About the $\mathbb{Z}_4$-linear Reed-Muller $\mathcal{ZRM}^-(r, m-1)$ and $\mathcal{RM}_s(r, m)$ codes*

J. Rifà[1] and L. Ronquillo[1]

[1] Dept. of Information and Communications Engineering, Universitat Autònoma de Barcelona, Spain ({josep.rifa,lorena.ronquillo}@autonoma.edu).

Abstract. Several different families of quaternary codes related to Reed-Muller binary linear codes can be found in the literature. Two definitions of such families are denoted as $\mathcal{ZRM}^-(r, m)$ and $\{\mathcal{RM}_s(r, m)\}$. In the current paper $\mathcal{ZRM}^-(r, m-1)$ and $\{\mathcal{RM}_s(r, m)\}$ codes are shown to be equal exactly for $s = 0$ $(0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor)$. Therefore, for the above-mentioned value of s, $\mathbb{Z}_4$-linear Reed-Muller codes with the same parameters and properties as the usual binary linear Reed-Muller code are obtained with both definitions.

Key words: Plotkin construction, Reed-Muller codes, $\mathbb{Z}_4$-linear codes.

1 Introduction

The concept of $\mathbb{Z}_4$-linearity of binary codes was pioneered by Nechaev in [10]. This result opened up a new direction in Coding Theory. It basically stated that certain non-linear binary codes, for instance Kerdock codes, can be derived from linear codes over the ring $\mathbb{Z}_4$.

In a later work, Hammons, Kumar, Calderbank, Sloane and Solé [6], defined two families of quaternary codes called $\mathcal{QRM}(r, m)$ and $\mathcal{ZRM}(r, m)$ codes. Moreover, in respect of the usual binary linear Reed-Muller codes $RM(r, m)$, they conjectured their $\mathbb{Z}_4$-linearity for $r \in \{0, 1, 2, m-1, m\}$, but not for $3 \leq r \leq m-2$ (whenever $m \geq 5$). They proved it for $r = m-2$ but the remain values of r were not validated until the work of Hou, Lahtonen and Koponen [7].

Zhe-Xian Wan also defined $\mathcal{ZRM}(r, m)$ codes with the aim of reviewing the codes first defined in [6]. However, in [2] it is proved that they happened to be a different definition of quaternary Reed-Muller codes, which from now on will be denoted as $\mathcal{ZRM}^-(r, m)$. In fact, as stated in [2], $\mathcal{ZRM}(r, m)$ and $\mathcal{ZRM}^-(r, m)$ just coincide for the above-named values of $r \in \{0, 1, 2, m-1, m\}$ that make their corresponding binary images to be Reed-Muller codes.

* This work has been partially supported by the Spanish MEC and the European FEDER Grants MTM2006-03250 and TSI2006-14005-C02-01.

Codes $\mathcal{QRM}(r,m)$ are such that the binary linear Reed-Muller codes $RM(r,m)$ are obtained after computing, for each r, $0 \leq r \leq m$, the modulo two instead of the Gray map. These codes were further generalized in [1], where it is defined a class $\overline{\mathcal{QRM}}(r,m)$ of quaternary codes that includes $\mathcal{QRM}(r,m)$.

Just as binary Reed-Muller codes can be built by means of the Plotkin construction [9], in [12] quaternary Plotkin constructions are introduced to build new families of quaternary Reed-Muller codes, denoted as $\{\mathcal{RM}_s(r,m)\}$. These families were constructed in such a way that the corresponding $\mathbb{Z}_4$-linear codes, obtained under the Gray map, are binary codes which have the same parameters and properties as the binary linear Reed-Muller codes $RM(r,m)$.

Comparing the above-named definitions of $\mathcal{ZRM}^-(r,m)$ and $\{\mathcal{RM}_s(r,m)\}$ families of codes, we found that, actually, the families $\{\mathcal{RM}_s(r,m)\}$ can be seen as a generalization of $\mathcal{ZRM}^-(r,m-1)$, since this last one coincides with the specific family $s=0$, that is with $\mathcal{RM}_0(r,m)$.

This paper has been organized as follows: in Section 2 some basic definitions and notation, which will be needed in the remainder of the paper, are given. In Section 3 some properties of binary Reed-Muller codes are reviewed whereas Section 4 is focused on quaternary Reed-Muller codes. Section 4.1 reviews the definition and construction of $\mathcal{ZRM}^-(r,m)$ codes introduced by [13], and Section 4.2 is devoted to $\{\mathcal{RM}_s(r,m)\}$ families of codes, from [12]. In Section 5 the equality between the $\mathcal{ZRM}^-(r,m-1)$ and $\{\mathcal{RM}_0(r,m)\}$ families is established and proved. Finally, some conclusions are drawn in Section 6 and future lines of research are given in Section 7.

2 Definitions

Let $\mathbb{Z}_2$ and $\mathbb{Z}_4$ be the ring of integers modulo two and modulo four, respectively. Let $\mathbb{Z}_2^n$ denote the set of all n-length vectors over $\mathbb{Z}_2$ and $\mathbb{Z}_4^N$ be the set of all N-length vectors over $\mathbb{Z}_4$. Any non-empty subset C of $\mathbb{Z}_2^n$ is a *binary code* and, moreover, a subgroup of $\mathbb{Z}_2^n$ is called a *binary linear code*. Equivalently, any non-empty subset $\mathcal{C}$ of $\mathbb{Z}_4^n$ is a *quaternary code* which is also called *quaternary linear code* if it is a subgroup of $\mathbb{Z}_4^n$. In general, any non-empty subgroup $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is a $\mathbb{Z}_2\mathbb{Z}_4$-*additive code*.
We will denote by $\mathbf{0}$, $\mathbf{1}$ and $\mathbf{2}$ the all-zeroes, the all-ones and the all-twos vectors, respectively. It will be clear by the context whether we refer to binary vectors $\mathbf{0}$, $\mathbf{1}$ or to quaternary vectors.

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

In the case of quaternary codes the Lee metric is used, which, actually, coincides with the Hamming weight in $\mathbb{Z}_2$. However, the elements of $\mathbb{Z}_4$ have the following Lee weights: $w_L(0) = 0$, $w_L(1) = w_L(3) = 1$ and $w_L(2) = 2$. The *Lee weight* of a vector $\mathbf{u} \in \mathbb{Z}_4^N$ is the addition of the weights of its coordinates. The *Lee distance* $d_L(\mathbf{u}, \mathbf{v})$ between two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_4^N$ is defined as $d_L(\mathbf{u}, \mathbf{v}) = w_L(\mathbf{u} - \mathbf{v})$.

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code and let C be the code obtained from $\Phi(\mathcal{C})$, where $\Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \longrightarrow \mathbb{Z}_2^{\alpha+2\beta}$ is given by the map $\Phi(u_1, \ldots, u_\alpha | v_1, \ldots, v_\beta) = (u_1, \ldots, u_\alpha | \phi(v_1), \ldots, \phi(v_\beta))$ where $\phi(0) = (0, 0)$, $\phi(1) = (0, 1)$, $\phi(2) = (1, 1)$ and $\phi(3) = (1, 0)$ are the usual Gray map from $\mathbb{Z}_4$ onto $\mathbb{Z}_2^2$. Now, it is clear that

$$\mathbf{u} + \mathbf{v} = \Phi(\Phi^{-1}(\mathbf{u}) + \Phi^{-1}(\mathbf{v})),\ \forall \mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^n.$$

Hamming and Lee weights (or distances) of a vector in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ can be computed by adding the corresponding weights (or distances) of the α coordinates and β coordinates. It is known that Gray map is a distance preserving mapping, specifically, the Hamming distance of a binary code C coincides with the Lee distance computed in the additive code $\mathcal{C} = \Phi^{-1}(C)$ where it comes from. Hence, Hamming distance will be used in binary codes whereas Lee distance will be used in additive codes.

Since a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, it is also isomorphic to an abelian structure like $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, $\mathcal{C}$ has $|\mathcal{C}| = 2^\gamma 4^\delta$ codewords and, moreover, $2^{\gamma+\delta}$ of them have order two. This code $\mathcal{C}$ is called a $\mathbb{Z}_2\mathbb{Z}_4$-*additive code of type* $(\alpha, \beta; \gamma, \delta)$ and its binary image $C = \Phi(\mathcal{C})$ is a $\mathbb{Z}_2\mathbb{Z}_4$-*linear code of type* $(\alpha, \beta; \gamma, \delta)$.
A $\mathbb{Z}_2\mathbb{Z}_4$-additive code with $\alpha = 0$ is a quaternary linear code and its corresponding binary image is called a $\mathbb{Z}_4$-*linear code*, whereas a $\mathbb{Z}_2\mathbb{Z}_4$-additive code with $\beta = 0$ is a binary code. Hence, $\mathbb{Z}_2\mathbb{Z}_4$-additive codes could be considered as a generalization of binary linear codes and $\mathbb{Z}_4$-linear codes.

A generator matrix of size $(\gamma + \delta) \times (\alpha + \beta)$ for a $\mathbb{Z}_2\mathbb{Z}_4$-additive code is of the form

$$\mathcal{G} = \left(\begin{array}{c|c} B_2 & Q_2 \\ \hline B_1 & Q_1 \end{array}\right)$$

where B_2 and B_1 are binary matrices of size $\gamma \times \alpha$ and $\delta \times \alpha$, respectively; Q_2 is a $\gamma \times \beta$-quaternary matrix which contains order two row vectors; and Q_1 is a $\delta \times \beta$-quaternary matrix with order four row vectors.

Two $\mathbb{Z}_2\mathbb{Z}_4$-additive codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are *monomially equivalent* if one can be obtained from the other by permuting the coordinates and, if necessary, changing the sign of certain quaternary coordinates. If these $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, $\mathcal{C}_1$ and $\mathcal{C}_2$, differ just in one permutation of coordinates, then they are *permutation equivalent*.

Let C be a subset of a linear space, $\langle C \rangle$ denotes the linear subspace spanned by C.

The *standard inner product* of any two vectors $\mathbf{u}$, $\mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is defined as:

$$\mathbf{u} \cdot \mathbf{v} = 2(\sum_{i=1}^{\alpha} u_i v_i) + \sum_{j=\alpha+1}^{\alpha+\beta} u_j v_j \ \in \ \mathbb{Z}_4.$$

The $\mathbb{Z}_2\mathbb{Z}_4$-*additive dual code* of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is the set of vectors which are orthogonal to all codewords of $\mathcal{C}$, i.e.,

$$\mathcal{C}^\perp = \{\mathbf{u} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \mid \mathbf{u}\cdot\mathbf{v} = 0, \quad \text{for all } \mathbf{v} \in \mathcal{C}\}.$$

The $\mathbb{Z}_2\mathbb{Z}_4$-additive dual code $\mathcal{C}^\perp$ obtained by the inner product is also an additive code. Its weight enumerator is related to the weight enumerator of $\mathcal{C}$ by the MacWilliams identity. The corresponding binary code $\Phi(\mathcal{C}^\perp)$ is denoted by $C_\perp$ and it is called $\mathbb{Z}_2\mathbb{Z}_4$-*dual code* of C. When $\alpha = 0$, the code $\mathcal{C}^\perp$ is also called the *quaternary dual code* of $\mathcal{C}$ whereas $C_\perp$ is the $\mathbb{Z}_4$-*dual code* of C. Furthermore, note that C and $C_\perp$ are formal duals since they are not necessarily dual in the binary linear sense but the weight enumerator polynomial of $C_\perp$ is the MacWilliams transform of the weight enumerator polynomial of C.

Henceforward, we focus our attention specifically to $\mathbb{Z}_2\mathbb{Z}_4$-additive codes with $\alpha = 0$, i.e. quaternary linear codes such that, under the Gray map, they give rise to $\mathbb{Z}_4$-linear codes. We will denote their type as $(N; \gamma, \delta)$, whenever $\alpha = 0$ and $\beta = N$.

In [12] two constructions of quaternary linear codes are defined. The most important of them for the current paper is the Plotkin construction [9], which was generalized to quaternary linear codes.

Let $\mathcal{A}$ and $\mathcal{B}$ be two quaternary linear codes of types $(N; \gamma_A, \delta_A)$ and $(N; \gamma_B, \delta_B)$ and minimum distances d_A and d_B, respectively. The *quaternary Plotkin construction* defines a new quaternary linear code in terms of the above-named codes as follows

$$\mathcal{PC}(\mathcal{A}, \mathcal{B}) = \{(\mathbf{u}_1|\mathbf{u}_1 + \mathbf{u}_2) : \mathbf{u}_1 \in \mathcal{A}, \mathbf{u}_2 \in \mathcal{B}\},$$

where "|" denotes concatenation. For additive codes, the above construction can also be defined in terms of generator matrices. Let $\mathcal{G}_\mathcal{A}$ and $\mathcal{G}_\mathcal{B}$ be the generator matrices of $\mathcal{A}$ and $\mathcal{B}$, respectively. Then, the code $\mathcal{PC}(\mathcal{A}, \mathcal{B})$ has the following generator matrix:

$$\mathcal{G}_{PC} = \begin{pmatrix} \mathcal{G}_\mathcal{A} & \mathcal{G}_\mathcal{A} \\ 0 & \mathcal{G}_\mathcal{B} \end{pmatrix}. \tag{1}$$

As proved in [12], the obtained quaternary linear code $\mathcal{PC}(\mathcal{A}, \mathcal{B})$ is of type $(2N; \gamma, \delta)$, where $\gamma = \gamma_\mathcal{A} + \gamma_\mathcal{B}$ and $\delta = \delta_\mathcal{A} + \delta_\mathcal{B}$; the binary length is $n = 4N$; the size is $2^{\gamma+2\delta}$ and the minimum distance is $d = min\{2d_\mathcal{A}, d_\mathcal{B}\}$.

3 Reed-Muller codes

As it is shown in [9], a binary linear rth-order Reed-Muller code $RM(r+1, m+1)$ with $0 \leq r \leq m$ and $m \geq 1$ can be described using the Plotkin construction in terms of $RM(r+1, m)$ and $RM(r, m)$ as

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

where $RM(0, m)$ is the repetition code $\{\mathbf{0}, \mathbf{1}\}$ and "|" denotes concatenation. There is an equivalent statement in terms of generator matrices. Let $G(r, m)$ be a generator matrix of $RM(r, m)$, then

$$G(r+1, m+1) = \begin{pmatrix} G(r+1, m) & G(r+1, m) \\ 0 & G(r, m) \end{pmatrix}, \tag{2}$$

where $G(0, m) = (\mathbf{1})$.

As it can be noted, a previous sequence $RM(r, m)$ is needed to obtain a new sequence $RM(r, m+1)$ by means of the Plotkin construction. We can start the construction of the different families $\{RM(r, m)\}$ by using the sequence $\{RM(-1, 2), RM(0, 2), RM(1, 2), RM(2, 2)\}$, where $RM(-1, 2)$ is the code with only a zero vector, $RM(0, 2)$ is the code $\{\mathbf{0}, \mathbf{1}\}$, $RM(1, 2)$ is the even code of binary length four and $RM(2, 2)$ is the full space $\mathbb{Z}_2^{2^2}$. After doing the Plotkin construction in the family $\{RM(r, m)\}$, new codes $RM(-1, m+1) = \{\mathbf{0}\}$ and $RM(m+1, m+1) = \mathbb{Z}_2^{2^{m+1}}$ need to be added to the obtained family.

Theorem 1 *[9] The rth-order binary Reed-Muller code $RM(r, m)$ of length 2^m, $0 \leq r \leq m$, $m \geq 1$, has the following properties:*

- *The dimension of the code is $k = \sum_{i=0}^{r} \binom{m}{i}$.*
- *The minimum distance is $d = 2^{m-r}$.*
- *For all $r < m$, we have $RM(r, m) \subseteq RM(r+1, m)$. Code $RM(0, m)$ is the repetition code $\{\mathbf{0}, \mathbf{1}\}$, code $RM(m-1, m)$ is the even code, which consists of all even weight words of length 2^m, and $RM(m, m)$ is the full space $\mathbb{Z}_2^{2^m}$.*
- *$RM(r, m)^{\perp} = RM(m-r-1, m)$, $\forall\ 0 \leq r < m$. For instance, the code $RM(1, m)$ is the binary linear Hadamard code whereas the code $RM(m-2, m)$ is its dual, i.e. the extended binary Hamming code of length 2^m.*

Theorem 2 *[6,7] The rth-order Reed-Muller code $RM(r,m)$ of length $n = 2^m$, $m \geq 1$, is $\mathbb{Z}_4$-linear for $r = 0, 1, 2, m-1, m$ and is not $\mathbb{Z}_4$-linear for $m - 2 \geq r \geq 3$.*

4 Some quaternary Reed-Muller codes

4.1 Additive $\mathcal{ZRM}^-(r, m)$ codes

Let r, m be integers such that $0 \leq r \leq m$. Let $RM(r, m)$ be a rth-order binary Reed-Muller code and $G(r, m)$ its generator matrix.

The following definition can be found in [13]. Let $\mathcal{ZRM}^-(r,m)$ be the quaternary code of quaternary length 2^m generated by the matrix

$$\begin{pmatrix} G(r-1,m) \\ 2G(r,m) \end{pmatrix}, \tag{3}$$

where we consider the ones from the binary matrices G as ones in the quaternary ring $\mathbb{Z}_4$.

Denote by $ZRM^-(r,m) = \Phi(\mathcal{ZRM}^-(r,m))$ the $\mathbb{Z}_4$-linear code of length 2^{m+1}.

We will also use the notation $\mathcal{ZRM}^-(m+1,m)$ for the code defined by the matrix

$$\begin{pmatrix} G(m,m) \\ 2G(m,m) \end{pmatrix}. \tag{4}$$

Proposition 1 *[6,13] Let $r = 0, 1, 2, m-1, m$. Then, $ZRM^-(r, m-1) = RM(r,m)$.*

4.2 Additive $\mathcal{RM}_s(r,m)$ codes

$\mathcal{RM}_s(r,m)$ codes were proposed in [12] with the aim of constructing new families of quaternary linear codes such that, after the Gray map, $\mathbb{Z}_4$-linear codes with the parameters and properties quoted in Theorem 1 are obtained.

Just as there is only one RM family in the binary case, in the quaternary case there are $\lfloor \frac{m+1}{2} \rfloor$ families for each value of m. It is known that for any m there exist $\lfloor \frac{m+1}{2} \rfloor$ non-isomorphic $\mathbb{Z}_4$-linear extended perfect codes [4,8]. Hence, it is expected to obtain $\lfloor \frac{m+1}{2} \rfloor$ families of quaternary linear Reed-Muller codes. Each one of them will contain one of the above-mentioned $\mathbb{Z}_4$-linear extended perfect codes.

Following the same notation than [12], each different family $\{\mathcal{RM}_s(r,m)\}$ is identified by a subindex $s \in \{0, \ldots, \lfloor \frac{m-1}{2} \rfloor\}$.

Theorem 3 *[12] Let $\mathcal{RM}_s(r, m-1)$ and $\mathcal{RM}_s(r-1, m-1)$, $0 \le s \le \lfloor \frac{m-2}{2} \rfloor$, be any two $\mathcal{RM}$ codes of binary length $n = 2^{m-1}$; 2^{k_r} and $2^{k_{r-1}}$ codewords; minimum distance 2^{m-r-1} and 2^{m-r}, respectively, where $k_r = \sum_{i=0}^{r} \binom{m-1}{i}$, $k_{r-1} = \sum_{i=0}^{r-1} \binom{m-1}{i}$. Let $\mathcal{G}_s(r,m)$ be a generator matrix of $\mathcal{RM}_s(r,m)$.*

For any r and $m \ge 2$, $0 < r < m$, the code of which generator matrix is obtained by using the quaternary Plotkin construction

$$\mathcal{G}_s(r,m) = \begin{pmatrix} \mathcal{G}_s(r,m-1) & \mathcal{G}_s(r,m-1) \\ 0 & \mathcal{G}_s(r-1,m-1) \end{pmatrix},$$

where $0 \le s \le \lfloor \frac{m-1}{2} \rfloor$, is a quaternary linear code of binary length $n = 2^m$; 2^k codewords, where $k = \sum_{i=o}^{r} \binom{m}{i}$; minimum distance 2^{m-r} and, moreover, $\mathcal{RM}_s(r-1,m) \subset \mathcal{RM}_s(r,m)$.

The quaternary linear Reed-Muller code $\mathcal{RM}_s(0, m)$ is the repetition code with only one nonzero codeword (the all-twos vector). The code $\mathcal{RM}_s(m, m)$ is the whole space $\mathbb{Z}_4^{2^{m-1}}$ and the codes $\mathcal{RM}_s(1, m)$ and $\mathcal{RM}_s(m-2, m)$ are, respectively, a $\mathbb{Z}_4$-linear Hadamard code and a $\mathbb{Z}_4$-linear extended perfect code.

Among all families we will focus just on the family $s = 0$. As described in [12], this family can be obtained by applying the quaternary Plotkin construction of Theorem 3 starting with the family

$$\{\mathcal{RM}_0(0, 2), \mathcal{RM}_0(1, 2), \mathcal{RM}_0(2, 2)\}. \tag{5}$$

5 Equality between $\mathcal{ZRM}^-(r, m-1)$ and $\mathcal{RM}_s(r, m)$

Theorem 4 *Let $\mathcal{ZRM}^-(r, m-1)$ be the family of quaternary Reed-Muller codes defined as in Section 4.1 and let $\{\mathcal{RM}_0(r, m)\}$ be the family of $\mathcal{RM}_s(r, m)$ codes such that $s = 0$, defined in Section 4.2. Both families of codes are equal.*

Proof. The family of codes $\mathcal{RM}_0(r, m)$ can be obtained by means of the Plotkin construction (see Theorem 3), starting with the family of codes $\{\mathcal{RM}_0(0, 2), \mathcal{RM}_0(1, 2), \mathcal{RM}_0(2, 2)\}$, such that their generator matrices are, respectively, $\begin{pmatrix} 2 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

The family $\{\mathcal{RM}_0(r, m)\}$, is obtained performing the Plotkin construction. Straight afterwards, the codes

$$\mathcal{RM}_0(-1, m+1) = \{\mathbf{0}\}, \mathcal{RM}_0(m+1, m+1) = \mathbb{Z}_4^{2^m}, \tag{6}$$

must be added to the resulting sequence of codes.

Taking into account the generator matrix of $\mathcal{ZRM}^-(r, m)$ codes defined in (3), we proceed to see the coincidence between $\mathcal{ZRM}^-(r, 2)$ and $\{\mathcal{RM}_0(r, 3)\}$ families of codes, for $0 \leq r \leq 3$.

For $r = 0$, the generator matrix of the $\mathcal{ZRM}^-(0, 2)$ code is $\begin{pmatrix} G(-1, 2) \\ 2G(0, 2) \end{pmatrix} = \begin{pmatrix} 2 & 2 & 2 & 2 \end{pmatrix}$ and it exactly coincides with the generator matrix of the $\mathcal{RM}_0(0, 3)$ code.

For $r = 1$, $\mathcal{ZRM}^-(1, 2)$ has the following matrix $\begin{pmatrix} G(0, 2) \\ 2G(1, 2) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix}$ as generator matrix, since $G(1, 2) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ by (2). In this case the resulting matrix also coincides with the generator matrix of the $\mathcal{RM}_0(1, 3)$ code, which can be computed from the matrix $\begin{pmatrix} \mathcal{G}_0(1, 2) & \mathcal{G}_0(1, 2) \\ 0 & \mathcal{G}_0(0, 2) \end{pmatrix}$ by Theorem 3.

For $r = 2$, the generator matrix of the $\mathcal{ZRM}^-(2,2)$ code is $\begin{pmatrix} G(1,2) \\ 2G(2,2) \end{pmatrix} = \begin{pmatrix} 1\,0\,0\,1 \\ 0\,1\,0\,1 \\ 0\,0\,1\,1 \\ 0\,0\,0\,2 \end{pmatrix}$ and it also coincides with the one from the $\mathcal{RM}_0(2,3)$ code, which can be computed from $\begin{pmatrix} \mathcal{G}_0(2,2) & \mathcal{G}_0(2,2) \\ 0 & \mathcal{G}_0(1,2) \end{pmatrix}$.

Finally, for $r = 3$, the $\mathcal{ZRM}^-(3,2)$ code has the following generator matrix $\begin{pmatrix} G(2,2) \\ 2G(2,2) \end{pmatrix} = \mathbb{Z}_4^4$, by (4) and, once more, it coincides by definition with the generator matrix of the $\mathcal{RM}_0(3,3)$ code.

As it has been just proved, the $\mathcal{ZRM}^-(r,2)$ family of codes exactly coincides with the family $\{\mathcal{RM}_0(r,3)\}$.

Let us assume we perform the Plotkin construction with $\mathcal{ZRM}^-(r,m)$ and $\mathcal{ZRM}^-(r+1,m)$ codes. Then, by (2), the construction generates the following matrix:

$$\begin{pmatrix} G(r,m) & G(r,m) \\ 2G(r+1,m) & 2G(r+1,m) \\ 0 & G(r-1,m) \\ 0 & 2G(r,m) \end{pmatrix}.$$

It can be noted that

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

and

$$\begin{pmatrix} 2G(r+1,m) & 2G(r+1,m) \\ 0 & 2G(r,m) \end{pmatrix} = 2G(r+1,m+1),$$

since binary linear Reed-Muller codes can be constructed using the Plotkin construction (see (2)).

Therefore, the Plotkin construction has given the following matrix:

$$\begin{pmatrix} G(r,m+1) \\ 2G(r+1,m+1) \end{pmatrix},$$

which, by (3), corresponds to the generator matrix of the code $\mathcal{ZRM}^-(r+1,m+1)$.

Thus, as it has been proved, the $\mathcal{ZRM}^-(r,m+1)$ family is obtained from the Plotkin construction performed over the $\mathcal{ZRM}^-(r,m)$ family. Once the whole new family is constructed, the $\mathcal{ZRM}^-(-1,m+1) = \{\mathbf{0}\}$ and $\mathcal{ZRM}^-(m+1,m+1) = \mathbb{Z}_4^{2^{m+1}}$ codes must be added to the resulting sequence of codes, in the same way as we did in the $\{\mathcal{RM}_0(r,m+1)\}$ family

(see (6)). Note that both added codes coincide with the corresponding added codes for the $\{\mathcal{RM}_0(r, m+1)\}$ family.
As it has been shown, the family $\{\mathcal{RM}_0(r, 3)\}$ coincides with the family $\mathcal{ZRM}^-(r, 2)$ and, performing the same Plotkin construction to both families, we obtain the different $\{\mathcal{RM}_0(r, m+1)\}$ and $\mathcal{ZRM}^-(r, m)$ families of codes. Hence, all these families coincide for all values of m.

□

6 Conclusions

In this paper a step forward has been given in the classification of the different quaternary codes present in the literature and related to the binary Reed-Muller codes. We have proved that not only $\mathcal{ZRM}^-(r, m-1)$ and $\{\mathcal{RM}_s(r, m)\}$ families of codes are equivalent, but they are also equal for the specific family $s = 0$. Therefore, it is possible to obtain $\mathbb{Z}_4$-linear Reed-Muller codes with the same parameters and properties as the binary linear Reed-Muller code, with both definitions. Moreover, the equality also implies that $\mathcal{ZRM}^-(r, m-1)$ codes can be constructed by means of the Plotkin construction in the same way as $\mathcal{RM}_0(r, m)$ codes were constructed.

7 Further research

Further work needs to be carried out to study the natural inclusion of Delsarte-Goethals, Goethals-Delsarte, Goethals, Preparata, as well as Kerdock codes, within the $\{\mathcal{RM}_0(r, m)\}$ family of codes. In the $\{\mathcal{RM}_0(r, 4)\}$ family, and more specifically in the code $\mathcal{RM}_0(2, 4)$, we have found the quaternary Kerdock code of quaternary length 8 as a subspace. In the $\{\mathcal{RM}_0(r, 6)\}$ family, we have realized that the code $\mathcal{RM}_0(2, 6)$ is the quaternary Delsarte-Goethals code of quaternary length 32. We have also found the quaternary Kerdock code as a subspace of the $\mathcal{RM}_0(2, 6)$ code, even though its construction has been done in a practical and not theoretical way. Future lines of research should also analyze the relationship between the codes found within a given code, and the codes which can be found within the dual of the given code.

References

[1] J. Borges, C. Fernández and K.T. Phelps, "Quaternary Reed-Muller codes", *IEEE Trans. on Information Theory*, vol. 51(7), pp. 2686-2691, 2005.

[2] J. Borges, C. Fernández and K.T. Phelps, "ZRM codes", *IEEE Trans. on Information Theory*, vol. 54(1), pp. 380-386, 2008.

[3] J. Borges, K.T. Phelps, J. Rifà and V.A.Zinoviev, "On $\mathbb{Z}_4$-linear Preparata-like and Kerdock-like codes", *IEEE Trans. on Information Theory*, vol. 49(11), pp. 2834-2843, 2003.

[4] J. Borges, and J. Rifà, "A characterization of 1-perfect additive codes," *IEEE Trans. Inform. Theory*, v. 45, n. 5, pp. 1688-1697, 1999.

[5] C. Carlet, "$\mathbb{Z}_{2^k}$-Linear codes", *IEEE Trans. on Information Theory*, vol. 44, pp. 1543-1547, 1998.

[6] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Solé, "The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals and related codes", *IEEE Trans. on Information Theory*, vol. 40, pp. 301-319, 1994.

[7] X. -D. Hou, J. T. Lahtonen, and S. Koponen, "The Reed-Muller Code $R(r, m)$ is not $\mathbb{Z}_4$-linear for $3 \leq r \leq m-2$", *IEEE Trans. on Information Theory*, vol. 45, pp. 798-799, 1998.

[8] D. S. Krotov, "$\mathbb{Z}_4$-linear Hadamard and extended perfect codes", *International Workshop on Coding and Cryptography*, Paris (France), pp. 329-334, Jan. 8-12, 2001.

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

[10] A. A. Nechaev, "Kerdock codes in a cyclic form", *Disc. Math.*, vol. 1(4), pp. 123-139, 1989.

[11] J. Pujol, J. Rifà, "Additive Reed-Muller codes", Proc. of *Int. Symp. on Information Theory*, Ulm, Germany, pp. 508, 1997.

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

[13] Zhe-Xian Wan, *Quaternary codes*, World Scientific Publishing Co. Pte. Ltd, Singapore, 1997.