathcal{RM}_s(r,m)$ codes, are constructed in such a way that, after the Gray map, the $\mathbb{Z}_4$-linear codes fulfill the same properties and fundamental characteristics as the binary linear Reed–Muller codes. In this paper, a structural invariant for binary codes, the dimension of the kernel, is used to classify these new families of quaternary linear Reed–Muller codes as well as their binary images under the Gray map. Note that all these codes are completely classified from r, m and the dimension of the kernel. Using a recursive construction, we give the generator matrices of the kernel and compute the exact values of the dimension of the kernel for all the feasible values of s, r and m. This invariant allows us to classify all the codes except when m is odd, $m \geq 5$, and r is even. In these cases, there are two codes with the same dimension of the kernel, but in fact these two codes are equal.

As we already mentioned, there are other families of quaternary linear Reed–Muller codes, like the ones presented in [19], denoted by $\mathcal{CRM}(r,m)$. The codes in $\mathcal{CRM}(r,m)$ are constructed starting from all quaternary linear Hadamard and extended 1-perfect codes and using just the Plotkin construction. Therefore, their corresponding $\mathbb{Z}_4$-linear codes do not satisfy the properties (4) and (5) quoted in Proposition 2. Moreover, after computing the dimension of the kernel for the $\mathcal{RM}_s(r,m)$ codes, they are not included in the $\mathcal{CRM}(r,m)$ family. For example, for $r = 3$ and $m = 5$, the three $\mathcal{RM}_s(3,5)$ codes have dimensions of the kernel $\{14, 16, 20\}$, and the two $\mathcal{CRM}(3,5)$ codes have dimensions of the kernel $\{16, 20\}$. Note that each code in $\mathcal{CRM}(r,m)$ is monomially equivalent to a code in $\mathcal{RM}_s(r,m)$, and vice versa, for all $m \geq 1$ and $r \in \{0, 1, m-2, m-1, m\}$. Finally, note that we could construct more quaternary linear Reed–Muller codes, using the same techniques as in [19] and the $\mathcal{RM}_s(r,m)$ codes not included in the $\mathcal{CRM}(r,m)$ codes. These new codes, which will may not satisfy the properties (4) and (5) quoted in Proposition 2, will probably not be equivalent neither to the $\mathcal{RM}_s(r,m)$ nor to the $\mathcal{CRM}(r,m)$ codes.

Another family of quaternary Reed–Muller codes are the ones presented in [5], denoted by $\mathcal{QRM}(r,m)$. The codes in $\mathcal{QRM}(r,m)$ can not be compared with the $\mathcal{RM}_s(r,m)$ codes, as quaternary codes. Note that the minimum Lee distances of the $\mathcal{RM}_s(r,m)$ codes are exactly the same as the minimum Hamming distances of the RM codes, and for the $\mathcal{QRM}(r,m)$ codes these distances are not known. On the other hand, after the modulo 2 map for the $\mathcal{QRM}(r,m)$ codes, and the Gray map for the $\mathcal{RM}_s(r,m)$ codes, we obtain binary codes with the same parameters as the RM codes. The difference is that the former are always linear, and the latter are nonlinear, for example, for all $m \geq 5$ and $r \in \{3, \ldots, m-2\}$.

Acknowledgment

The authors wish to thank the referees for a careful reading of the manuscript and for their very helpful comments.

References

[1] J. Pernas, J. Pujol, and M. Villanueva, "Kernel dimension for some families of quaternary Reed–Muller codes," in *Mathematicals Methods in Computer Science*, Karlsruhe, Germany, Dec. 2008, vol. 5393, pp. 128–141.

[2] F. J. MacWilliams and N. J. A. Sloane*, The Theory of Error-Correcting Codes: Vol.: 1*. Amsterdam, The Netherlands: North-Holland, 1977.

[3] W. C. Huffman and V. Pless*, Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[4] H. Bauer, B. Ganter, and F. Hergert, "Algebraic techniques for nonlinear codes," *Combinatorica*, vol. 3, pp. 21–33, 1983.

[5] A. Hammons, P. Kumar, A. Calderbank, N. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 301–319, 1994.

[6] X. Hou, J. Lahtonen, and S. Koponen, "The Reed–Muller code $R(r,m)$ is not $\mathbb{Z}_4$-linear for $3 < r < m-2$," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 798–799, 1998.

[7] J. Pujol, J. Rifà, and F. I. Solov'eva, "Quaternary Plotkin constructions and quaternary Reed–Muller codes," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Bangalore, India, Dec. 2007, vol. 4851, pp. 148–157.

[8] J. Pujol, J. Rifà, and F. I. Solov'eva, "Construction of $\mathbb{Z}_4$-linear Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 1, pp. 99–104, 2009.

[9] J. Borges, C. Fernández, and K. T. Phelps, "Quaternary Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2686–2691, 2005.

[10] J. Borges, K. T. Phelps, J. Rifà, and V. A. Zinoviev, "On $\mathbb{Z}_4$-linear Preparata-like and Kerdock-like codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 2834–2843, 2003.

[11] J. Borges, K. T. Phelps, and J. Rifà, "The rank and kernel of extended 1-perfect $\mathbb{Z}_4$-linear and additive non-$\mathbb{Z}_4$-linear codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 8, pp. 2028–2034, 2003.

[12] D. S. Krotov, "$\mathbb{Z}_4$-linear Hadamard and extended perfect codes," in *Proc. Int. Workshop on Coding and Cryptography*, Paris, France, Jan. 2001, pp. 329–334.

[13] 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," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 316–319, 2006.

[14] J. Cannon and W. Bosma, *Handbook of Magma Functions*. Sydney, Australia: Univ. of Sydney Press, 1994.

[15] J. Pernas, J. Pujol, and M. Villanueva, Codes Over $\mathbb{Z}_4$. A Magma Package Univ. Autònoma de Barcelona, Bellaterra, 2008 [Online]. Available: http://scg.uab.cat

[16] C. Fernàndez-Córdoba, J. Pujol, and M. Villanueva, "On rank and kernel of $\mathbb{Z}_4$-linear codes," in *Coding Theory and Applications*, Medina del Campo, Spain, Sep. 2008, vol. 5228, pp. 231–247.

[17] C. Fernández-Córdoba, J. Pujol, and M. Villanueva, "$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: Rank and kernel," *Designs, Codes Cryptogr.*, vol. 56, no. 1, pp. 43–51, 2010.

[18] J. Borges, C. Fernández-Córdoba, and K. T. Phelps, "ZRM codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 380–386, 2008.

[19] F. I. Solov'eva, "On $\mathbb{Z}_4$-linear codes with the parameters of Reed–Muller codes," *Probl. Inf. Transm.*, vol. 43, no. 1, pp. 26–32, 2007.

[20] Z. Wan and C. H. Wan, *Quaternary Codes*. : World Scientific Publishing Co. Pte. Ltd., 1997.

[21] J. Rifà and L. Ronquillo, "About the $\mathbb{Z}_4$-linear Reed–Muller $\mathcal{ZRM}^-(r, m-1)$ and $\mathcal{RM}\ (r, m)$ codes," in *VI Jornadas de Matemática Discreta y Algorítmica*, Lleida, Spain, May 2008, vol. 6, pp. 517–526.

Jaume Pernas was born in Barcelona, Catalonia, Spain, in April 1982. He received the B.S. and M.S. degrees in computer science from the Universitat Autònoma de Barcelona, Spain, in 2005 and 2008, respectively. He is currently working in the Information and Communications Engineering Department at the same university while pursuing the Ph.D. degree. His research interests include subjects related to combinatorics, algebra and coding theory.

Jaume Pujol was born in Seu d'Urgell, Catalonia, Spain, in December 1955. He received the B.S. degree in mathematics in 1978, the B.S. degree in computer science in 1989, and the M.S. and Ph.D. degrees in computer science in 1991 and 1995, respectively.

Since 1988, he has been a member of the Information and Communications Engineering Department at the Universitat Autònoma de Barcelona, Spain, where he is currently an Associate Professor. His research interest include subjects related to digital communications, coding theory, data compression, and graph theory.

Mercè Villanueva was born in Roses, Catalonia, Spain, in January 1972. She received the B.S. degree in mathematics in 1994 from the Universitat Autònoma de Barcelona, and the M.S. and Ph.D. degrees in computer science in 1996 and 2001, respectively, from the same university.

In 1994, she joined the Information and Communications Engineering Department, at the Universitat Autònoma de Barcelona, as an Assistant Professor, and was promoted to Associate Professor in 2002. Her research interests include subjects related to combinatorics, algebra, coding theory and graph theory.

Appendix D

On the Permutation Automorphism Group of Quaternary Linear Hadamard Codes

On the Permutation Automorphism Group of Quaternary Linear Hadamard Codes[*]

Jaume Pernas, Jaume Pujol, and Mercè Villanueva

jaume.pernas@uab.cat, jaume.pujol@uab.cat, merce.villanueva@uab.cat
Universitat Autònoma de Barcelona, Spain

Abstract. A quaternary linear Hadamard code $\mathcal{C}$ is a code over $\mathbb{Z}_4$ such that, after the Gray map, gives a binary Hadamard code. The permutation automorphism group of a quaternary linear code $\mathcal{C}$ is defined as $\mathrm{PAut}(\mathcal{C}) = \{\sigma \in S_n : \sigma(\mathcal{C}) = \mathcal{C}\}$. In this paper, the order of the permutation automorphism group of all quaternary linear Hadamard codes is established by computing the orbits of the action of $\mathrm{PAut}(\mathcal{C})$ on $\mathcal{C}$. Since the dual of a Hadamard code is an extended 1-perfect code in the quaternary sense, their permutation automorphism group is also computed.

Keywords: Quaternary linear codes, Hadamard codes, 1-perfect codes, permutation automorphism group.

1 Introduction

Let $\mathbb{Z}_2$ and $\mathbb{Z}_4$ be the ring of integers modulo 2 and modulo 4, respectively. Let $\mathbb{Z}_2^n$ be the set of all binary vectors of length n and let $\mathbb{Z}_4^n$ be the set of all quaternary vectors of length n. Any nonempty subset C of $\mathbb{Z}_2^n$ is a binary code and a subgroup of $\mathbb{Z}_2^n$ is called a *binary linear code*. Equivalently, any nonempty subset $\mathcal{C}$ of $\mathbb{Z}_4^n$ is a quaternary code and a subgroup of $\mathbb{Z}_4^n$ is called a *quaternary linear code*.

Let $\mathcal{C}$ be a quaternary linear code. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$, it is isomorphic to an abelian structure $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, $\mathcal{C}$ is of type $2^\gamma 4^\delta$ as a group, it has $|\mathcal{C}| = 2^{\gamma+2\delta}$ codewords and $2^{\gamma+\delta}$ codewords of order two. Let ϕ be the Gray map defined as $\phi : \mathbb{Z}_4^n \longrightarrow \mathbb{Z}_2^{2n}$, $\phi(v_1, \ldots, v_n) = (\varphi(v_1), \ldots, \varphi(v_n))$, where $\varphi(0) = (0,0)$, $\varphi(1) = (0,1)$, $\varphi(2) = (1,1)$, $\varphi(3) = (1,0)$. The binary image $C = \phi(\mathcal{C})$ of any quaternary linear code $\mathcal{C}$ of length n and type $2^\gamma 4^\delta$ is called a $\mathbb{Z}_4$*-linear code* of length $2n$ and type $2^\gamma 4^\delta$.

Recently, new families of quaternary linear Reed-Muller codes such that, after the Gray map, the corresponding $\mathbb{Z}_4$-linear codes have the same parameters and properties as the

[*] This work has been partially supported by the Spanish MICINN under Grants PCI2006-A7-0616 and TIN2010-17358, and by the Catalan AGAUR under Grant 2009SGR1224.

codes in the usual binary linear Reed-Muller family have been introduced [1,2]. Specifically, there are $\lfloor\frac{m+1}{2}\rfloor$ such families, and these quaternary codes of length 2^{m-1} are denoted by $\mathcal{RM}_s(r,m)$, $m \geq 1$, $0 \leq r \leq m$ and $0 \leq s \leq \lfloor\frac{m-1}{2}\rfloor$. It is known that all $\mathbb{Z}_4$-linear Hadamard and extended 1-perfect codes are included in these Reed-Muller families of codes taking $r = 1$ and $r = m - 2$, respectively. The codes for these two values of r were classified in [3] using the dimension of the kernel and the rank, respectively. Later, all codes from these families were classified in [4] using the dimension of the kernel.

Let S_n be the symmetric group of permutations on the set $\{1,\dots,n\}$. A $\sigma \in S_n$ acts on words of $\mathbb{Z}_4^n$ by permuting the coordinates, $\sigma((c_1,c_2,\dots,c_n)) = (c_{\sigma^{-1}(1)}, c_{\sigma^{-1}(2)},\dots, c_{\sigma^{-1}(n)})$. The group operation in S_n is the function composition, denoted by juxtaposition of the permutations. The composition $\sigma_1\sigma_2$ maps any element x to $\sigma_1(\sigma_2(x))$. The *permutation automorphism group* of a quaternary linear code $\mathcal{C}$ is defined as $\mathrm{PAut}(\mathcal{C}) = \{\sigma \in S_n : \sigma(\mathcal{C}) = \mathcal{C}\}$, where $\sigma(\mathcal{C}) = \{\sigma(c) : c \in \mathcal{C}\}$. It is said that two quaternary linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of length n are *permutational equivalent* if there exists $\sigma \in S_n$ such that $\mathcal{C}_1 = \sigma(\mathcal{C}_2)$.

The automorphism group of a code is an invariant, so it can help in the classification of some families of codes. Moreover, knowing the automorphism group can also be used in decoding algorithms and to describe some other properties like the weight distribution. The automorphism group of $\mathbb{Z}_2\mathbb{Z}_4$-linear 1-perfect codes, which include the $\mathbb{Z}_4$-linear 1-perfect codes, has been studied in [5]. In general, the permutation automorphism group of (nonlinear) binary 1-perfect codes has also been studied before, obtaining some partial results [6,7,8,9].

In this paper, we will study the permutation automorphism group of the quaternary linear Hadamard codes, that is, $\mathrm{PAut}(\mathcal{RM}_s(1,m))$ for any $m \geq 1$ and $0 \leq s \leq \lfloor\frac{m-1}{2}\rfloor$. For shortness reasons we will denote this group by $P_{s,m} = \mathrm{PAut}(\mathcal{RM}_s(1,m)) \leq S_n$, where $n = 2^{m-1}$; the Hadamard code by $\mathcal{H}_{s,m} = \mathcal{RM}_s(1,m)$; and its generator matrix by $\mathcal{G}_{s,m}$.

The *orbit* of a codeword $u \in \mathcal{H}_{s,m}$ under the action of $P_{s,m}$ is denoted by the set $P_{s,m}(u) = \{\sigma(u) : \sigma \in P_{s,m}\}$. Note that, since $P_{s,m}$ is the permutation automorphism group of $\mathcal{H}_{s,m}$, $P_{s,m}(u) \subseteq \mathcal{H}_{s,m}$. Moreover, two codewords $u,v \in \mathcal{H}_{s,m}$ are said to be *$P_{s,m}$-equivalent* if there exists a permutation $\sigma \in P_{s,m}$ such that $\sigma(u) = v$. Since this is an equivalence relationship, $\mathcal{H}_{s,m}$ is partitioned into classes or *orbits*. On the other hand, the *stabiliser* of $u \in \mathcal{H}_{s,m}$ in $P_{s,m}$ is denoted by the subgroup $N^u_{s,m} = \{\sigma \in P_{s,m} : \sigma(u) = u\}$. Moreover, given a set $\{u_1,\dots,u_t\}$, the stabiliser of all this set of codewords is denoted by $N^{u_1,\dots,u_t}_{s,m} = \{\sigma \in P_{s,m} : \sigma(u_i) = u_i, \forall i \in \{1,\dots,t\}\}$. Finally, the orbit-stabiliser theorem shows that $|P_{s,m}| = |P_{s,m}(u)||N^u_{s,m}|$ for all $u \in \mathcal{H}_{s,m}$ [10].

2 Quaternary linear Hadamard codes

Now, we give a recursive construction for the quaternary linear Hadamard codes $\mathcal{H}_{s,m}$, $m \geq 1$ and $0 \leq s \leq \lfloor\frac{m-1}{2}\rfloor$. For every admissible pair s and m, there is one Hadamard code of length 2^{m-1} and type $2^{m-2s-1}4^{s+1}$. In [1,2], a general way to construct $\mathcal{RM}_s(r,m)$ codes is described, but for this particular case where $r = 1$, the following recursive construction can also be used:

$$\mathcal{G}_{0,1} = (1)\,;$$
$$\mathcal{G}_{s,m} = \begin{pmatrix} \mathcal{G}_{s,m-1} & \mathcal{G}_{s,m-1} \\ \mathbf{0} & \mathbf{2} \end{pmatrix} \text{ if } m > 2s+1,\ s \geq 0; \qquad (1)$$

$$\mathcal{G}_{s,m} = \begin{pmatrix} \mathcal{G}_{s-1,m-2} & \mathcal{G}_{s-1,m-2} & \mathcal{G}_{s-1,m-2} & \mathcal{G}_{s-1,m-2} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \end{pmatrix} \text{ if } m = 2s+1,\ s \geq 1; \qquad (2)$$

where $\mathbf{0}$, $\mathbf{1}$, $\mathbf{2}$ and $\mathbf{3}$ means the repetition of symbol $0, 1, 2$ and 3, respectively.

Using this construction, the vectors of order four remain in the upper part of the generator matrix $\mathcal{G}_{s,m}$ and the vectors of order two in the lower part. From now on, given a Hadamard code $\mathcal{H}_{s,m}$ of type $2^\gamma 4^\delta$, we will denote by $\{v_1, \dots, v_\delta\}$ the vectors of order four in $\mathcal{G}_{s,m}$ and $\{u_1, \dots, u_\gamma\}$ the vectors of order two, conserving the order given by the construction of $\mathcal{G}_{s,m}$.

Lemma 1. *The codewords of a quaternary linear Hadamard code $\mathcal{H}_{s,m}$ of length $n = 2^{m-1}$, where $m \geq 1$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$, can be classified into three types:*

(a) The four codewords $\mathbf{0}$, $\mathbf{1}$, $\mathbf{2}$ and $\mathbf{3}$.
(b) The codewords with only zeros and twos or only ones and threes. The number of zeros, ones, twos or threes is always $n/2$ in each codeword.
(c) The codewords with all symbols $0, 1, 2, 3$. The number of zeros, ones, twos and threes is always $n/4$ in each codeword.

Moreover, there are 4 codewords of type (a), $2^{m-s+1} - 4$ of type (b), and $2^{m+1} - 2^{m-s+1}$ of type (c).

Proof. The code $\mathcal{H}_{0,1}$ only contains the four codewords of type (a). The result can be proved by induction on m separated in two cases: for $m > 2s+1$ using the construction given by matrix (1), and for $m = 2s+1$ using the construction given by matrix (2). □

3 Permutation automorphism groups

In this section, we will give the order of the permutation automorphism group for the codes $\mathcal{H}_{s,m}$, where $m \geq 1$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$. In order to study these groups, we computed them for some fixed s and m. We used a program presented in [11] which can compute automorphism groups of quaternary linear codes.

Note that, $P_{0,m} = \mathrm{PAut}(\mathcal{H}_{0,m})$ is isomorphic to the permutation automorphism group of the binary linear Hadamard code of length 2^{m-1}, which is the general affine group $GA(m-1, 2)$ [12]. Therefore, $|P_{0,m}| = |GA(m-1,2)| = 2^{m-1}(2^{m-1}-1)(2^{m-1}-2)\dots(2^{m-1}-2^{m-2})$, which is equivalent to the expression given by Theorem 6 taking $s = 0$.

By construction using matrix (1), given a permutation of degree $n = 2^{m-2}$ that fixes the Hadamard code generated by the matrix $\mathcal{G}_{s,m-1}$, it is possible to construct a permutation of degree $2n$ that fixes the Hadamard code generated by $\mathcal{G}_{s,m}$ as it follows. Let $\sigma \in S_n$ be a permutation. We define the permutation $(\sigma|\sigma) = \tau\sigma\tau\sigma \in S_{2n}$ where $\tau = (1, 1+n)(2, 2+n)\dots(n, 2n)$. Note that $\tau\sigma\tau$ is the same permutation as σ but applied on the coordinates $\{n+1, \dots, 2n\}$. Then, it is easy to see that σ and $\tau\sigma\tau$ are disjoint, and if $\sigma \in P_{s,m-1}$ then $(\sigma|\sigma) \in P_{s,m}$. Let $P < S_n$ be a subgroup of permutations. We define the subgroup $(P|P) = \{(\sigma|\sigma) : \sigma \in P\} < S_{2n}$. By construction, P fixes the code $\mathcal{H}_{s,m-1}$ if and only if $(P|P)$ fixes the code $\mathcal{H}_{s,m}$.

Proposition 2. *The codewords of $\mathcal{H}_{s,m}$ of length $n = 2^{m-1}$, where $m \geq 1$ odd and $s = \frac{m-1}{2}$, are partitioned into the next orbits under the action of $P_{s,m}$:*

(i) *four orbits of one element with the four codewords of type (a);*
(ii) *one orbit with the codewords of order two and type (b) with* $2^{m-s}-2$ *elements; another orbit with the codewords of order four and type (b) with* $2^{m-s}-2$ *elements;*
(iii) *one orbit with the codewords of type (c) with* $2^{m+1}-2^{m-s+1}$ *elements.*

Proof. The result can be proved by induction on $m \geq 1$ odd, and using Lemma 1. An important fact is that, in this case, the code $\mathcal{H}_{s,m}$ is of type $2^0 4^{s+1}$, so there are not rows of order two in the generator matrix $\mathcal{G}_{s,m}$. □

Corollary 3. *Let* $\mathcal{H}_{s,m}$ *be a quaternary linear Hadamard code of length* $n = 2^{m-1}$*, where* $m \geq 1$ *odd and* $s = \frac{m-1}{2}$*. The permutation automorphism group of the codewords of type (c) is* $P_{s,m}$*.*

Proposition 4. *The codewords of* $\mathcal{H}_{s,m}$ *of length* $n = 2^{m-1}$*, where* $m \geq 1$ *and* $0 \leq s \leq \lfloor \frac{m-2}{2} \rfloor$*, are partitioned into the next orbits under the action of* $P_{s,m}$*:*

(i) *four orbits of one element with the four codewords of type (a);*
(ii) *one orbit with the codewords of type (b) and form* $u = \sum_{i=1}^{\delta} \lambda_i v_i, \lambda_i \in \{0,2\}$ *with* $2^{s+1}-2$ *elements; another orbit with the codewords of type (b) and form* $u + \mathbf{1}$ *with* $2^{s+1}-2$ *elements;*
(iii) *one orbit with the remaining codewords of order two and type (b) with* $2^{m-s}-2^{s+1}$ *elements; another orbit with the remaining codewords of order four and type (b) with* $2^{m-s}-2^{s+1}$ *elements;*
(iv) *one orbit with the codewords of type (c) with* $2^{m+1}-2^{m-s+1}$ *elements.*

Proof. The result can be proved by induction on $m > 2s+1$, and using Lemma 1. In this case, there are two orbits more because the codewords of type (b) are partitioned into four orbits. That is consequence of the fact that the codewords $\{u_1, \ldots, u_\gamma\}$ in $\mathcal{G}_{s,m}$ are not linear combinations of the codewords $\{v_1, \ldots, v_\delta\}$ in $\mathcal{G}_{s,m}$. □

Corollary 5. *Let* $\mathcal{H}_{s,m}$ *be a quaternary linear Hadamard code of length* $n = 2^{m-1}$*, where* $m \geq 1$ *and* $0 \leq s \leq \lfloor \frac{m-2}{2} \rfloor$*. The permutation automorphism group of the codewords of type (c) is* $P_{s,m}$*.*

Theorem 6. *Let* $\mathcal{H}_{s,m}$ *be a quaternary linear Hadamard code of length* $n = 2^{m-1}$*, where* $m \geq 1$ *and* $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$*. The order of the permutation automorphism group* $P_{s,m} = \mathrm{PAut}(\mathcal{H}_{s,m})$ *is:*

- $|P_{0,1}| = 1$*;*
- $|P_{s,m}| = |P_{s-1,m-2}| \cdot 4^{s-1} \cdot (2^{2s+2} - 2^{s+2})$*, if* $m = 2s+1$*;*
- $|P_{s,m}| = |P_{s,m-1}| \cdot 2^{m-s-2} \cdot (2^{m-s} - 2^{s+1})$*, if* $m > 2s+1$*.*

Proof. The code $\mathcal{H}_{0,1}$ is of length 1, so the permutation automorphism group $P_{0,1}$ only contains the identity permutation.

In general, first of all, note that the stabiliser $N_{s,m}^{u_\gamma,\ldots,u_1,v_\delta,\ldots,v_2}$ only contains the identity permutation. This can be proved by induction on the rows of the generator matrix $\mathcal{G}_{s,m}$. Thus, we can compute the order of $|P_{s,m}|$ using the orbit-stabiliser property recursively as follows:

$$|P_{s,m}| = |P_{s,m}(u_\gamma)||N_{s,m}^{u_\gamma}| = |P_{s,m}(u_\gamma)||N_{s,m}^{u_\gamma}(u_{\gamma-1})||N_{s,m}^{u_\gamma,u_{\gamma-1}}| = \cdots$$

$$= |P_{s,m}(u_\gamma)||N_{s,m}^{u_\gamma}(u_{\gamma-1})||N_{s,m}^{u_\gamma,u_{\gamma-1}}(u_{\gamma-2})| \cdots |N_{s,m}^{u_\gamma,\ldots,u_1}(v_\delta)|$$

$$|N_{s,m}^{u_\gamma,\ldots,u_1,v_\delta}(v_{\delta-1})| \cdots |N_{s,m}^{u_\gamma,\ldots,u_1,v_\delta,\ldots,v_3}(v_2)||N_{s,m}^{u_\gamma,\ldots,u_1,v_\delta,\ldots,v_2}|.$$

For $m > 2s+1$, the chain of orbits for the codewords $\{u_{\gamma-1}, \ldots, u_1, v_\delta, \ldots, v_2\}$ is the same as for $\mathcal{H}_{s,m-1}$, but having double number of codewords: $(v|v)$ and $(v|v+\mathbf{2})$. Then, we can rewrite the above expression as $|P_{s,m}| = |P_{s,m-1}| \cdot 2^{\gamma+\delta-2} \cdot |P_{s,m}(u_\gamma)|$. The result follows since by Proposition 4 we know the size of the orbit that contains u_γ and $\gamma+\delta-2 = m-s-2$.

For $m = 2s+1$, we have a similar scenario, except that the chain of orbits contains four times more codewords than for $\mathcal{H}_{s-1,m-1}$, since the code is also four times bigger. Moreover, in this case $\gamma = 0$, so the first orbit is $P_{s,m}(v_\delta)$. Since the size of this orbit containing v_δ is given by Proposition 2, the result follows. □

Corollary 7. *Let $\mathcal{H}_{s,m}$ be a quaternary linear Hadamard code of length $n = 2^{m-1}$, where $m \geq 1$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$. The order of the permutation automorphism group $P_{s,m} = \mathrm{PAut}(\mathcal{H}_{s,m})$ is:*

- $|P_{0,1}| = 1$;
- $|P_{s,m}| = \prod_{i=1}^{s} 2^{3i}(2^i - 1)$, *if* $m = 2s+1$ *and* $s \geq 1$;
- $|P_{s,m}| = |P_{s,2s+1}| \prod_{i=2s+2}^{m} 2^{i-1}(2^{i-2s-1} - 1)$, *if* $m > 2s+1$.

Table 1. Order of $P_{s,m} = \mathrm{PAut}(\mathcal{H}_{s,m})$ for $1 \leq m \leq 9$. Note that $n = 2^{m-1}$.

$s \backslash m$	1	2	3	4	5	6	7	8	9
0	1	2	$2^3 \cdot 3$	$2^6 \cdot 3 \cdot 7$	$2^{10} \cdot 3 \cdot 7 \cdot 15$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
1			2^3	2^6	$2^{10} \cdot 3$	$2^{15} \cdot 3 \cdot 7$	$2^{21} \cdot 3 \cdot 7 \cdot 15$	$\ldots$	$\ldots$
2					$2^9 \cdot 3$	$2^{14} \cdot 3$	$2^{20} \cdot 3^2$	$2^{27} \cdot 3^2 \cdot 7$	$2^{35} \cdot 3^2 \cdot 7 \cdot 15$
3							$2^{18} \cdot 3 \cdot 7$	$2^{25} \cdot 3 \cdot 7$	$2^{33} \cdot 3^2 \cdot 7$
4									$2^{30} \cdot 3 \cdot 7 \cdot 15$

Given a quaternary linear code $\mathcal{C}$ of length $n = 2^m$, the *inner product* for any two vectors $u, v \in \mathbb{Z}_4^n$ is defined as: $\langle u, v \rangle = \sum_{i=1}^{n} u_i v_i \in \mathbb{Z}_4$, and the *quaternary dual code* of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined in the standard way as:

$$\mathcal{C}^\perp = \{u \in \mathbb{Z}_4^n \ : \ \langle u, v \rangle = 0 \text{ for all } v \in \mathcal{C}\}.$$

Note that the quaternary dual of a Hadamard code $\mathcal{H}_{s,m}$ is a quaternary linear extended 1-perfect code denoted by $\mathcal{E}_{s,m} = \mathcal{H}_{s,m}^\perp$. It is easy to prove that for any quaternary linear code $\mathcal{C}$, we have that $\mathrm{PAut}(\mathcal{C}) = \mathrm{PAut}(\mathcal{C}^\perp)$. Therefore, in particular, $\mathrm{PAut}(\mathcal{H}_{s,m}) = \mathrm{PAut}(\mathcal{E}_{s,m})$.

4 Conclusions

Several problems related to quaternary codes can be addressed by computing the automorphism group of these codes. In this paper, the order of the permutation automorphism grup of all quaternary linear Hadamard codes and their duals (all quaternary linear extended 1-perfect codes) is computed. To compute this order, the structure of the orbits of the codewords under the action of this group is deeply studied. In a further work a complete description of these permutation automorphism groups and their relations with the corresponding binary codes will be established, as well as, a generalization of these results for all quaternary linear Reed Muller codes $\mathcal{RM}_s(r,m)$, $m \geq 1$, $0 \leq r \leq m$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$ [2].

References

1. J. Pujol, J. Rifà, and F. I. Solov'eva, "Quaternary Plotkin constructions and quaternary Reed-Muller codes," in *Proc. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, ser. LNCS, vol. 4851, India, Dec. 2007, pp. 148–157.
2. J. Pujol, J. Rifà, and F. I. Solo'eva, "Construction of $\mathbb{Z}_4$-linear Reed-Muller codes," *Trans. Inf. Theory*, vol. 55, no. 1, pp. 99–104, 2009.
3. D. S. Krotov, "$\mathbb{Z}_4$-linear Hadamard and extended perfect codes," in *Proc. Int. Workshop on Coding and Cryptography*, Paris, France, Jan. 2001, pp. 329–334.
4. J. Pernas, J. Pujol, and M. Villanueva, "Classification of some families of quaternary Reed-Muller codes," *accepted in Trans. Inf. Theory*, 2011.
5. K. T. Phelps and J. Rifà, "On binary 1-perfect additive codes: some structural properties," *Trans. Inf. Theory*, vol. 48, no. 9, pp. 2087–2592, 2002.
6. O. Heden, F. Pasticci, and T. Westerback, "On the existance of extended perfect binary codes with trivial symmetry group," *Advances in Mathematics of Communications*, vol. 3, no. 3, pp. 295–309, 2009.
7. O. Heden, "On the symmetry group of perfect 1-error correcting binary codes," *J. Combin. Math. Combin. Comput.*, vol. 52, pp. 109–115, 2005.
8. S. V. Avgustinovich, F. I. Solov'eva, and O. Heden, "On the structure of symmetry groups of vasil'ev codes," *Advances in Mathematics of Communications*, vol. 41, no. 2, pp. 105–112, 2005.
9. C. Fernández-Córdoba, K. Phelps, and M. Villanueva, "Involutions in binary perfect codes," *accepted in Trans. Inf. Theory*, 2011.
10. P. J. Cameron, *Permutation Groups*. Cambridge Univ. Press, 1999.
11. T. Feulner, "The automorphism groups of linear codes and canonical representatives of their semilinear isometry classes," *Advances in Mathematics of Communications*, vol. 4, no. 3, pp. 363–383, 2009.
12. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes: Vol.: 1* . North-Holland Publishing Company, 1977.

Appendix E

Characterization of the Automorphism Group of Quaternary Linear Hadamard Codes

Des. Codes Cryptogr.
DOI 10.1007/s10623-012-9678-2

Characterization of the Automorphism Group of Quaternary Linear Hadamard codes

Jaume Pernas · Jaume Pujol · Mercè Villanueva

Received: 14 November 2011 / Accepted: 29 February 2012

Abstract A quaternary linear Hadamard code $\mathcal{C}$ is a code over $\mathbb{Z}_4$ that under the Gray map, gives a binary Hadamard code. The permutation automorphism group of a quaternary linear code $\mathcal{C}$ of length n is defined as $\mathrm{PAut}(\mathcal{C}) = \{\sigma \in S_n : \sigma(\mathcal{C}) = \mathcal{C}\}$. In this paper, the order of the permutation automorphism group of a family of quaternary linear Hadamard codes is established. Moreover, these groups are completely characterized by computing the orbits of the action of $\mathrm{PAut}(\mathcal{C})$ on $\mathcal{C}$ and by giving the generators of the group. Since the dual of a Hadamard code is an extended 1-perfect code in the quaternary sense, the permutation automorphism group of these codes is also computed.

Keywords Quaternary linear codes, Hadamard codes, 1-perfect codes, permutation automorphism group.

1 Introduction

Let $\mathbb{Z}_2$ and $\mathbb{Z}_4$ be respectively the ring of integers modulo 2 and modulo 4. Let $\mathbb{Z}_2^n$ be the set of all binary words of length n and let $\mathbb{Z}_4^n$ be the set of all quaternary words of length n. Any nonempty subset C of $\mathbb{Z}_2^n$ is a binary code and a subgroup of $\mathbb{Z}_2^n$ is called a *binary linear code*. Equivalently, any nonempty subset $\mathcal{C}$ of $\mathbb{Z}_4^n$ is a quaternary code and a subgroup of $\mathbb{Z}_4^n$ is called a *quaternary linear code*.

This work has been partially supported by the Spanish MICINN under Grant TIN2010-17358, and by the Catalan AGAUR under Grant 2009SGR1224. The material in this paper was presented in part at the 3rd International Castle Meeting on Coding Theory and Applications, Cardona, Spain, September 11-15, 2011 [1].

Departament d'Enginyeria de la Informació i de les Comunicacions
Universitat Autònoma de Barcelona
E-mail: jaume.pernas@uab.cat, jaume.pujol@uab.cat, merce.villanueva@uab.cat

Let $\mathcal{C}$ be a quaternary linear code. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$, it is isomorphic to an abelian structure $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, $\mathcal{C}$ is of type $2^\gamma 4^\delta$ as a group: it has $|\mathcal{C}| = 2^{\gamma+2\delta}$ codewords and $2^{\gamma+\delta}$ of these have order two. Let ϕ be the Gray map defined as $\phi : \mathbb{Z}_4^n \longrightarrow \mathbb{Z}_2^{2n}$, $\phi(v_1, \ldots, v_n) = (\varphi(v_1), \ldots, \varphi(v_n))$, where $\varphi(0) = (0, 0)$, $\varphi(1) = (0, 1)$, $\varphi(2) = (1, 1)$, $\varphi(3) = (1, 0)$. The binary image $C = \phi(\mathcal{C})$ of any quaternary linear code $\mathcal{C}$ of length n and type $2^\gamma 4^\delta$ is called a $\mathbb{Z}_4$*-linear code* of length $2n$ and type $2^\gamma 4^\delta$.

Recently, new families of quaternary linear Reed-Muller codes such that, under the Gray map, the corresponding $\mathbb{Z}_4$-linear codes have the same parameters and properties (length, dimension, minimum distance, inclusion and duality relation) as those in the usual binary linear Reed-Muller family have been introduced [2,3]. Specifically, there are $\lfloor \frac{m+1}{2} \rfloor$ such families, and these quaternary codes of length 2^{m-1} are denoted by $\mathcal{RM}_s(r, m)$, $m \geq 1$, $0 \leq r \leq m$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$. It is known that all $\mathbb{Z}_4$-linear Hadamard and extended 1-perfect codes are included in these Reed-Muller families of codes taking $r = 1$ and $r = m-2$, respectively. These codes for $r = 1$ and $r = m-2$ were classified in [4] by using the dimension of the kernel and the rank, respectively. Later, the corresponding $\mathbb{Z}_4$-linear codes for all $\mathcal{RM}_s(r, m)$ codes were classified in [5] by using the dimension of the kernel.

Let S_n be the symmetric group of permutations on the set $\{1, \ldots, n\}$, and let $id \in S_n$ be the identity permutation. The group operation in S_n is the function composition, denoted by $\circ$. The composition $\sigma_1 \circ \sigma_2$ maps any element x to $\sigma_1(\sigma_2(x))$. A $\sigma \in S_n$ acts linearly on words of $\mathbb{Z}_2^n$ or $\mathbb{Z}_4^n$ by permuting the coordinates, $\sigma((c_1, c_2, \ldots, c_n)) = (c_{\sigma^{-1}(1)}, c_{\sigma^{-1}(2)}, \ldots, c_{\sigma^{-1}(n)})$.

Two quaternary linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of length n are said to be *monomially equivalent*, if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. They are said to be *permutation equivalent* if they differ only by a permutation of coordinates. The *permutation automorphism group* of a quaternary linear code $\mathcal{C}$ is defined as $\mathrm{PAut}(\mathcal{C}) = \{\sigma \in S_n : \sigma(\mathcal{C}) = \mathcal{C}\}$, where $\sigma(\mathcal{C}) = \{\sigma(c) : c \in \mathcal{C}\}$.

The permutation automorphism group of a code is an invariant, so it can help in the classification of some families of codes. Moreover, the automorphism group can also be used in decoding algorithms and to describe some other properties like the weight distribution. The permutation automorphism group of $\mathbb{Z}_2\mathbb{Z}_4$-linear extended 1-perfect codes, which include the $\mathbb{Z}_4$-linear extended 1-perfect codes, has been studied in [6,7]. The permutation automorphism group of (nonlinear) binary 1-perfect codes has also been studied before, obtaining some partial results [8–11].

In this paper, we will study the permutation automorphism group of a family of quaternary linear Hadamard codes, that is, $\mathrm{PAut}(\mathcal{RM}_s(1, m))$ for any $m \geq 1$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$. For shortness reasons, we will denote this group by $P_{s,m} = \mathrm{PAut}(\mathcal{RM}_s(1, m)) \leq S_n$, where $n = 2^{m-1}$, the Hadamard code by $\mathcal{H}_{s,m} = \mathcal{RM}_s(1, m)$, and its generator matrix by $\mathcal{G}_{s,m}$.

Let us recall some fundamental concepts of group theory applied to the group $P_{s,m}$ acting on $\mathcal{H}_{s,m}$. The *orbit* of a codeword $u \in \mathcal{H}_{s,m}$ under the action of $P_{s,m}$ is the set $P_{s,m}(u) = \{\sigma(u) : \sigma \in P_{s,m}\}$. Note that, since $P_{s,m}$

is the permutation automorphism group of $\mathcal{H}_{s,m}$, $P_{s,m}(u) \subseteq \mathcal{H}_{s,m}$. Moreover, two codewords $u, v \in \mathcal{H}_{s,m}$ are said to be $P_{s,m}$*-equivalent* if there exists a permutation $\sigma \in P_{s,m}$ such that $\sigma(u) = v$. Since this is an equivalence relation, $\mathcal{H}_{s,m}$ is partitioned into classes or *orbits*. If there is only one orbit, it is said that the action is *transitive*. The *stabilizer* of $u \in \mathcal{H}_{s,m}$ in $P_{s,m}$ is the subgroup $N^u_{s,m} = \{\sigma \in P_{s,m} : \sigma(u) = u\}$. Finally, the orbit-stabilizer theorem shows that $|P_{s,m}| = |P_{s,m}(u)||N^u_{s,m}|$ for all $u \in \mathcal{H}_{s,m}$ [12].

2 Quaternary linear Hadamard codes

In this section, we will give a recursive construction for the quaternary linear Hadamard codes $\mathcal{H}_{s,m}$, $m \geq 1$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$, and a classification of their codewords.

For every admissible pair s and m, there is a quaternary linear Hadamard code $\mathcal{H}_{s,m}$ of length 2^{m-1} and type $2^{m-2s-1}4^{s+1}$. In [2,3], a general method to construct the $\mathcal{RM}_s(r, m)$ codes is described. However, when $r = 1$, in order to construct the codes $\mathcal{H}_{s,m}$, the following recursive construction of their generator matrices $\mathcal{G}_{s,m}$ over the ring $\mathbb{Z}_4$ can also be used:

$$\mathcal{G}_{0,1} = \begin{pmatrix} 1 \end{pmatrix};$$

$$\mathcal{G}_{s,m} = \begin{pmatrix} \mathcal{G}_{s,m-1} & \mathcal{G}_{s,m-1} \\ \mathbf{0} & \mathbf{2} \end{pmatrix} \text{ if } m > 2s+1,\ s \geq 0; \tag{1}$$

$$\mathcal{G}_{s,m} = \begin{pmatrix} \mathcal{G}_{s-1,m-2} & \mathcal{G}_{s-1,m-2} & \mathcal{G}_{s-1,m-2} & \mathcal{G}_{s-1,m-2} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \end{pmatrix} \text{ if } m = 2s+1,\ s \geq 1; \tag{2}$$

where $\mathbf{0}$, $\mathbf{1}$, $\mathbf{2}$ and $\mathbf{3}$ means the repetition of symbol $0, 1, 2$ and 3, respectively.

Using this construction, the rows of order four remain in the upper part of the generator matrix $\mathcal{G}_{s,m}$ and the rows of order two in the lower part. From now on, given a Hadamard code $\mathcal{H}_{s,m}$ of type $2^\gamma 4^\delta$, we will denote by $\{v_1, \ldots, v_\delta\}$ the rows of order four in $\mathcal{G}_{s,m}$ and $\{u_1, \ldots, u_\gamma\}$ the rows of order two, maintaining the order given by the construction of $\mathcal{G}_{s,m}$. Note that we always have that $v_2 = (0, 1, 2, 3, 0, 1, \ldots, 0, 1, 2, 3)$, $v_\delta = (\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3})$ and $u_\gamma = (\mathbf{0}, \mathbf{2})$.

Lemma 1 *The codewords of the quaternary linear Hadamard code $\mathcal{H}_{s,m}$ of length $n = 2^{m-1}$, where $m \geq 1$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$, can be classified into three types.*

(a) The four codewords $\mathbf{0}$, $\mathbf{1}$, $\mathbf{2}$ *and* $\mathbf{3}$.
(b) The codewords with only zeros and twos or only ones and threes. The number of zeros, ones, twos and threes is in each codeword always $n/2$.
(c) The codewords with all symbols $0, 1, 2, 3$. *The number of zeros, ones, twos and threes is in each codeword always* $n/4$.

Moreover, there are 4 codewords of type (a), $2^{m-s+1} - 4$ *of type (b), and* $2^{m+1} - 2^{m-s+1}$ *of type (c).*

Proof The code $\mathcal{H}_{0,1}$ only contains the four codewords of type (a). The result for $m \geq 2$ can be proved by induction on m. Assume that for any $1 \leq m' < m$ and $s \geq 0$ the code $\mathcal{H}_{s,m'}$ has its codewords classified into these three types. On the one hand, if $m > 2s+1$, the code $\mathcal{H}_{s,m}$ is constructed using matrix (1). In this case, $\mathcal{H}_{s,m} = \{(u,u),\ (u,u+\mathbf{2}) : u \in \mathcal{H}_{s,m-1}\}$. If u is of type (a), (b) or (c), then (u,u) is of type (a), (b) or (c), respectively, and $(u,u+\mathbf{2})$ is of type (b), (b) or (c), respectively. On the other hand, if $m = 2s+1$, the code $\mathcal{H}_{s,m}$ is constructed using matrix (2). In this case, $\mathcal{H}_{s,m} = \{(u,u,u,u),\ (u,u+\mathbf{1},u+\mathbf{2},u+\mathbf{3}),\ (u,u+\mathbf{2},u,u+\mathbf{2}),\ (u,u+\mathbf{3},u+\mathbf{2},u+\mathbf{1}) : u \in \mathcal{H}_{s-1,m-2}\}$. Using the above argument, it is also easy to see that these codewords are of type (a), (b) or (c).

Finally, we will determine how many codewords of each type there are. The four codewords of type (a) are in any code $\mathcal{H}_{s,m}$ by construction. The codewords of order two are of type (b). Any codeword with only ones and threes can be written as a codeword of order two plus $\mathbf{1}$. Therefore, since there are $2^{\gamma+\delta} = 2^{m-s}$ codewords of order two, we have $2^{m-s+1} - 4$ of type (b). The total number of codewords is 2^{m+1}, so the rest of codewords must be of type (c). □

3 Permutation automorphism groups

In this section, we will establish the order of the permutation automorphism groups $P_{s,m}$ for the codes $\mathcal{H}_{s,m}$. Moreover, we will completely describe these groups by computing the orbits of the action of $P_{s,m}$ on $\mathcal{H}_{s,m}$ and by giving the generators of the group. In order to study these groups, we have computed them for some fixed s and m using a computer program presented in [13].

It is easy to see that $P_{0,m}$ is isomorphic to the permutation automorphism group of the binary linear Hadamard code of length 2^{m-1}, which is the general affine group $GA(m-1,2)$ [14]. Therefore, $|P_{0,m}| = |GA(m-1,2)| = 2^{m-1}(2^{m-1}-1)(2^{m-1}-2)\dots(2^{m-1}-2^{m-2})$, which is equivalent to the expression given by Theorem 1 or Corollary 2 taking $s = 0$. The results in this section will focus on codes with $s \geq 1$.

Given two permutations $\sigma_1 \in S_{n_1}$ and $\sigma_2 \in S_{n_2}$, we define the permutation $(\sigma_1|\sigma_2) \in S_{n_1+n_2}$, where σ_1 acts on the coordinates $\{1,\dots,n_1\}$ and σ_2 acts on the coordinates $\{n_1+1,\dots,n_1+n_2\}$. In the same way, we can introduce the permutation $(\sigma_1|\sigma_2|\dots|\sigma_k)$. It is easy to see that if $\sigma \in P_{s,m-1}$ then $(\sigma|\sigma) \in P_{s,m}$, and if $\sigma \in P_{s-1,m-2}$ then $(\sigma|\sigma|\sigma|\sigma) \in P_{s,m}$. Given a subgroup of permutations $P \leq S_n$, we define the subgroup $(P|P) = \{(\sigma|\sigma) : \sigma \in P\} \leq S_{2n}$ and, in general the subgroup $(P|P|\dots|P) = \{(\sigma|\sigma|\dots|\sigma) : \sigma \in P\}$. We also define the subgroups $(id|P) = \{(id|\sigma) : \sigma \in P\}$, and $(id|P|P^2|P^3) = \{(id|\sigma|\sigma^2|\sigma^3) : \sigma \in P\}$ when P is commutative.

Let $A_{s,m}$ and $B_{s,m}$ be two subsets of permutations defined as:

$$A_{s,m} = \{\sigma \in S_n\ :\ \sigma(c) = c + w_c,\ w_c \in \{\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3}\},\ \forall c \in \mathcal{G}_{s,m}\}, \tag{3}$$

$$B_{s,m} = \{\sigma \in S_n\ :\ \sigma(c) = c + w_c,\ w_c \in \{\mathbf{0},\mathbf{2}\},\ \forall c \in \mathcal{G}_{s,m}\}. \tag{4}$$

where $n = 2^{m-1}$. These two subsets will play an important role for determining the structure of $P_{s,m}$.

Lemma 2 *Let $A_{s,m}$ and $B_{s,m}$ be the subsets defined in (3) and (4), respectively.*

(i) The subsets $A_{s,m}$ and $B_{s,m}$ are subgroups of $P_{s,m}$ and $B_{s,m} \leq A_{s,m}$.
(ii) The subgroups $A_{s,m}$ and $B_{s,m}$ are commutative.
(iii) The subgroups $A_{s,m} \trianglelefteq P_{s,m}$ and $B_{s,m} \trianglelefteq P_{s,m}$ are normal.

Proof Note that the words $\mathbf{0}, \mathbf{1}, \mathbf{2}$ and $\mathbf{3}$ belong to any code $\mathcal{H}_{s,m}$. Moreover, any permutation of either $A_{s,m}$ or $B_{s,m}$ fixes the code $\mathcal{H}_{s,m}$, so $A_{s,m} \subseteq P_{s,m}$ and $B_{s,m} \subseteq P_{s,m}$. It is easy to check that they are subgroups of $P_{s,m}$ and $B_{s,m} \leq A_{s,m}$. Furthermore, $A_{s,m}$ and $B_{s,m}$ are commutative. Clearly, for any σ_1, σ_2 in $A_{s,m}$ or $B_{s,m}$, we have that $\sigma_1 \circ \sigma_2(c) = \sigma_2 \circ \sigma_1(c) = c + w_c + w'_c$ for all $c \in \mathcal{H}_{s,m}$, since $\sigma_1(c) = c + w_c$ and $\sigma_2(c) = c + w'_c$, where w_c and $w'_c \in \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}\}$, and the codewords $\mathbf{0}, \mathbf{1}, \mathbf{2}$ and $\mathbf{3}$ are invariant under any permutation. Finally, the same technique can be used to proof the normality of both subgroups. Let $\sigma \in A_{s,m}$. For all $\tau \in P_{s,m}$ and $c \in \mathcal{H}_{s,m}$, we have that $\tau \circ \sigma \circ \tau^{-1}(c) = \tau(\sigma(\tau^{-1}(c))) = \tau(\tau^{-1}(c) + w_{\tau^{-1}(c)}) = c + w_{\tau^{-1}(c)}$, where $w_{\tau^{-1}(c)} \in \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}\}$. Thus, $\tau \circ \sigma \circ \tau^{-1} \in A_{s,m}$. □

Lemma 3 *The subgroup $A_{s,m}$ has order $n = 2^{m-1}$ and is generated by*

(i) $A_{0,1} = \{id\}$;
(ii) $A_{s,m} = \langle (A_{s-1,m-2}|A_{s-1,m-2}|A_{s-1,m-2}|A_{s-1,m-2}), \sigma_1 \rangle$, if $m = 2s + 1$;
(iii) $A_{s,m} = \langle (A_{s,m-1}|A_{s,m-1}), \sigma_2 \rangle$, if $m > 2s + 1$;
where $\sigma_1 = \prod_{i=1}^{n/4}(i, i+n/4, i+n/2, i+3n/4)$ and $\sigma_2 = \prod_{i=1}^{n/2}(i, i+n/2)$.

Proof We will start by showing that the generators belong to $A_{s,m}$. For $m = 1$, it is obvious. For $m = 2s + 1$, the code is constructed using Matrix (2), so we consider the coordinates of any codeword as divided into four blocks of the same size. It is clear that if $\sigma \in A_{s-1,m-2}$, then $(\sigma|\sigma|\sigma|\sigma) \in A_{s,m}$. Moreover, since σ_1 just cycles the four blocks of any codeword, and $\sigma_1(c) = c + \mathbf{3}$ for $c = (\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3})$, we have that $\sigma_1 \in A_{s,m}$. For $m > 2s+1$, the code is constructed using Matrix (1), so now we consider the coordinates as divided into two blocks. Since σ_2 cycles the blocks of any codeword, the above argument can also be used to prove this case.

Let X and Y be the groups $X = (A_{s-1,m-2}|A_{s-1,m-2}|A_{s-1,m-2}|A_{s-1,m-2})$ and $Y = (A_{s,m-1}|A_{s,m-1})$. Note that $X \cap \langle \sigma_1 \rangle = \{id\}$, since the permutations in $\langle \sigma_1 \rangle$ cycle blocks and the ones in X do not. For the same reason, $Y \cap \langle \sigma_2 \rangle = \{id\}$. Moreover, since $A_{s,m}$ is commutative by Lemma 2, $|\langle X, \sigma_1 \rangle| = |X||\langle \sigma_1 \rangle|$ and $|\langle Y, \sigma_2 \rangle| = |Y||\langle \sigma_2 \rangle|$. Note that σ_1 is of order four and σ_2 of order two. Then, by induction on m, it is easy to prove that the subgroups $\langle X, \sigma_1 \rangle \leq A_{s,m}$ and $\langle Y, \sigma_2 \rangle \leq A_{s,m}$ are both of order 2^{m-1}.

By induction on m, $A_{s,m}$ is transitive on the set of coordinates $\{1, 2, \ldots, n\}$: for $m = 1$, the group is trivial; assuming that $A_{s,m'}$ is transitive for all $1 \leq m' < m$, and using the fact that σ_1 and σ_2 cycle the blocks. Finally, since the group $A_{s,m}$ is commutative by Lemma 2, and transitive on $\{1,2,\ldots,n\}$, the stabilizer of every point is trivial. Therefore, the order of $A_{s,m}$ is $n = 2^{m-1}$. □

Corollary 1 *The subgroup $B_{s,m}$ has order 2^{m-s-1} and is generated by*

(i) $B_{0,1} = \{id\}$;

(ii) $B_{s,m} = \langle (B_{s-1,m-2}|B_{s-1,m-2}|B_{s-1,m-2}|B_{s-1,m-2}), \sigma_1^2\rangle$, *if* $m = 2s+1$;

(iii) $B_{s,m} = \langle (B_{s,m-1}|B_{s,m-1}), \sigma_2\rangle$, *if* $m > 2s+1$;

where $\sigma_1 = \prod_{i=1}^{n/4}(i, i+n/4, i+n/2, i+3n/4)$ *and* $\sigma_2 = \prod_{i=1}^{n/2}(i, i+n/2)$.

Proof By Lemma 2, $B_{s,m} \leq A_{s,m}$. Also note that the permutations in $A_{s,m}$ are of order $1, 2$ or 4; and the ones in $B_{s,m}$ are of order either 1 or 2. Moreover, it is not difficult to check that if $\sigma \in A_{s,m}$ and σ is of order 1 or 2, then $\sigma \in B_{s,m}$. Thus $|B_{s,m}| = 2^{m-2s-1}2^s = 2^{m-s-1}$. □

In order to describe some permutations of $P_{s,m}$, we will need the application $f_b(\tau) = \prod_{i=1}^{b}((t_1-1)b+i, (t_2-1)b+i)$ defined for any transposition $\tau = (t_1, t_2)$. For any permutation σ that can be expressed as a product of disjoint transpositions, $\sigma = \prod \tau_i$, we define $f_b(\sigma) = \prod f_b(\tau_i)$. Note that $f_b(\sigma)$ is a permutation similar to σ, but moving blocks of coordinates of length b. Moreover, if $\sigma \in S_{n/b}$, then $f_b(\sigma) \in S_n$

Lemma 4 *Let $P_{s,m}$ be the permutation automorphism group of the code $\mathcal{H}_{s,m}$ of length $n = 2^{m-1}$, where $m \geq 3$ and $1 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$. Then, $\pi_1, \pi_2 \in P_{s,m}$ if $m = 2s+1 \geq 5$, $\pi_3, \pi_4 \in P_{s,m}$ if $m > 2s+1$, and $\pi_5 \in P_{s,m}$ if $m > 2s+2$, where*

(i) $\pi_1 = (id|\sigma_3|\sigma_3^2|\sigma_3^3) \in S_n$ *with* $\sigma_3 = (p|p|\ldots|p) \in S_{n/4}$ *and* $p = (1,2,3,4) \in S_4$;

(ii) $\pi_2 = (q_{m-2}|q_{m-2}|q_{m-2}|q_{m-2}) \circ q_m \in S_n$ *with* $q_3 = id$, $q_m = f_{2^{m-5}}(q_5) \in S_n$ *and* $q_5 = (2,5)(3,9)(4,13)(7,10)(8,14)(12,15) \in S_{16}$;

(iii) $\pi_3 = (id|\sigma_4) \in S_n$ *with* $\sigma_4 = (p^2|p^2|\ldots|p^2) \in S_{n/2}$;

(iv) $\pi_4 = \prod_{i=1}^{n/4}(2i-1, 2i-1+n/2) \in S_n$;

(v) $\pi_5 = \prod_{i=1}^{n/4}(i, i+n/2) \in S_n$.

Proof

(i) By Lemma 3, since $p \in A_{1,3}$, $\sigma_3 \in A_{s-1,m-2}$. Thus, it is easy to see that π_1 fixes all the rows of $\mathcal{G}_{s,m}$ except v_2, and $\pi_1(v_2) = v_2 + 3v_\delta$. Therefore, $\pi_1 \in P_{s,m}$.

(ii) It is easy to check that $q_5 \in P_{2,5}$. Moreover, assuming that $q_{m-2} \in P_{s-1,m-2}$, we have that $(q_{m-2}|q_{m-2}|q_{m-2}|q_{m-2}) \in P_{s,m}$ by induction. The permutation q_m moves blocks of coordinates of length 2^{m-5}. Thus, it is easy to see that q_m fixes all the rows of $\mathcal{G}_{s,m}$ except $v_{\delta-1}$ and v_δ, $q_m(v_\delta) = v_{\delta-1}$, and $q_m(v_{\delta-1}) = v_\delta$. Therefore, $\pi_2 \in P_{s,m}$.

(iii) By Corollary 1, since $p^2 \in B_{1,3}$, $\sigma_4 \in B_{s,m-1}$. Moreover, since $m > 2s+1$, $\mathcal{G}_{s,m}$ is of the form given by (1). Applying the permutation π_3 to the rows of the form (w, w), we obtain either (w, w) or $(w, w + \mathbf{2})$, which are codewords.

(iv) Since $m > 2s+1$, $\mathcal{G}_{s,m}$ is of the form given by (1). The permutation π_4 fixes all the rows of $\mathcal{G}_{s,m}$, except $u_\gamma = (\mathbf{0}, \mathbf{2})$, since they are of the form (w, w). Moreover, $\pi_4(u_\gamma) = u_\gamma + 2v_2 + \mathbf{2}$ is a codeword.

(v) Since $m > 2s+2$, $\mathcal{G}_{s,m}$ is of the form given by (1) and $u_{\gamma-1} = (\mathbf{0}, \mathbf{2}, \mathbf{0}, \mathbf{2})$. The permutation π_5 fixes all the rows of $\mathcal{G}_{s,m}$, except $u_\gamma = (\mathbf{0}, \mathbf{2})$, since they are of the form (w, w). Moreover, $\pi_5(u_\gamma) = u_\gamma + u_{\gamma-1} + \mathbf{2}$ is a codeword.

□

The codewords of the quaternary linear Hadamard code $\mathcal{H}_{s,m}$ are partitioned into orbits under the action of its permutation automorphism group $P_{s,m}$. The next Propositions 1 and 2 give us a description of these orbits in terms of the codewords of type (a), (b) and (c) defined in Lemma 1.

Proposition 1 *The codewords of $\mathcal{H}_{s,m}$ of length $n = 2^{m-1}$, where $m \geq 3$ odd and $s = \frac{m-1}{2}$, are partitioned into the following orbits under the action of $P_{s,m}$:*

(i) four orbits of just one element, each containing one of the four codewords of type (a);

(ii) one orbit with the codewords of order two and type (b) with $2^{m-s} - 2$ elements; another orbit with the codewords of order four and type (b) with $2^{m-s} - 2$ elements;

(iii) one orbit with the codewords of type (c) with $2^{m+1} - 2^{m-s+1}$ elements.

Proof Note that codewords of different types or orders can not be in the same orbit, so there are at least 7 orbits by Lemma 1. Also note that, in this case, since $m = 2s+1$, the code $\mathcal{H}_{s,m}$ is of type $2^0 4^{s+1}$. Thus, there are not any rows of order two in the generator matrix $\mathcal{G}_{s,m}$. That is, all codewords of type (b) and order two are of the form $2v$ for some v of type (c). Equivalently, all codewords of type (b) and order four are of the form $2v + \mathbf{1}$ for some v of type (c). Therefore, since $2\sigma(v) = \sigma(2v)$ and $2\sigma(v) + \mathbf{1} = \sigma(2v + \mathbf{1})$ for any $\sigma \in S_n$ and any word v, it is enough to prove that all codewords of type (c) are in the same orbit.

Now, we prove that there is only one orbit of type (c), by induction on $m \geq 3$ odd. For $m = 3$, we can compute the group and see that the result is true. Assume that there are exactly 7 orbits (with only one orbit of type (c)) for $\mathcal{H}_{s-1,m-2}$. Note that $\mathcal{H}_{s,m} = \{(u, u, u, u),\ (u, u+\mathbf{1}, u+\mathbf{2}, u+\mathbf{3}),\ (u, u+\mathbf{2}, u, u+\mathbf{2}),\ (u, u+\mathbf{3}, u+\mathbf{2}, u+\mathbf{1}) : u \in \mathcal{H}_{s-1,m-2}\}$. Therefore, under the action of $(P_{s-1,m-2}|P_{s-1,m-2}|P_{s-1,m-2}|P_{s-1,m-2}) \leq P_{s,m}$, all codewords of $\mathcal{H}_{s,m}$ are partitioned into 28 orbits, 16 of them of type (c). We will show that the codewords in the 4 orbits coming from the orbit of type (c) in $\mathcal{H}_{s-1,m-2}$ are in the same orbit under the action of $P_{s,m}$. Note that the second row v_2 in $\mathcal{G}_{s,m}$ is in one of these 4 orbits of type (c). Moreover, using $\pi_1 = (id|\sigma_1|\sigma_1^2|\sigma_1^3) \in P_{s,m}$ as defined in Lemma 4, since $\sigma_1(v_2) = v_2 + \mathbf{3}$, we have that π_1, π_1^2 and π_1^3 move v_2 among these 4 orbits. On the other hand, the 12 remaining orbits of type (c) are of the form $(u, u+\mathbf{1}, u+\mathbf{2}, u+\mathbf{3})$ or $(u, u+\mathbf{3}, u+\mathbf{2}, u+\mathbf{1})$ with

$u \in \mathcal{H}_{s-1,m-2}$ of type (a) or (b). Let $x = (x_1, x_2, x_3, x_4, \ldots, x_n)$ be one of the codewords in these 12 orbits. Using $\pi_2 \in P_{s,m}$ defined in Lemma 4, we have that $\pi_2(x) = y$, where $y = (x_1, x_{\frac{n}{4}+1}, x_{\frac{2n}{4}+1}, x_{\frac{3n}{4}+1}, \ldots)$. By construction, $\{x_1, x_{\frac{n}{4}+1}, x_{\frac{2n}{4}+1}, x_{\frac{3n}{4}+1}\} = \{0,1,2,3\}$, so y belongs to one of the previous 4 orbits.

It is straightforward to obtain the number of codewords in every orbit by Lemma 1. □

Proposition 2 *The codewords of $\mathcal{H}_{s,m}$ of length $n = 2^{m-1}$, where $m \geq 3$ and $1 \leq s \leq \lfloor \frac{m-2}{2} \rfloor$, are partitioned into the following orbits under the action of $P_{s,m}$:*

(i) four orbits of just one element, each containing one of the four codewords of type (a);

(ii) one orbit with the codewords of type (b) and form $u = \sum_{i=1}^{\delta} \lambda_i v_i, \lambda_i \in \{0,2\}$ with $2^{s+1} - 2$ elements; another orbit with the codewords of type (b) and form $u + \mathbf{1}$ with $2^{s+1} - 2$ elements;

(iii) one orbit with the remaining codewords of order two and type (b) with $2^{m-s} - 2^{s+1}$ elements; another orbit with the remaining codewords of order four and type (b) with $2^{m-s} - 2^{s+1}$ elements;

(iv) one orbit with the codewords of type (c) with $2^{m+1} - 2^{m-s+1}$ elements.

Proof By Lemma 1, there are at least 7 orbits such that each one contains codewords of the same type and order. We will prove the statement by induction on m. Using also Proposition 1, we can assume that this is true for $\mathcal{H}_{s,m-1}$ for all $m > 2s+1$. Note that $\mathcal{H}_{s,m} = \{(u,u),\ (u, u+\mathbf{2}) : u \in \mathcal{H}_{s,m-1}\}$.

We start by proving point (iv). All codewords of type (c) in $\mathcal{H}_{s,m-1}$ are in the same orbit under the action of $P_{s,m-1}$. Thus, under the action of $(P_{s,m-1}|P_{s,m-1}) \leq P_{s,m}$, there are 2 orbits with codewords of type (c) in $\mathcal{H}_{s,m}$, $\{(u,u) : u \in \mathcal{H}_{s,m-1}$ of type (c)$\}$ and $\{(u, u+\mathbf{2}) : u \in \mathcal{H}_{s,m-1}$ of type (c)$\}$. Using $\pi_3 = (id|\sigma_4) \in P_{s,m}$ defined in Lemma 4, since $\sigma_4(v_2) = v_2 + \mathbf{2}$, we have that $\pi_3(v_2, v_2) = (v_2, v_2 + \mathbf{2})$. Therefore, all codewords of type (c) in $\mathcal{H}_{s,m}$ are in the same orbit.

For points (ii) and (iii), we just need to prove that there are exactly 2 orbits with all codewords of order two and type (b). Since all codewords of order two and form $u = \sum_{i=1}^{\delta} \lambda_i v_i, \lambda_i \in \{0,2\}$, are constructed from codewords of type (c), clearly they belong to the same orbit. For the remaining codewords of order two and type (b), we need to distinguish two cases.

If $m = 2s+2$, all codewords of order two and type (b) in $\mathcal{H}_{s,m-1}$ are in one orbit under the action of $P_{s,m-1}$. Thus, under the action of $(P_{s,m-1}|P_{s,m-1})$, there are 4 orbits with codewords of order two and type (b) in $\mathcal{H}_{s,m}$: two of the forms $(2v, 2v)$ and $(2v, 2v+\mathbf{2})$, and two with the codewords $(\mathbf{0}, \mathbf{2})$ and $(\mathbf{2}, \mathbf{0})$. The one with codewords of the form $(2v, 2v)$ gives the orbit of point (ii). Using $\pi_4 \in P_{s,m}$ as defined in Lemma 4, it is easy to see that all codewords in the other 3 orbits are in the same orbit under the action of $P_{s,m}$. Note that $\pi_4(\mathbf{0}, \mathbf{2}) = (2v', 2v'+\mathbf{2})$ and $\pi_4(\mathbf{2}, \mathbf{0}) = (2v'', 2v''+\mathbf{2})$ for some $v', v'' \in \mathcal{H}_{s,m-1}$.

On the other hand, if $m > 2s+2$, the orbits from points (ii) and (iii) in $\mathcal{H}_{s,m-1}$ are not empty. Therefore, under the action of $(P_{s,m-1}|P_{s,m-1})$, there are 6 orbits with codewords of order two and type (b) in $\mathcal{H}_{s,m}$: four of the forms $(2v, 2v)$, $(2v, 2v+\mathbf{2})$, (u, u) and $(u, u+\mathbf{2})$, where $2v$ and u are from orbits (ii) and (iii), respectively; and two with the codewords $(\mathbf{0}, \mathbf{2})$ and $(\mathbf{2}, \mathbf{0})$. The one with codewords of the form $(2v, 2v)$ gives the orbit of point (ii). Now, we will see that the codewords in the other 5 orbits are in the same orbit under the action of $P_{s,m}$. Using $\pi_5 \in P_{s,m}$ as defined in Lemma 4, it is easy to check that $\pi_5(\mathbf{0}, \mathbf{2}) = (\mathbf{2}, \mathbf{0}, \mathbf{0}, \mathbf{2})$ and $\pi_5(\mathbf{2}, \mathbf{0}) = (\mathbf{0}, \mathbf{2}, \mathbf{2}, \mathbf{0})$, which are of the form $(u, u+\mathbf{2})$. We can also see that $\pi_5(2v, 2v+\mathbf{2}) = (2v, 2v) + (\mathbf{2}, \mathbf{0}, \mathbf{0}, \mathbf{2}) = (2v, 2v) + (\mathbf{2}, \mathbf{0}, \mathbf{2}, \mathbf{0}) + (\mathbf{0}, \mathbf{0}, \mathbf{2}, \mathbf{2})$, which is also of the form $(u, u+\mathbf{2})$. Taking σ_2 from Corollary 1, it is easy to see that $(id|\sigma_2) \in (id|B_{s,m-1}) \leq P_{s,m}$ and $(id|\sigma_2)(\mathbf{0}, \mathbf{2}, \mathbf{0}, \mathbf{2}) = (\mathbf{0}, \mathbf{2}, \mathbf{2}, \mathbf{0})$, which is again of the form $(u, u+\mathbf{2})$.

We will see that the previous 2 orbits can not be joined. Suppose that there is $\tau \in P_{s,m}$ such that $u^{(iii)} = \tau(u^{(ii)})$, where $u^{(ii)}$ is in the orbit of point (ii) and $u^{(iii)}$ is in the orbit of point (iii). Then, there is $v^{(ii)}$ of type (c) such that $u^{(ii)} = 2v^{(ii)}$. Since $\tau(v^{(ii)})$ must be of type (c), and $u^{(iii)} = 2\tau(v^{(ii)})$, we have that $u^{(iii)}$ is in the orbit of point (ii). This gives us a contradiction, so there are exactly 2 orbits.

It is straightforward to count the number of codewords in every orbit by Lemma 1. □

Theorem 1 *Let $\mathcal{H}_{s,m}$ be the quaternary linear Hadamard code of length $n = 2^{m-1}$, where $m \geq 1$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$. The order of the permutation automorphism group $P_{s,m} = \mathrm{PAut}(\mathcal{H}_{s,m})$ is*

(i) $|P_{0,1}| = 1$;
(ii) $|P_{s,m}| = |P_{s-1,m-2}| \cdot 4^{s-1} \cdot (2^{2s+2} - 2^{s+2})$, *if* $m = 2s+1$, $s \geq 1$;
(iii) $|P_{s,m}| = |P_{s,m-1}| \cdot 2^{m-s-2} \cdot (2^{m-s} - 2^{s+1})$, *if* $m > 2s+1$, $s \geq 0$.

Proof The code $\mathcal{H}_{0,1}$ is of length 1, so $P_{0,1} = \{id\}$.

For $m > 2s+1$, the generator matrix $\mathcal{G}_{s,m}$ is given by (1), so $\mathcal{H}_{s,m} = \{(u, u),\ (u, u+\mathbf{2}) : u \in \mathcal{H}_{s,m-1}\}$. By the orbit-stabilizer theorem, $|P_{s,m}| = |P_{s,m}(u_\gamma)||N_{s,m}^{u_\gamma}|$, where $u_\gamma = (\mathbf{0}, \mathbf{2})$. By Proposition 2 (iii), the size of the orbit that contains u_γ is $|P_{s,m}(u_\gamma)| = 2^{m-s} - 2^{s+1}$. The permutations in the stabilizer of u_γ must be of the form $(\varsigma_1|\varsigma_2)$, where $\varsigma_1, \varsigma_2 \in P_{s,m-1}$. If $\varsigma_1 = \varsigma_2$, we have that $(P_{s,m-1}|P_{s,m-1}) \leq N_{s,m}^{u_\gamma}$. If $\varsigma_1 \neq \varsigma_2$, we also have that the permutations of the form $(id|\varsigma_2 \circ \varsigma_1^{-1})$ belongs to $N_{s,m}^{u_\gamma}$, because $(\varsigma_1^{-1}|\varsigma_1^{-1}) \in N_{s,m}^{u_\gamma}$. Since the codewords of $\mathcal{H}_{s,m}$ are of the form (u, u) or $(u, u+\mathbf{2})$, where $u \in \mathcal{H}_{s,m-1}$, $\varsigma_2 \circ \varsigma_1^{-1}$ belongs to $B_{s,m-1}$. Thus, $N_{s,m}^{u_\gamma} = \langle (P_{s,m-1}|P_{s,m-1}), (id|B_{s,m-1}) \rangle$. Since $B_{s,m-1} \trianglelefteq P_{s,m-1}$ by Lemma 2, then $(P_{s,m-1}|P_{s,m-1})$ and $(id|B_{s,m-1})$ commute. Moreover, it is clear that $(P_{s,m-1}|P_{s,m-1}) \cap (id|B_{s,m-1}) = \{id\}$. Therefore, $|N_{s,m}^{u_\gamma}| = |\langle (P_{s,m-1}|P_{s,m-1}), (id|B_{s,m-1}) \rangle| = |P_{s,m-1}||B_{s,m-1}|$. The result follows, since $|B_{s,m-1}| = 2^{m-s-2}$ by Corollary 1.

For $m = 2s+1$, the generator matrix $\mathcal{G}_{s,m}$ is given by (2), so $\mathcal{H}_{s,m} = \{(u, u, u, u),\ (u, u+\mathbf{1}, u+\mathbf{2}, u+\mathbf{3}),\ (u, u+\mathbf{2}, u, u+\mathbf{2}),\ (u, u+\mathbf{3}, u+\mathbf{2}, u+\mathbf{1}) : u \in \mathcal{H}_{s-1,m-2}\}$. By the orbit-stabilizer theorem, $|P_{s,m}| = |P_{s,m}(v_\delta)||N_{s,m}^{v_\delta}|$, where

Table 1 Order of $P_{s,m} = \mathrm{PAut}(\mathcal{H}_{s,m})$ for $1 \leq m \leq 8$.

s \ m	1	2	3	4	5	6	7	8
0	1	2	$2^3 \cdot 3$	$2^6 \cdot 3 \cdot 7$	$2^{10} \cdot 3 \cdot 7 \cdot 15$	$\dots$	$\dots$	$\dots$
1			2^3	2^6	$2^{10} \cdot 3$	$2^{15} \cdot 3 \cdot 7$	$2^{21} \cdot 3 \cdot 7 \cdot 15$	$\dots$
2					$2^9 \cdot 3$	$2^{14} \cdot 3$	$2^{20} \cdot 3^2$	$2^{27} \cdot 3^2 \cdot 7$
3							$2^{18} \cdot 3 \cdot 7$	$2^{25} \cdot 3 \cdot 7$

$v_\delta = (\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3})$. By Proposition 1 (iii), the size of the orbit that contains v_δ is $|P_{s,m}(v_\delta)| = 2^{2s+2} - 2^{s+2}$. Using the same technique as in the case $m > 2s+1$, we have that $(P_{s-1,m-2}|P_{s-1,m-2}|P_{s-1,m-2}|P_{s-1,m-2}) \leq N^{v_\delta}_{s,m}$, and the rest of permutations in $N^{v_\delta}_{s,m}$ are of the form $(id|\varsigma_1|\varsigma_2|\varsigma_3)$, where $\varsigma_1, \varsigma_2, \varsigma_3 \in P_{s-1,m-2}$. Since these permutations $(id|\varsigma_1|\varsigma_2|\varsigma_3)$ applied to any codeword must maintain any of the four possible forms described before, $\varsigma_1, \varsigma_3 \in A_{s-1,m-2}$. Moreover, $\varsigma_1(\varsigma_3(v)) = v$ for all $v \in \mathcal{H}_{s-1,m-2}$. That is, $\varsigma_1 \circ \varsigma_3 \in N^v_{s-1,m-2}$ for all $v \in \mathcal{H}_{s-1,m-2}$. It is not difficult to see that the intersection of all stabilizers is $\{id\}$. Then, $\varsigma_3 = \varsigma_1^{-1} = \varsigma_1^3$. Equivalently, $\varsigma_2 = \varsigma_1^{-2} = \varsigma_1^2$. Therefore, $N^{v_\delta}_{s,m} = \langle (P_{s-1,m-2}|P_{s-1,m-2}|P_{s-1,m-2}|P_{s-1,m-2}), (id|A_{s-1,m-2}|A^2_{s-1,m-2}|A^3_{s-1,m-2}) \rangle$. Finally, using again the same arguments as in the case $m > 2s+1$, $|N^{v_\delta}_{s,m}| = |P_{s-1,m-2}||A_{s-1,m-2}| = |P_{s-1,m-2}|2^{m-3} = |P_{s-1,m-2}|4^{s-1}$, by Lemma 2 and Proposition 3. □

Corollary 2 *Let $\mathcal{H}_{s,m}$ be the quaternary linear Hadamard code of length $n = 2^{m-1}$, where $m \geq 1$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$. The order of the permutation automorphism group $P_{s,m} = \mathrm{PAut}(\mathcal{H}_{s,m})$ is*

(i) $|P_{0,1}| = 1$;
(ii) $|P_{s,m}| = \prod_{i=1}^{s} 2^{3i}(2^i - 1)$, *if* $m = 2s+1$, $s \geq 1$;
(iii) $|P_{s,m}| = |P_{s,2s+1}| \prod_{i=2s+2}^{m} 2^{i-1}(2^{i-2s-1} - 1)$, *if* $m > 2s+1$, $s \geq 0$.

Theorem 2 *Let $\mathcal{H}_{s,m}$ be the quaternary linear Hadamard code of length $n = 2^{m-1}$, where $m \geq 3$ and $1 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$. The permutation automorphism group $P_{s,m} = \mathrm{PAut}(\mathcal{H}_{s,m})$ is generated by*

(i) $P_{1,3} = \langle (2,4), (1,2)(3,4) \rangle$;
(ii) $P_{s,m} = \langle (P_{s-1,m-2}|P_{s-1,m-2}|P_{s-1,m-2}|P_{s-1,m-2}),$
$(id|A_{s-1,m-2}|A^2_{s-1,m-2}|A^3_{s-1,m-2}), \pi_2 \rangle$, *if* $m = 2s+1$, $s \geq 2$;
(iii) $P_{s,m} = \langle (P_{s,m-1}|P_{s,m-1}), (id|B_{s,m-1}), \pi_4 \rangle$, *if* $m = 2s+2$, $s \geq 1$;
(iv) $P_{s,m} = \langle (P_{s,m-1}|P_{s,m-1}), (id|B_{s,m-1}), \pi_5 \rangle$, *if* $m > 2s+2$, $s \geq 1$;

where π_2, π_4, π_5 are defined in Lemma 4.

Proof The same proof applies to all of the cases. By the proof of Theorem 1, note that without the permutations π_2, π_4 and π_5, we obtain the stabilizer of the row $u_\gamma = (\mathbf{0}, \mathbf{2})$ or $v_\delta = (\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3})$. By Propositions 1 and 2, π_2, π_4 and π_5, are the permutations needed to obtain all of the orbits. □

The next proposition gives another characterization of $P_{s,m}$ in terms of the codewords of type (c).

Proposition 3 *Let $\mathcal{H}_{s,m}$ be the quaternary linear Hadamard code of length $n = 2^{m-1}$, where $m \geq 3$ and $1 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$. The permutation automorphism group of the codewords of type (c) is $P_{s,m}$.*

Proof Let $P'_{s,m}$ be the permutation automorphism group of the codewords of type (c). Since $s \geq 1$, the row $v_2 \in \mathcal{G}_{s,m}$, and the set of codewords of type (c) is not empty. It is clear that $P_{s,m} \subseteq P'_{s,m}$. In order to prove that $P'_{s,m} \subseteq P_{s,m}$, we take any $\tau \in P'_{s,m}$. We have that $\tau(v_1) \in \mathcal{H}_{s,m}$. Moreover, the rows $v_i \in \mathcal{G}_{s,m}$ for all $i \in \{2, \ldots, \delta\}$ are of type (c), thus $\tau(v_i) \in \mathcal{H}_{s,m}$. As for the rows $u_j \in \mathcal{G}_{s,m}$ for all $j \in \{1, \ldots, \gamma\}$, since $u_j + v_2$ is a codeword of type (c), then $\tau(u_j + v_2) \in \mathcal{H}_{s,m}$. Therefore, $\tau(u_j) = \tau(u_j + v_2) - \tau(v_2) \in \mathcal{H}_{s,m}$. □

Given a quaternary linear code $\mathcal{C}$ of length $n = 2^m$, the *inner product* for any two words $u, v \in \mathbb{Z}_4^n$ is defined as: $\langle u, v \rangle = \sum_{i=1}^{n} u_i v_i \in \mathbb{Z}_4$, and the *quaternary dual code* of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined in the usual way as:

$$\mathcal{C}^\perp = \{u \in \mathbb{Z}_4^n \;:\; \langle u, v \rangle = 0 \text{ for all } v \in \mathcal{C}\}.$$

Corollary 3 *Let $\mathcal{H}_{s,m}$ be the quaternary linear Hadamard code of length $n = 2^{m-1}$, where $m \geq 1$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$. Let $\mathcal{E}_{s,m} = \mathcal{H}_{s,m}^\perp$ be its quaternary dual code, which is a quaternary linear extended 1-perfect code. Then,* $\mathrm{PAut}(\mathcal{H}_{s,m}) = \mathrm{PAut}(\mathcal{E}_{s,m})$.

Proof We observe that for any quaternary linear code $\mathcal{C}$, thus $\mathrm{PAut}(\mathcal{C}) = \mathrm{PAut}(\mathcal{C}^\perp)$.

4 Conclusions

Several problems related to quaternary codes can be addressed by computing the automorphism group of these codes. In this paper, the order of the permutation automorphism group $\mathrm{PAut}(\mathcal{H}_{s,m})$ of a family of quaternary linear Hadamard codes $\mathcal{H}_{s,m}$ and their duals (quaternary linear extended 1-perfect codes) is computed. The groups are completely characterized by providing their generators and also by computing their action on $\mathcal{H}_{s,m}$

Given any monomial matrix M (with nonzero entries 1 and 3), we can obtain another code $\mathcal{H}_{s,m} \cdot M$, which is monomially equivalent to $\mathcal{H}_{s,m}$. In a further work, we will study the permutation automorphism groups of these equivalent codes, as well as the monomial automorphism group $\mathrm{MAut}(\mathcal{H}_{s,m})$ of $\mathcal{H}_{s,m}$. Recall that the monomial automorphism group $\mathrm{MAut}(\mathcal{C})$ of $\mathcal{C}$ is the set of all monomial matrices M such that $\mathcal{C}M = \mathcal{C}$. It would also be interesting to generalize these results to all quaternary linear Reed Muller codes $\mathcal{RM}_s(r, m)$, $m \geq 1$, $0 \leq r \leq m$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$ [3].

References

1. J. Pernas, J. Pujol, and F. I. M. Villanueva, "On the Permutation Automorphism Group of Quaternary Linear Hadamard Codes," in *3rd International Castle Meeting on Coding Theory and Applications*, Cardona, Spain, Sep. 2011, pp. 213–218.
2. J. Pujol, J. Rifà, and F. I. Solov'eva, "Quaternary Plotkin constructions and quaternary Reed-Muller codes," in *Proc. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, ser. LNCS, vol. 4851, India, Dec. 2007, pp. 148–157.
3. J. Pujol, J. Rifà, and F. I. Solo'eva, "Construction of $\mathbb{Z}_4$-linear Reed-Muller codes," *Trans. Inf. Theory*, vol. 55, no. 1, pp. 99–104, 2009.
4. D. S. Krotov, "$\mathbb{Z}_4$-linear Hadamard and extended perfect codes," in *Proc. Int. Workshop on Coding and Cryptography*, Paris, France, Jan. 2001, pp. 329–334.
5. J. Pernas, J. Pujol, and M. Villanueva, "Classification of some families of quaternary Reed-Muller codes," *Trans. Inf. Theory*, vol. 57, no. 9, pp. 6043–6051, 2011.
6. K. T. Phelps and J. Rifà, "On binary 1-perfect additive codes: some structural properties," *Trans. Inf. Theory*, vol. 48, no. 9, pp. 2087–2592, 2002.
7. D. S. Krotov, "On the Automorphism Groups of the Additive 1-Perfect Binary Codes," in *3rd International Castle Meeting on Coding Theory and Applications*, Cardona, Spain, Sep. 2011, pp. 171–176.
8. O. Heden, F. Pasticci, and T. Westerbäck, "On the existance of extended perfect binary codes with trivial symmetry group," *Advances in Mathematics of Communications*, vol. 3, no. 3, pp. 295–309, 2009.
9. O. Heden, "On the symmetry group of perfect 1-error correcting binary codes," *J. Combin. Math. Combin. Comput.*, vol. 52, pp. 109–115, 2005.
10. S. V. Avgustinovich, F. I. Solov'eva, and O. Heden, "On the structure of symmetry groups of vasil'ev codes," *Advances in Mathematics of Communications*, vol. 41, no. 2, pp. 105–112, 2005.
11. C. Fernández-Córdoba, K. Phelps, and M. Villanueva, "Involutions in binary perfect codes," *Trans. Inf. Theory*, vol. 57, no. 9, pp. 5926–5931, 2011.
12. P. J. Cameron, *Permutation Groups.* Cambridge Univ. Press, 1999.
13. T. Feulner, "The automorphism groups of linear codes and canonical representatives of their semilinear isometry classes," *Advances in Mathematics of Communications*, vol. 4, no. 3, pp. 363–383, 2009.
14. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes: Vol.: 1* . North-Holland Publishing Company, 1977.

Jaume Pernas Vallès

Bellaterra, Maig de 2012