Information sets from defining sets for Reed-Muller codes of first and second order

José Joaquín Bernal and Juan Jacobo Simón (Member, IEEE).
Departamento de Matemáticas
Universidad de Murcia, 30100 Murcia, Spain.
Email: {josejoaquin.bernal, jsimon}@um.es

Abstract

Reed-Muller codes belong to the family of affine-invariant codes. As such codes they have a defining set that determines them uniquely, and they are extensions of cyclic group codes. In this paper we identify those cyclic codes with multidimensional abelian codes and we use the techniques introduced in [4] to construct information sets for them from their defining set. For first and second order Reed-Muller codes, we describe a direct method to construct information sets in terms of their basic parameters.

I. Introduction

The family of Reed-Muller codes was introduced by D. E. Muller in 1954 [15] and a specific decoding algorithm for them was presented by I. S. Reed in the same year [17]. Since then, many authors have paid attention to this family of codes for many reasons. On the one hand, they can be implemented and decoded easily, and on the other hand they have a rich algebraic structure which allows us to see them from different points of view. Originally, Reed-Muller codes were defined in terms of boolean functions by Muller and, equivalently, from this point of view they can be constructed as polynomial codes. In another context, they can be treated as geometric codes; specifically, they can be identified with codes of the designs of points and flats in the affine space over the binary field. Finally, they also possess an algebraic structure that let us treat them as group algebra codes. We are interested in this last point of view. Specifically, any Reed-Muller code can be identified with an ideal in a group algebra of an elementary abelian group. Moreover, the family of Reed-Muller codes is contained in the family of so-called affine-invariant codes and so a defining set can be defined for them. The reader may see [2] for a comprehensive explanation on the structures of Reed-Muller codes.

In particular, we are interested in the problem of finding information sets for Reed-Muller codes, a question that has been addressed for many authors earlier. From the geometric point of view several ideas for finding information sets has been presented. In [8] and [16] Moorhouse and Blokhuis gave bases formed by the incidence vectors of certain lines valid for a more general family of geometric codes. Later, J. D. Key, T. P. McDonough and V. C. Mavron extended these definitions in [12] in order to apply the permutation decoding algorithm. Finally, in [13], the same authors gave a simple description of information sets for Reed-Muller codes by using the polynomial approach.

In this work we use the fact that Reed-Muller codes can be seen as extended-cyclic affine-invariant codes to get information sets. From this context any Reed-Muller code is a parity check extension of a cyclic group code, so any information set of that cyclic code is obviously an information set for the Reed-Muller code; moreover, there exists a direct connection between the respective defining sets. On the other hand, in [4] we introduced a method for constructing information sets for any abelian code starting from its defining set. Then, the goal of this paper is to obtain information sets for Reed-Muller codes of first and second order respectively by applying those techniques shown in [4] to the punctured cyclic group code seen as a multidimensional abelian code.

The paper is structured as follows. Section II includes the basic notation and the necessary preliminaries about abelian codes. In Section III we recall how the method given in [4] works in the particular case of two-dimensional abelian codes. In Section IV we prove some necessary results related to the case of cyclic codes seen as two-dimensional cyclic codes; these results will be essential in the rest of the paper. In Section V we focus on Reed-Muller codes: we recall their definition as affine-invariant codes in an abelian group algebra and the description of the defining sets. Then we show how to apply the results in Section IV to Reed-Muller codes under some restrictions on their parameters. Section VI and Secion VII are devoted to develop in detail the construction of information sets for first-order and second-order Reed-Muller codes respectively. In the case of first-order Reed-Muller codes we get a description of the information sets directly from the previous sections; for second-order Reed-Muller codes, although the development is more complicated, involving several technical results, it is remarkable that again the description turns out to be particularly simple in the end.

This work was partially supported by MINECO, project MTM2016-77445-P, and Fundación Séneca of Murcia, project 19880/GERM/15. An extended abstract of a part of this paper was presented at Fith International Castle Meeting on Coding Theory and Applications, Estonia, 2017

II. PRELIMINARIES

In this paper we deal with Reed-Muller codes identified as abelian codes, so for the convenience of the reader we give an introduction to abelian codes just in the binary case. Then all throughout $\mathbb{F}$ denotes the field with two elements.

A binary abelian code is an ideal of a group algebra $\mathbb{F}G$, where G is an abelian group. It is well-known that there exist integers $r_1, \ldots, r_l$ such that G is isomorphic to the direct product $C_{r_1} \times \cdots \times C_{r_l}$, with C_{r_i} the cyclic group of order r_i, $i = 1, \ldots, l$. Moreover, this decomposition yields an isomorphism of $\mathbb{F}$-algebras from $\mathbb{F}G$ to

$$\mathbb{F}[X_1, \ldots, X_l] / \langle X_1^{r_1} - 1, \ldots, X_l^{r_l} - 1 \rangle .$$

We denote this quotient algebra by $\mathbb{A}(r_1, \ldots, r_l)$ and we identify the codewords with polynomials $P(X_1, \ldots, X_l)$ such that every monomial satisfies that the degree of the indeterminate X_i is in $\mathbb{Z}_{r_i}$, the ring of integers modulo r_i, and that we always write as canonical representatives (that is, non negative integers less than r_i). We write the elements $P \in \mathbb{A}(r_1, \ldots, r_l)$ as $P = P(X_1, \ldots, X_l) = \sum a_{\mathbf{j}} X^{\mathbf{j}}$, where $\mathbf{j} = (j_1, \ldots, j_l) \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_l}$, $X^{\mathbf{j}} = X_1^{j_1} \cdots X_l^{j_l}$ and $a_{\mathbf{j}} \in \mathbb{F}$. We always assume that r_i is odd for every $i = 1, \ldots, l$, that is, we assume that $\mathbb{A}(r_1, \ldots, r_l)$ is a semisimple algebra.

Our main tool to study the construction of information sets for abelian codes is the notion of defining set.

Definition 1. *Let $\mathcal{C} \subseteq \mathbb{A}(r_1, \ldots, r_l)$ be an abelian code. Let R_i be the set of r_i-th roots of unity, $i = 1, \ldots, l$. Then the root set of $\mathcal{C}$ is given by*

$$\mathcal{Z}(\mathcal{C}) = \left\{ (\beta_1, \ldots, \beta_l) \in \prod_{i=1}^{l} R_i \ \mid \ P(\beta_1, \ldots, \beta_l) = 0 \text{ for all } P(X_1, \ldots, X_l) \in \mathcal{C} \right\}.$$

Then, for a fixed primitive r_i-th root of unity α_i in some extension of $\mathbb{F}$, $i = 1, \ldots, l$, the defining set of $\mathcal{C}$ with respect to $\alpha = \{\alpha_1, \ldots, \alpha_l\}$ is

$$D_\alpha(\mathcal{C}) = \{ (a_1, \ldots, a_l) \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_l} \ \mid \ (\alpha_1^{a_1}, \ldots, \alpha_l^{a_l}) \in \mathcal{Z}(\mathcal{C}) \}.$$

It can be proved that, fixed a collection of primitive roots of unity, every abelian code is totally determined by its defining set.

Remark 2. *The reader may check that in the case $l = 1$ the previous definitions coincide with the classical notions of zeros and defining set of a cyclic code.*

In order to describe the structure of the defining set of an abelian code we need to introduce the following definitions.

Definition 3. *Let a, r and γ be integers. The 2^γ-cyclotomic coset of a modulo r is the set*

$$C_{2^\gamma, r}(a) = \left\{ a \cdot 2^{\gamma \cdot i} \ \mid \ i \in \mathbb{N} \right\} \subseteq \mathbb{Z}_r.$$

We shall write $C_r(a)$ when $\gamma = 1$.

Definition 4. *Given $(a_1, \ldots, a_l) \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_l}$, its 2-orbit modulo $(r_1, \ldots, r_l)$ is the set*

$$Q(a_1, \ldots, a_l) = \left\{ \left(a_1 \cdot 2^i, \ldots, a_l \cdot 2^i \right) \ \mid \ i \in \mathbb{N} \right\} \subseteq \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_l}.$$

It is well known that for every abelian code $\mathcal{C} \subseteq \mathbb{A}(r_1, \ldots, r_l)$, $D(\mathcal{C})$ is closed under multiplication by 2 in $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_l}$, and so $D(\mathcal{C})$ is a disjoint union of 2-orbits modulo $(r_1, \ldots, r_l)$. Conversely, every union of 2-orbits modulo $(r_1, \ldots, r_l)$ defines an abelian code in $\mathbb{A}(r_1, \ldots, r_l)$. From now on, we will only write 2-orbit, and the tuple of integers will always be clear by the context.

To finish this section we give the notion of information set of a code in the context of abelian codes. For $P = \sum a_{\mathbf{j}} X^{\mathbf{j}} \in \mathbb{A}(r_1, \ldots, r_l)$ and $\mathcal{I}$ be a subset of $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_l}$, we denote by $P_\mathcal{I}$ the vector $(a_{\mathbf{j}})_{\mathbf{j} \in \mathcal{I}} \in \mathbb{F}^{|\mathcal{I}|}$. Now, for an abelian code $\mathcal{C} \subseteq \mathbb{A}(r_1, \ldots, r_l)$ we denote by $\mathcal{C}_\mathcal{I}$ the linear code $\{P_\mathcal{I} : P \in \mathcal{C}\} \subseteq \mathbb{F}^{|\mathcal{I}|}$.

Definition 5. *An information set for an abelian code $\mathcal{C} \subseteq \mathbb{A}(r_1, \ldots, r_l)$ with dimension k is a set $\mathcal{I} \subseteq \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_l}$ such that $|\mathcal{I}| = k$ and $\mathcal{C}_\mathcal{I} = \mathbb{F}^k$.*

The complementary set $(\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_l}) \setminus \mathcal{I}$ is called a set of check positions for $\mathcal{C}$.

As usual, we denote by $\mathcal{C}^\perp$ the dual code of $\mathcal{C}$, that is, the set of codewords $v \in \mathbb{A}(r_1, \ldots, r_l)$ such that $v \cdot u = 0$, for all $u \in \mathcal{C}$, where " $\cdot$ " denotes the usual inner product. It is easy to see that any information set for $\mathcal{C}$ is a set of check positions for $\mathcal{C}^\perp$ and vice versa.

III. Information sets for abelian codes

In [4] we introduced a method for constructing information sets for any multidimensional abelian code just in terms of its defining set. In this section we only recall the two-dimensional construction because it is the unique case that we will use. So, from now on we take $l = 2$ and the ambient space will be $\mathbb{A}(r_1, r_2)$.

Let $e = (e_1, e_2) \in \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$. We define

$$m(e_1) = |C_{r_1}(e_1)|$$

and

$$m(e) = m(e_1, e_2) = \left|C_{2^{m(e_1)}, r_2}(e_2)\right|. \tag{1}$$

The construction of information sets is based on the computation of the parameters defined in (1) on a special subset of the defining set of the given abelian code. Specifically this set has to satisfy the conditions described in the following definition. For any $A \subset \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$ we denote its projection onto the first coordinate by A_1.

Definition 6. *Let D be a union of 2-orbits modulo (r_1, r_2) and $\overline{D} \subset D$ a complete set of representatives. Then $\overline{D}$ is called a set of restricted representatives if $\overline{D}_1$ is a complete set of representatives of the 2-cyclotomic cosets modulo r_1 in D_1.*

Remark 7. *In [4] we gave the notion of restricted representatives associated to a fixed ordering on the indeterminates X_1, X_2. In the two-dimensional case that definition is equivalent to Definition 6 when we fix the ordering $X_1 < X_2$. This will be our default ordering, so we will make no reference to the order on the indeterminates in the rest of the paper.*

Example 8. *Consider $r_1 = 3, r_2 = 5$ and let $\mathcal{C} \subseteq \mathbb{A}(3, 5)$ be the abelian code with defining set $\mathcal{D}(\mathcal{C}) = Q(1,1) \cup Q(1,2) \cup Q(0,0)$, where $Q(1,1) = \{(1,1), (2,2), (1,4), (2,3)\}$, $Q(1,2) = \{(1,2), (2,4), (1,3), (2,1)\}$ and $Q(0,0) = \{(0,0)\}$. Then, according to Definition 6, the set of representatives $\{(1,1), (2,1), (0,0)\}$ is not restricted, because $C_3(1) = C_3(2)$, while $\{(1,1), (1,2), (0,0)\}$ is indeed restricted.*

Now, let $\mathcal{C} \subseteq \mathbb{A}(r_1, r_2)$ be an abelian code with defining set $D_\alpha \subseteq \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$, with respect to $\alpha = \{\alpha_1, \alpha_2\}$. Take $\overline{D} \subset D_\alpha$ a set of restricted representatives. Given $e_1 \in \overline{D}_1$, let

$$R(e_1) = \{e_2 \in \mathbb{Z}_{r_2} \mid (e_1, e_2) \in \overline{D}\}.$$

For each $e_1 \in \overline{D}_1$, we define

$$M(e_1) = \sum_{e_2 \in R(e_1)} m\,(e_1, e_2) \tag{2}$$

and we consider the values $\{M(e_1)\}_{e_1 \in \overline{D}_1}$. Then we denote

$$\begin{aligned} f_1 &= \max_{e_1 \in \overline{D}_1} \{M(e_1)\} \qquad \text{and} \\ f_i &= \max_{e_1 \in \overline{D}_1} \{M(e_1) \mid M(e_1) < f_{i-1}\}. \end{aligned}$$

So, we obtain the sequence

$$f_1 > \cdots > f_s > 0 = f_{s+1}, \tag{3}$$

that is, we denote by f_s the minimum value of the parameters $M(\cdot)$ and we set $f_{s+1} = 0$ by convention. Note that $M(e_1) > 0$, for all $e_1 \in \overline{D}_1$, by definition.

From the previous values f_i we define for $i = 1, \ldots, s$

$$g_i = \sum_{M(e_1) \geq f_i} m(e_1) \tag{4}$$

and then we obtain the sequence

$$g_1 < g_2 < \cdots < g_s. \tag{5}$$

Finally, we define the set

$$\Gamma(\mathcal{C}) = \{(i_1, i_2) \in \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \mid \text{ there exists } 1 \leq j \leq s \text{ with } f_{j+1} \leq i_2 < f_j, \text{ and } 0 \leq i_1 < g_j\}. \tag{6}$$

The following theorem, proved in [4] for any abelian code, establishes that $\Gamma(\mathcal{C})$ is a set of check positions for $\mathcal{C}$, and consequently $\Gamma(\mathcal{C})$ defines an information set for $\mathcal{C}^\perp$.

Theorem 9. *Let r_1, r_2 be odd integers and let $\mathcal{C}$ be an abelian code in $\mathbb{A}(r_1, r_2)$ with defining set $\mathcal{D}_\alpha(\mathcal{C})$ with respect to $\alpha = \{\alpha_1, \alpha_2\}$. Then $\Gamma(\mathcal{C})$ is a set of check positions for $\mathcal{C}$.*

Let us observe that given an abelian code $\mathcal{C} \subseteq \mathbb{A}(r_1, r_2)$ with defining set $D_\alpha(\mathcal{C})$ if one chooses different primitive roots of unity, say $\gamma = \{\gamma_1, \gamma_2\}$, then the *structure* of the q-orbits in $D_\gamma(\mathcal{C})$ is the same as in $D_\alpha(\mathcal{C})$, that is, we obtain the same

values for the parameters (1) and (2), so we get the same set of check positions $\Gamma(\mathcal{C})$ (see [7, p.100]). That is why we do not use any reference to the roots of unity taken in the notation of the set of check positions. So, in the rest of the paper, for any abelian code $\mathcal{C}$ we denote its defining set by $D(\mathcal{C})$ and the corresponding set of check positions by $\Gamma(\mathcal{C})$ without any mention of the primitive roots.

Example 10. *We continue with the code $\mathcal{C}$ considered in Example 8. Then $\mathcal{D}(\mathcal{C}) = Q(1,1) \cup Q(1,2) \cup Q(0,0)$ and we take $\overline{\mathcal{D}} = \{(1,1),(1,2),(0,0)\}$ as set of restricted representatives. From (2) we have that $M(1) = m(1,1) + m(1,2) = 2+2 = 4$ and $M(0) = m(0,0) = 1$. So $f_1 = 4 > f_2 = 1 > f_3 = 0$. On the other hand, from (4) we obtain $g_1 = m(1) = 2, g_2 = g_1 + m(0) = 3$. Therefore,*

$$\begin{aligned}\Gamma(\mathcal{C}) &= \{(i_1,i_2) \in \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \mid (1 \leq i_2 < 4 \text{ and } 0 \leq i_1 < 2) \text{ or } (0 \leq i_2 < 1 \text{ and } 0 \leq i_1 < 3)\} \\ &= \{(0,0),(0,1),(0,2),(0,3),(1,0),(1,1),(1,2),(1,3),(2,0)\}\end{aligned}$$

is a set of check positions for $\mathcal{C}$.

Remark 11. *In [4] we showed how to construct the previous set of check positions for any multidimensional abelian code. As we have already mentioned, in this paper we only need to use the two-dimensional case which yields the same information set that was introduced by H. Imai in [11].*

IV. Cyclic codes as two-dimensional cyclic codes

We are going to construct an information set for the punctured cyclic code of a Reed-Muller code viewed as a multidimensional abelian code. So, we are interested in applying the results of the previous section when the original abelian code is in fact cyclic.

Let $\mathcal{C}^*$ be a binary cyclic code with length $n = r_1 \cdot r_2$. All throughout this section we assume that $\gcd(r_1, r_2) = 1$ and r_1, r_2 are odd. Then let $T : \mathbb{Z}_n \to \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$ be an isomorphism, and let us denote $T = (T_1, T_2)$; that is, $T_i(e)$ is the projection of $T(e)$ onto $\mathbb{Z}_{r_i}$, for $i = 1, 2$ and any $e \in \mathbb{Z}_n$.

The proof of the following result is straightforward.

Lemma 12. *For every $e \in \mathbb{Z}_n$ the equality $T(C_n(e)) = Q(T(e))$ holds; in particular $|C_n(e)| = |Q(T(e))|$. Moreover, one has that the projection of $Q(T(e))$ onto $\mathbb{Z}_{r_1}$ is equal to $C_{r_1}(T_1(e))$.*

Let $\mathcal{D}^* = D_\alpha(\mathcal{C}^*) \subseteq \mathbb{Z}_n$ be the defining set of $\mathcal{C}^*$ with respect to an arbitrary primitive n-th root of unity α. Then, since there exist integers η_1, η_2 such that $\eta_1 r_1 + \eta_2 r_2 = 1$, we have that $\alpha_1 = \alpha^{\eta_2 r_2}$ and $\alpha_2 = \alpha^{\eta_1 r_1}$ are primitive r_1-th and r_2-th roots of unity respectively. Fix T an isomorphism as above and set $T(1) = (\delta_1, \delta_2)$; observe that $\gcd(\delta_1, r_1) = 1$ and $\gcd(\delta_2, r_2) = 1$. We define the abelian code $\mathcal{C} = \mathcal{C}_{(\mathcal{C}^*, T)} \subseteq \mathbb{A}(r_1, r_2)$ as the code with defining set $\mathcal{D} = D(\mathcal{C}) = T(\mathcal{D}^*)$, with respect to $(\beta_1, \beta_2) = (\alpha_1^{\delta_1^{-1}}, \alpha_2^{\delta_2^{-1}})$. In this situation, we have that $\mathcal{C}$ is the image of $\mathcal{C}^*$ by the map

$$\begin{aligned}\mathbb{A}(n) &\longrightarrow \mathbb{A}(r_1, r_2) \\ \sum a_i X^i &\hookrightarrow \sum b_{jl} X^j Y^l,\end{aligned}$$

where $b_{jl} = a_i$ if and only if $T(i) = (j, l)$. Therefore, $\mathcal{I}$ is an information set for $\mathcal{C}$ if and only if $T^{-1}(\mathcal{I})$ is an information set for $\mathcal{C}^*$. Usually, we omit the reference to the original cyclic code and the isomorphism T in the notation of the new abelian code, and we will write $\mathcal{C}$ instead of $\mathcal{C}_{(\mathcal{C}^*, T)}$; those references will by clear by the context.

For the rest of this section we assume that we have fixed a choice of α and T (consequently, the roots β_1, β_2 are also fixed).

Then, the goal of this section is to describe the values of the parameters defined in (1) and (2), used to get a set of check positions for $\mathcal{C}$ (see 6), just in terms of the defining set of $\mathcal{C}^*$. This will allow us to define an information set for the original cyclic code $\mathcal{C}^*$ without any mention to the abelian code $\mathcal{C}$.

Remark 13. *Let us observe that, since the defining set $\mathcal{D}^* = D_\alpha(\mathcal{C}^*)$ depends on the choice of α, if we fix another one β, we get a new defining set $D_\beta(\mathcal{C}^*)$ and consequently we obtain a different abelian code $\mathcal{C}$. However, this new abelian code has a defining set with the same structure of q-orbits so it yields the same set $\Gamma(\mathcal{C})$ (see paragraph after Theorem 9).*

On the other hand, it is easy to prove that any change of the isomorphism T is equivalent to a change of the primitive root α in order to get the same abelian code in $\mathbb{A}(r_1, r_2)$. Nevertheless, this implies that, since we get the same set $\Gamma(\mathcal{C})$, we could obtain a different set of check positions $T^{-1}(\Gamma(\mathcal{C}))$ at the end. Therefore, by the method we are describing in this section we get at most as many information sets as there are isomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$ exist.

Let $\overline{\mathcal{D}^*} \subseteq \mathcal{D}^* \subseteq \mathbb{Z}_n$ be a complete set of representatives of the 2-cyclotomic cosets modulo n in $\mathcal{D}^*$. As we have noted, for any $e \in \overline{\mathcal{D}^*}$, $T(C_n(e)) = Q(T(e))$, so $T(\overline{D^*})$ is a complete set of representatives of the 2-orbits modulo (r_1, r_2) in $T(D^*)$. However, it might not be a set of restricted representatives according to Definition 6. Then we introduce the following definition.

Definition 14. *Let $\overline{\mathcal{D}^*} \subseteq \mathcal{D}^*$ be a complete set of representatives of the 2-cyclotomic cosets modulo n in $\mathcal{D}^*$. Then $\overline{\mathcal{D}^*}$ is said to be a suitable set of representatives if $T(\overline{\mathcal{D}^*})$ is a set of restricted representatives of the 2-orbits in $T(\mathcal{D}^*)$.*

The next lemma shows that we will always be able to take a suitable set of representatives in $\mathcal{D}^*$.

Lemma 15. *Let $\mathcal{D}^*$ be the defining set of a cyclic code $\mathcal{C}^* \subseteq \mathbb{A}(n)$. Let $\mathcal{C} \subseteq \mathbb{A}(r_1, r_2)$ be the abelian code with defining set $T(\mathcal{D}^*)$. Then, there always exists a suitable set of representatives $\overline{\mathcal{D}^*} \subseteq \mathcal{D}^*$.*

Proof. From Lemma 12, for any $e \in \mathcal{D}^*$ we have that $Q(T(e))_1 = C_{r_1}(T_1(e))$. Let $\overline{\mathcal{D}^*}$ be a complete set of representatives of the 2-cycloctomic cosets modulo n in $\mathcal{D}^*$. Take A a complete set of the 2-cyclotomic cosets modulo r_1 in $\{T_1(e) : e \in \mathcal{D}^*\}$. Now, take $e \in \overline{\mathcal{D}^*}$ and let $a \in A$ be such that $T_1(e) \in C_{r_1}(a)$. Then there exists $e' \in C_n(e)$ that satisfies $T_1(e') = a$; if $e' \neq e$ then we redefine $\overline{\mathcal{D}^*}$ by replacing e with e'. This concludes the proof. □

Example 16. *Let us consider binary cyclic codes of length $n = 21$, so $r_1 = 3, r_2 = 7$. Let $\mathcal{C}^* \subseteq \mathbb{A}(21)$ be the cyclic code such that its defining set, with respect to a 21-th primitive root of unity α, is the following union of 2-cyclotomic cosets modulo 21, $\mathcal{D}^* = \{1, 2, 4, 8, 11, 16\} \cup \{3, 6, 12\} \cup \{7, 14\}$. Take $T : \mathbb{Z}_{21} \to \mathbb{Z}_3 \times \mathbb{Z}_7$ the isomorphism given by the Chinese Remainder Theorem. Then $\mathcal{C}$ denotes the abelian code in $\mathbb{A}(3, 7)$ with defining set $\mathcal{D} = T(\mathcal{D}^*)$, that is, the following union of 2-orbits modulo $(3, 7)$, $T(\mathcal{D}) = \{(1, 1), (2, 2), (1, 4), (2, 1), (2, 4), (1, 2)\} \cup \{(0, 3), (0, 6), (0, 5)\} \cup \{(1, 0), (2, 0)\}$. The set $B = \{2, 3, 7\} \subseteq \mathcal{D}^*$ is a complete set of representatives of the 2-cyclotomic cosets in $\mathcal{D}^*$; however it is not a suitable set of representatives since $T(B) = \{(2, 2), (0, 3), (1, 0)\}$ is not a restricted set of representatives in $\mathcal{D}$ (note that $C_3(1) = C_3(2)$). We may solve this problem by replacing 2 by 1. Then $\overline{\mathcal{D}^*} = \{1, 3, 7\}$ is a suitable set of representatives because $T(\overline{\mathcal{D}^*}) = \{(1, 1), (0, 3), (1, 0)\}$ is a restricted set of representatives in $\mathcal{D}$.*

Now we deal with the construction of a set of check positions for the abelian code $\mathcal{C} = \mathcal{C}_{(\mathcal{C}^*, T)} \subseteq \mathbb{A}(r_1, r_2)$ just in terms of $\mathcal{D}^*$, the defining set of the cyclic code $\mathcal{C}^*$.

Given $\overline{\mathcal{D}^*} \subseteq \mathcal{D}^*$ a suitable set of representatives, we consider $\sim$ the equivalence relation on $\overline{\mathcal{D}^*}$ given by the rule

$$a \sim b \in \overline{\mathcal{D}^*} \text{ if and only if } a \equiv b \mod r_1. \tag{7}$$

From now on we denote by $\overline{\mathcal{D}^*}$ a suitable set of representatives and $\mathcal{U} \subseteq \overline{\mathcal{D}^*}$ a complete set of representatives of the equivalence classes related to $\sim$. In addition, for any $u \in \mathcal{U}$ we write

$$\mathcal{O}(u) = \{a \in \overline{\mathcal{D}^*} \mid a \sim u\}.$$

Observe that if $\overline{\mathcal{D}} = T(\overline{\mathcal{D}^*})$ then $\overline{D}_1 = T_1(\mathcal{U})$. Furthermore, for any $e \in \overline{\mathcal{D}^*}$ there exists a unique $u \in \mathcal{U}$ such that $T_1(u) = T_1(e)$. By abuse of notation, we will write

$$C_{r_1}(e) = C_{r_1}(T_1(e)) = C_{r_1}(T_1(u)) = C_{r_1}(u).$$

Example 17. *Following Example 16, from the suitable set of representatives $\overline{\mathcal{D}^*} = \{1, 3, 7\}$ we may define, for instance, $\mathcal{U} = \{1, 3\}$. Note that $\mathcal{O}(1) = \{1, 7\}$.*

Lemma 18. *For any $e \in \overline{\mathcal{D}^*}$ one has that*

$$m\left(T(e)\right) = \frac{|C_n(e)|}{|C_{r_1}(u)|},$$

where u is the unique element in $\mathcal{U}$ such that $T_1(u) = T_1(e)$.

Proof. By using the equalities in Lemma 12 and the definition of T one has that $|Q(T(e))| = m(T_1(e)) \cdot m(T(e))$. On the other hand $m(T_1(e)) = m(T_1(u)) = |C_{r_1}(T_1(u))| = |C_{r_1}(u)|$, so we are done. □

The following proposition shows how we can write the parameters (1) over the elements of $\overline{\mathcal{D}} = T(\overline{\mathcal{D}^*}) \subseteq \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$ in terms of elements in $\mathcal{U} \subseteq \overline{\mathcal{D}^*}$.

Proposition 19. *Take $e \in \overline{\mathcal{D}^*}$ and $u \in \mathcal{U}$ (unique) such that $T_1(u) = T_1(e)$. Let $\overline{\mathcal{D}} = T(\overline{\mathcal{D}^*}) \subseteq \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$. For each $k \in R(T_1(e))$ there exists a unique $v_k \in \mathcal{O}(u) \subseteq \overline{\mathcal{D}^*}$ satisfying $T(v_k) = (T_1(e), k)$ and*

$$m(T_1(e), k) = \frac{|C_n(v_k)|}{|C_{r_1}(u)|}.$$

Proof. Take $k \in R(T_1(e))$. Then $(T_1(e), k) \in \overline{\mathcal{D}} = T(\overline{\mathcal{D}^*})$, so there exists a unique $v_k \in \overline{\mathcal{D}^*}$ such that $T(v_k) = (T_1(e), k)$. Moreover, $v_k \in \mathcal{O}(u)$ because $T_1(v_k) = T_1(e) = T_1(u)$. Now

$$|C_n(v_k)| = |Q(T(v_k))| = |Q(T_1(e), k)| = m(T_1(e)) \cdot m(T_1(e), k) = m(T_1(u)) \cdot m(T_1(e), k) = |C_{r_1}(u)| \cdot m(T(e_1), k).$$

□

Now, we use the previous result to obtain the values $M(\cdot)$ (defined in (2)) corresponding with the set $\overline{\mathcal{D}} = T(\overline{\mathcal{D}^*}) \subset \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$, in terms of the elements in $\mathcal{U} \subseteq \mathbb{Z}_n$.

Theorem 20. *For each $(e_1, e_2) \in \overline{\mathcal{D}} = T(\overline{\mathcal{D}^*})$, there exists a unique $u \in \mathcal{U}$ such that $T_1(u) = e_1$ and*

$$M(e_1) = \frac{1}{|C_{r_1}(u)|} \sum_{v \in \mathcal{O}(u)} |C_n(v)| = \sum_{v \in \mathcal{O}(u)} |C_{2^{|C_{r_1}(u)|}, r_2}(T_2(v))|.$$

Proof. Take $(e_1, e_2) \in \overline{\mathcal{D}}$ and $e \in \overline{\mathcal{D}^*}$ such that $T(e) = (e_1, e_2)$. Then

$$M(e_1) = \sum_{k \in R(e_1)} m(e_1, k) = \sum_{k \in R(e_1)} m(T_1(e), k) = M(T_1(e)).$$

By Proposition 19, for any $k \in R(e_1)$ there exists a unique $v_k \in \mathcal{O}(u) \subseteq \overline{\mathcal{D}^*}$ such that $T(v_k) = (T_1(e), k)$ and $m(T_1(e), k) = \frac{|C_n(v_k)|}{|C_{r_1}(u)|}$. Now, note that if $k \neq k' \in R(e_1)$ then $v_k \neq v_{k'}$ because $T(v_k) = (e_1, k) \neq (e_1, k') = T(v_{k'})$. Finally, if $v \in \mathcal{O}(u)$ then $T_1(v) = T_1(u) = e_1$, and then there exists $k \in R(e_1)$ such that $T(v) = (e_1, k)$, so $v = v_k$. This finishes the proof. □

To sum up, fixing a n-th primitive root of unity α and an isomorphim $T : \mathbb{Z}_n \to \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$, let $\mathcal{C}^*$ be a cyclic code in $\mathbb{A}(n)$ with defining set with respect to α, $\mathcal{D}^*$, and let $\mathcal{C} = \mathcal{C}_{(\mathcal{C}^*, T)} \subseteq \mathbb{A}(r_1, r_2)$ be the abelian code with defining set $\mathcal{D} = T(\mathcal{D}^*)$ (taking as reference the suitable primitive roots of unity mentioned at the beginning of this section). We have shown that we can take a suitable set of representatives $\overline{\mathcal{D}^*} \subseteq \mathcal{D}^*$ and a set $\mathcal{U} \subseteq \overline{\mathcal{D}^*}$, with $T_1(\mathcal{U}) = \overline{\mathcal{D}}_1$ ($\overline{\mathcal{D}} = T(\overline{\mathcal{D}^*})$), in such a way that we are able to construct the set of check positions given in (6) for $\mathcal{C}$ in terms of $\mathcal{U}$ as follows:

Since for any $e_1 \in \overline{\mathcal{D}}_1$ there exists a unique element $u \in \mathcal{U}$ that satisfies $T_1(u) = e_1$, by abuse of notation, we may write $M(u) = M(T_1(u)) = M(e_1)$. Then, the set of values (2) can be described as

$$\left\{ M(u) = \frac{1}{|C_{r_1}(u)|} \sum_{v \in \mathcal{O}(u)} |C_n(v)| \ \mid \ u \in \mathcal{U} \right\} \tag{8}$$

which yields the sequence $f_1 > \cdots > f_s > 0 = f_{s+1}$ (see (3)). On the other hand, for any $k = 1, \ldots, s$ the values (4) can be computed as

$$g_k = \sum_{\substack{u \in \mathcal{U} \\ M(u) \geq f_k}} |C_{r_1}(u)|$$

which give us the sequence $g_1 < g_2 < \cdots < g_s$ (see (5)) and hence the set $\Gamma(\mathcal{C})$.

Remark 21. *From the development of the method we have described, the reader may note that the isomorphism T has no influence on the construction of $\Gamma(\mathcal{C})$. So, as we have said in Remark 13, we obtain at most as many information sets as there are isomorphisms.*

Example 22. *We apply the results in this section to the code $\mathcal{C}^*$ given in Example 16. Recall that its defining set is $\mathcal{D}^* = \{1, 2, 4, 8, 11, 16\} \cup \{3, 6, 12\} \cup \{7, 14\}$ and we were using the isomorphism given by the Chinese Remainder Theorem. We have chosen $\overline{\mathcal{D}^*} = \{1, 3, 7\}$ as suitable set of representatives and $\mathcal{U} = \{1, 3\}$. Then, from (8) we have*

$$\begin{aligned} M(1) &= \frac{1}{|C_3(1)|} \left(|C_{21}(1)| + |C_{21}(7)| \right) = \frac{1}{2}(6 + 2) = 4, \\ M(3) &= \frac{1}{|C_3(3)|} \cdot |C_{21}(3)| = \frac{1}{1} \cdot 3 = 3, \end{aligned}$$

and so $f_1 = 4 > f_2 = 3 > f_3 = 0$. On the other hand, $g_1 = m(1) = 2 < g_2 = 2 + m(0) = 3$. These sequences yield the set of check positions for $\mathcal{C}$

$$\Gamma(\mathcal{C}) = \{(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3), (2,0), (2,1), (2,2)\}.$$

Finally, we have that $T^{-1}(\Gamma(\mathcal{C})) = \{0, 1, 2, 3, 7, 8, 9, 10, 14, 15, 16\}$ is a set of check positions for $\mathcal{C}^*$.

Now, let us consider the isomorphism $\widehat{T} : \mathbb{Z}_{21} \to \mathbb{Z}_3 \times \mathbb{Z}_7$ given by $\widehat{T}(1) = (1, 2)$. Then

$$\widehat{T}^{-1}(\Gamma(\mathcal{C})) = \{0, 1, 4, 7, 8, 11, 12, 14, 15, 18, 19\},$$

which is a different set of check positions for $\mathcal{C}^*$.

V. REED-MULLER CODES

In this section we shall introduce Reed-Muller codes from the group-algebra point of view. Specifically, we are going to present Reed-Muller codes as a type of code contained in the family of so-called affine-invariant extended cyclic codes (see, for instance, [1], [2] or [9]).

Recall that $\mathbb{F}$ denotes the binary field. Let G be the additive subgroup of the field of 2^m elements. So G is an elementary abelian group of order $|G| = 2^m$ and $G^* = G \setminus \{0\}$ is a cyclic group. From now on we write $n = 2^m - 1$. We consider the group algebra $\mathbb{F}G$ which will be the ambient space for Reed-Muller codes. We denote the elements in $\mathbb{F}G$ as $\sum_{g\in G} a_g X^g$ and then the operations are written as follows

$$\begin{aligned}\sum_{g\in G} a_g X^g + \sum_{g\in G} b_g X^g &= \sum_{g\in G}(a_g + b_g)X^g \\ c \cdot \sum_{g\in G} a_g X^g &= \sum_{g\in G}(c \cdot a_g)X^g \ (c \in \mathbb{F}) \\ \left(\sum_{g\in G} a_g X^g\right) \cdot \left(\sum_{h\in G} b_h X^h\right) &= \sum_{g\in G}\left(\sum_{g_1+g_2=g} a_{g_1} b_{g_2}\right) X^g.\end{aligned}$$

Notice that X^0 is the unit element in $\mathbb{F}G$. The following definitions introduce the family of affine-invariant extended cyclic codes. All throughout this section we fix α, a generator of the cyclic group G^*, that is, a primitive n-th root of unity.

Definition 23. *Let α be a generator of G^*. A code $\mathcal{C} \subseteq \mathbb{F}G$ is an extended cyclic code if for any $\sum_{g\in G} a_g X^g \in \mathcal{C}$ one has that $\sum_{g\in G} a_g X^{\alpha g} \in \mathcal{C}$ and $\sum_{g\in G} a_g = 0$.*

Definition 24. *We say that an extended cyclic code $\mathcal{C} \subseteq \mathbb{F}G$ is affine-invariant if for any $\sum_{g\in G} a_g X^g \in \mathcal{C}$ one has that $\sum_{g\in G} a_g X^{hg+k}$ belongs to $\mathcal{C}$ for all $h, k \in G, h \neq 0$.*

It is clear that if $\mathcal{C} \subseteq \mathbb{F}G$ is affine-invariant then $\mathcal{C}$ is an ideal in $\mathbb{F}G$ and $\mathcal{C}^* \subseteq \mathbb{F}G^*$, the punctured code at the position X^0, is cyclic in the sense that it is the projection to $\mathbb{F}G^*$ of the image of a cyclic code via the map

$$\begin{aligned}\mathbb{A}(n) &\longrightarrow \mathbb{F}G \\ \sum_{i=0}^{n-1} a_i X^i &\hookrightarrow \left(-\sum_{i=0}^{n-1} a_i\right) X^0 + \sum_{i=0}^{n-1} a_i X^{\alpha^i},\end{aligned} \tag{9}$$

where α is the fixed n-th root of unity.

Now, for any $s \in \{0, \ldots, n = 2^m - 1\}$ we consider the $\mathbb{F}$-linear map $\phi_s : \mathbb{F}G \to G$ given by

$$\phi_s\left(\sum_{g\in G} a_g X^g\right) = \sum_{g\in G} a_g g^s$$

where we assume $0^0 = 1 \in \mathbb{F}$ by convention.

Definition 25. *Let $\mathcal{C} \subseteq \mathbb{F}G$ be an affine-invariant code. The set*

$$D(\mathcal{C}) = \{i \mid \phi_i(x) = 0 \text{ for all } x \in \mathcal{C}\}$$

is called the defining set of $\mathcal{C}$.

Note first that since $\mathcal{C}$ is an extended-cyclic code, one has that $0 \in D(\mathcal{C})$ because $\phi_0\left(\sum_{g\in G} a_g X^g\right) = \sum_{g\in G} a_g g^0 = \sum_{g\in G} a_g$. Furthermore, it follows from the equality $\phi_{2s}(x) = (\phi_s(x))^2$ $(x \in \mathcal{C})$ that $D(\mathcal{C})$ is a union of 2-cyclotomic cosets modulo n. On the other hand, keeping in mind the map (9), we talk about the set of zeros an the defining set of $\mathcal{C}^*$ when we are making reference to those of the corresponding cyclic code in $\mathbb{A}(n)$. So, fixing α a n-th primitive root of unity, the zeros of the cyclic code $\mathcal{C}^*$ are $\{\alpha^s \mid s \in D(\mathcal{C}), s \neq 0\}$ and the defining set of $\mathcal{C}^*$ (according to Definition 1 and with respect to that root of unity), is $D(\mathcal{C}^*) = D(\mathcal{C}) \setminus \{0\}$.

It is easy to prove that any affine-invariant code is totally determined by its defining set. Conversely, any subset of $\{0, \ldots, n\}$ which is a union of 2-cyclotomic cosets and contains 0 defines an affine-invariant code in $\mathbb{F}G$.

Remark 26. *It may occur that $n, 0 \in D(\mathcal{C})$ which could yield confusion considering the 2-cyclotomic cosets modulo n. Those elements are considered distinct and they indicate different properties of the code $\mathcal{C}$; namely, 0 always belongs to $D(\mathcal{C})$ because*

$\mathcal{C}$ is an extended cyclic code, while if n belongs to $D(\mathcal{C})$ then the cyclic code $\mathcal{C}^*$ is even-like which implies that $\mathcal{C}$ is a trivial extension.

Finally, to introduce the family of Reed-Muller codes as affine-invariant codes we need to recall the notions of binary expansion and 2-weight. For any natural number k its binary expansion is the sum $\sum_{r\geq 0} k_r 2^r = k$ with $k_r \in \{0,1\}$. The 2-weight or simply weight of k is $\mathrm{wt}(k) = \sum_{r\geq 0} k_r$.

Definition 27. *Let $0 < \rho < m$. The Reed-Muller code of order ρ and length 2^m, denoted by $R(\rho, m)$, is the affine-invariant code in $\mathbb{F}G$ with defining set*

$$D(R(\rho,m)) = \{i \mid 0 \leq i < 2^m - 1 \text{ and } \mathrm{wt}(i) < m - \rho\}.$$

From the classical point of view, Reed-Muller codes are also defined for the cases $\rho = 0, m$, but they correspond with the trivial cases $R(m,m) = \mathbb{F}G$ and $R(0,m) = \langle \sum_{g\in G} g\rangle$ (the repetition code) which do not have interest in the context of this paper. The following result summarizes some well known results about Reed-Muller codes that we will refer to further. The reader may see [2].

Proposition 28. *Let $0 < \rho < m$.*

1) The Reed-Muller code $R(\rho, m)$ is a code of length 2^m, dimension

$$k = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{\rho}$$

and minimum distance $2^{m-\rho}$.

2) $R(m-1,m) = \{\sum\limits_{g\in G} a_g g \mid \sum\limits_{g\in G} a_g = 0\}$, that is, the code of all even weight vectors in $\mathbb{F}G$.

3) $R(\rho,m)^\perp = R(m-\rho-1, m)$.

Since $R(m-1,m)^\perp = R(0,m)$ the problem of searching for information sets has no interest in the case $\rho = m-1$, so in the rest of the paper we will assume that $\rho < m-1$.

As a consequence of Definition 27 we have that the defining set of the punctured code $R^*(\rho,m)$, at the position X^0 and with respect to the fixed n-th root of unity α, is given by the following union of cyclotomic cosets modulo n

$$D(R^*(\rho,m)) = \bigcup_{i\in D(R(\rho,m))\setminus\{0\}} C_n(i).$$

In the following sections we will deal with the application of the results contained in Section IV to the cyclic code $R^*(\rho,m)$ in order to obtain an information set for $R(\rho,m)$. To use a notation congruent with that used in that section we write $\mathcal{D}^* = D(R^*(\rho,m))$. We assume that there exist integers r_1, r_2 such that $n = 2^m - 1 = r_1 \cdot r_2$ with r_1, r_2 odd and $\gcd(r_1, r_2) = 1$. Now, we fix some notation and introduce some definitions and important results that will be needed.

Remark 29. *Note that for any fixed primitive root of unity α, following the notation used to describe the elements in $\mathbb{F}G$, $\left(-\sum\limits_{i=0}^{n-1} a_i\right) X^0 + \sum\limits_{i=0}^{n-1} a_i X^{\alpha^i} \in \mathbb{F}G$, a set $\mathcal{I} \subseteq \{0, \alpha^0, \ldots, \alpha^{n-1}\}$ is an information set for a code $\mathcal{C} \subseteq \mathbb{F}G$ with dimension k, if $|\mathcal{I}| = k$ and $\mathcal{C}_\mathcal{I} = \mathbb{F}^{|\mathcal{I}|}$.*

On the other hand, since $R^*(\rho,m)$ is contained in $\mathbb{F}G^*$ we have that any information set for it will be a subset of $\{\alpha^0, \ldots, \alpha^{n-1}\}$. Obviously, an information set for $R^*(\rho,m)$ is an information set for $R(\rho,m)$ too. However, note that if Γ is a set of check positions for $R^*(\rho,m)$ then a set of check positions for $R(\rho,m)$ is $\Gamma \cup \{0\}$.

Now, we need to fix some notation. For any integer $0 < K < m-1$ we define

$$\Omega(K) \quad = \quad \{0 < j < 2^m - 1 \ \mid \ \mathrm{wt}(j) = K\} = \left\{2^{t_1} + \cdots + 2^{t_K} \ \mid \ 0 \leq t_1 < \cdots < t_K < m\right\}$$

and hence,

$$\mathcal{D}^* = \bigcup_{K=1}^{m-\rho-1} \{0 < j < 2^m - 1 \ \mid \ \mathrm{wt}(j) = K\} = \bigcup_{K=1}^{m-\rho-1} \Omega(K).$$

Example 30. *Take $m = 4$. Then $n = 2^4 - 1 = 15, r_1 = 3, r_2 = 5$. For these parameters one has that*

$$\Omega(1) = \{1,2,4,8\}, \Omega(2) = \{3,5,6,9,10,12\} \text{ and } \Omega(3) = \{7,11,13,14\}.$$

The code $R(1,4)$ has defining set $\mathcal{D}(R(1,4)) = \{0,1,2,3,4,5,6,8,9,10,12\}$ and so $\mathcal{D}^* = \mathcal{D}(R^*(1,4)) = \Omega(1) \cup \Omega(2) = \{1,2,3,4,5,6,8,9,10,12\}$.

Finally, the code $R(2,4)$ has defining set $\mathcal{D}(R(2,4)) = \{0,1,2,4,8\}$, which implies $\mathcal{D}^* = \mathcal{D}(R^*(2,4)) = \Omega(1)$.

Now, we take $\overline{\mathcal{D}^*}$ a suitable set of representatives in $\mathcal{D}^*$ and a set $\mathcal{U}$ as in the previous section (see Definition 14 and subsequent paragraphs).

We are interested in handling convenient elements in the fixed suitable set of representatives in order to compute the necessary cyclotomic cosets. We will describe them in Theorem 32. First, we need a lemma.

Lemma 31. *Let $j < i < K < m$ be natural numbers. Then*

1) $m - \left\lfloor \frac{im}{K} \right\rfloor = \left\lfloor \frac{(K-i)m}{K} \right\rfloor$ *or* $\left\lfloor \frac{(K-i)m}{K} \right\rfloor + 1$.

2) $\left\lfloor \frac{im}{K} \right\rfloor - \left\lfloor \frac{jm}{K} \right\rfloor = \left\lfloor \frac{(i-j)m}{K} \right\rfloor$ *or* $\left\lfloor \frac{(i-j)m}{K} \right\rfloor + 1$.

Proof. Let $\left\lfloor \frac{im}{K} \right\rfloor = \frac{im}{K} - \delta$ with $0 \leq \delta < 1$. Then

$$m - \left\lfloor \frac{im}{K} \right\rfloor = m - \frac{im}{K} + \delta = \frac{(K-i)m}{K} + \delta.$$

So, if $\delta = 0$ then $\left\lfloor \frac{(K-i)m}{K} \right\rfloor = m - \left\lfloor \frac{im}{K} \right\rfloor$, and if $\delta > 0$ then $\left\lfloor \frac{(K-i)m}{K} \right\rfloor = m - \left\lfloor \frac{im}{K} \right\rfloor - 1$. This proves *1)*.

Now, let $\left\lfloor \frac{jm}{K} \right\rfloor = \frac{jm}{K} - \delta'$ with $0 \leq \delta' < 1$. Then

$$\left\lfloor \frac{im}{K} \right\rfloor - \left\lfloor \frac{jm}{K} \right\rfloor = \frac{(i-j)m}{K} + \delta' - \delta.$$

Note that $-1 < \delta' - \delta < 1$. So, if $\delta \geq \delta'$ then $\left\lfloor \frac{(i-j)m}{K} \right\rfloor = \left\lfloor \frac{im}{K} \right\rfloor - \left\lfloor \frac{jm}{K} \right\rfloor$; otherwise, $\left\lfloor \frac{(i-j)m}{K} \right\rfloor = \left\lfloor \frac{im}{K} \right\rfloor - \left\lfloor \frac{im}{K} \right\rfloor - 1$. This finishes the proof. □

It is clear that if $e = 2^s \in \Omega(1)$, with $0 \leq s < m$, then $C_n(e) = C_n(1)$. The following theorem establishes a more general result for $\Omega(K)$ with $1 < K < m-1$.

Theorem 32. *Let $e = 2^{s_0} + 2^{s_1} + \cdots + 2^{s_{K-1}} \in \Omega(K)$ with $0 \leq s_0 < \cdots < s_{K-1} < m$ and $1 < K < m-1$. Then there exists*

$$e' = 1 + 2^{t_1} + \cdots + 2^{t_{K-1}}, \tag{10}$$

with $t_i \leq \left\lfloor \frac{im}{K} \right\rfloor$ for all $i = 1, \ldots, K-1$, such that $C_n(e) = C_n(e')$.

Proof. We can assume w.l.o.g. that $e = 1 + 2^{s_1} + 2^{s_2} + \cdots + 2^{s_{K-1}} \in \Omega(K)$ with $0 < s_1 < \cdots < s_{K-1} < m$ and $1 < K < m-1$. If e verifies the required conditions we are done, so suppose that e do not satisfies them and let δ_1, δ_2 be the integers such that

$$\begin{aligned} s_i &\leq \left\lfloor \tfrac{im}{K} \right\rfloor \qquad \text{for all} \quad i = 1, \ldots, \delta_1 - 1, \\ s_{\delta_1} &> \left\lfloor \tfrac{\delta_1 m}{K} \right\rfloor, \\ s_{K-i} &\leq \left\lfloor \tfrac{(K-i)m}{K} \right\rfloor \quad \text{for all} \quad i = 1, \ldots, \delta_2; \end{aligned}$$

and $K > \delta_1 + \delta_2$, that is, the binary expansion of e has at least $\delta_1 + \delta_2 - 1$ exponents satisfying the desired condition. Observe that $\delta_1 \geq 1, \delta_2 \geq 0$.

We define $u = m - s_{\delta_1}$ and consider $e' = 2^u e$ modulo n. Then, it is easy to see that $e' = 1 + 2^{s'_1} + \cdots + 2^{s'_{K-1}}$, with $0 < s'_1 < \cdots < s'_{K-1} < m$, where

$$s'_j \equiv s_{\delta_1 + j} + u \ (\text{ mod } m) \ \text{ if } \ j = 1, \ldots, K - \delta_1 - 1 \tag{11}$$

$$s'_{K-\delta_1} = u$$

$$s'_j = s_{\delta_1 + j - K} + u \ \text{ if } \ j = K - \delta_1 + 1, \ldots, K-1. \tag{12}$$

We claim that $s'_j \leq \left\lfloor \frac{jm}{K} \right\rfloor$ for any $j = K - (\delta_1 + \delta_2), \ldots, K-1$. Let us define $A = \{K - \delta_1 + 1, K - \delta_1 + 2, \ldots, K-1\}$ and $B = \{K - (\delta_1 + \delta_2), K - (\delta_1 + \delta_2) - 1, \ldots, K - \delta_1 - 1\}$, then $A \cup B \cup \{K - \delta_1\} = \{K - (\delta_1 + \delta_2), \ldots, K-1\}$. Note that in the cases $\delta_1 = 1$, $\delta_2 = 0$ one has that $A = \emptyset$, $B = \emptyset$ respectively.

On the one hand, by (12), one has that $s'_j = s_{\delta_1 + j - K} + u$ for any $j \in A$. Let us observe that $s_{\delta_1} - s_{\delta_1 - i} > \left\lfloor \frac{\delta_1 m}{K} \right\rfloor - \left\lfloor \frac{(\delta_1 - i)m}{K} \right\rfloor \geq \left\lfloor \frac{im}{K} \right\rfloor$ for any $i = 1 \ldots, \delta_1 - 1$ (see Lemma 31). Then,

$$s'_j = m - s_{\delta_1} + s_{\delta_1 - (K-j)} = m - (s_{\delta_1} - s_{\delta_1 - (K-j)}) < m - \left\lfloor \frac{(K-j)m}{K} \right\rfloor \leq \left\lfloor \frac{jm}{K} \right\rfloor + 1$$

(see Lemma 31), and so $s'_j \leq \left\lfloor \frac{jm}{K} \right\rfloor$ for any $j \in A$. Furthermore,

$$s'_{K-\delta_1} = u = m - s_{\delta_1} < m - \left\lfloor \frac{\delta_1 m}{K} \right\rfloor \leq \left\lfloor \frac{(K-\delta_1)m}{K} \right\rfloor + 1,$$

which implies $s'_{K-\delta_1} \leq \left\lfloor \frac{(K-\delta_1)m}{K} \right\rfloor$.

On the other hand, by (11), for any $j \in B$ we have that $s'_j \equiv s_{\delta_1+j} + u = m - s_{\delta_1} + s_{\delta_1+j} = m - (s_{\delta_1} - s_{\delta_1+j}) \bmod m$, so $s'_j = s_{\delta_1+j} - s_{\delta_1}$ (note that $s_{\delta_1+j} > s_{\delta_1}$). This leads us to

$$s'_j = s_{\delta_1+j} - s_{\delta_1} < \left\lfloor \frac{(\delta_1+j)m}{K} \right\rfloor - \left\lfloor \frac{\delta_1 m}{K} \right\rfloor \leq \left\lfloor \frac{jm}{K} \right\rfloor + 1,$$

and then $s'_j \leq \left\lfloor \frac{jm}{K} \right\rfloor$, so we are done.

Therefore, $e' = 2^u e$ satisfies that its binary expansion has at least $\delta_1 + \delta_2$ exponents verifying the desired condition, one more than in the case of e. If we repeat the argument successively by replacing e by e' then we get what we wanted. This finishes the proof. □

The previous result shows that for any element $e \in \Omega(K), 1 < K < m-1$, there exists another element $e' \in C_n(e)$ satisfying condition (10). As we will see in the next section, in the case $K = 2$, this fact becomes essential for our purposes. In addition, let us observe that the elements in a given suitable set of representatives might not satisfy condition (10); we include the next example to show that case.

Example 33. *Let us consider the Reed-Muller code $R(3,6)$. So $m = 6, n = 2^6 - 1 = 63, r_1 = 7, r_2 = 9$. For these parameters we have*

$$\Omega(1) = C_{63}(1) = \{1, 2, 4, 8, 16, 32\}$$

and

$$\Omega(2) = C_{63}(3) \cup C_{63}(5) \cup C_{63}(9) = \{3, 5, 6, 9, 10, 12, 17, 18, 20, 24, 33, 34, 36, 40, 48\}.$$

The defining set of $R^*(3,6)$ is $\mathcal{D}^* = \Omega(1) \cup \Omega(2)$. The set $\overline{\mathcal{D}^*} = \{1, 3, 10, 36\}$ is a suitable set of representatives according to Definition 14; however while 1 and 3 satisfy condition (10) the elements, $10 = 2 + 2^3$ and $36 = 2^2 + 2^5$ do not satisfy it. The reader may check that there does not exist any suitable set of representatives such that all its elements satisfy condition (10).

VI. Information sets for first-order Reed-Muller codes

In this section we are applying the results of Section IV to the punctured codes of first-order Reed-Muller codes. Specifically, we shall construct an information set for the punctured code $R^*(1,m)$ by using those techniques and then we shall give an information set for the Reed-Muller code $R(1,m)$. To use the mentioned results we need to assume that there exist odd integers r_1, r_2 such that $n = 2^m - 1 = r_1 \cdot r_2$ and $\gcd(r_1, r_2) = 1, r_1, r_2 > 1$.

All throughout this section we fix a primitive n-th root of unity α and $T : \mathbb{Z}_n \to \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$ an arbitrary isomorphism of groups.

We have two different possibilities to get an information set for the code $R(1,m)$; namely, from an information set of $R^*(1,m)$, which comes from the defining set of $R^*(1,m)$, and from a check of set positions of $R(1,m)^\perp = R(m-2,m)$, which depends on the defining set of $R^*(m-2,m)$. In general it is more convenient to develop the results in terms of $R^*(m-2,m)$ whose defining set is much smaller than that of $R^*(1,m)$.

Let us denote $\mathcal{C}^* = R^*(m-2,m)$. Then, following the notation fixed in the previous section, we have that

$$\mathcal{D}^* = \Omega(1)$$

where $\Omega(1) = \{2^t \mid 0 \leq t < m\}$. Observe that $\Omega(1) = C_n(1)$ so we take $\overline{\mathcal{D}^*} = \{1\}$ as our suitable set of representatives (see Definition 14). Then $\mathcal{U} = \{1\}$.

The following theorem gives us the description of an information set for the code $R(1,m)$. We denote by $\mathrm{Ord}_{r_1}(2)$ the order of 2 modulo r_1, that is, the smallest integer such that $2^{\mathrm{Ord}_{r_1}(2)} \equiv 1$ modulo r_1.

Theorem 34. *Suppose that $n = 2^m - 1 = r_1 \cdot r_2$, where r_1, r_2 are odd integers such that $\gcd(r_1, r_2) = 1, r_1, r_2 > 1$. Let $\mathcal{C}^* = R^*(m-2,m)$ and $a = \mathrm{Ord}_{r_1}(2)$. Let $\mathcal{D}^* \subseteq \mathbb{Z}_n$ be the defining set of $\mathcal{C}^*$ with respect to α, a primitive n-th root of unity, and let $\mathcal{C} \subseteq \mathbb{A}(r_1, r_2)$ be the abelian code with defining set $D(\mathcal{C}) = T(\mathcal{D}^*)$. Then, the set $T^{-1}(\Gamma)$ where*

$$\Gamma = \Gamma(\mathcal{C}) = \left\{ (i_1, i_2) \in \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \mid 0 \leq i_1 < a, 0 \leq i_2 < \frac{m}{a} \right\}$$

is a set of check positions for $R^*(m-2,m)$. Furthermore, $\{0, \alpha^i \mid i \in T^{-1}(\Gamma)\}$ is an information set for $R(1,m)$ and $\{\alpha^i \mid i \notin T^{-1}(\Gamma)\}$ is an information set for $R(m-2,m)$.

Proof. By definition $\mathcal{D}^* = \Omega(1)$. We take $\overline{\mathcal{D}^*} = \mathcal{U} = \{1\}$. To construct the set $\Gamma(\mathcal{C})$ given in (6) we need to compute the sequences (3) and (5). By the results in Section IV we have that those sequences are obtained from (8).

In this case, since $\overline{\mathcal{D}^*} = \mathcal{U} = \mathcal{O}(1) = \{1\}$, we have a unique value

$$M(1) = \frac{1}{|C_{r_1}(1)|} \cdot |C_n(1)| = \frac{m}{a}.$$

Note that $C_n(1) = \{1, 2, \ldots, 2^{m-1}\}$ and since r_1 divides n then a divides m. Then, the sequences (3) and (5) are

$$f_1 = \frac{m}{a} > f_2 = 0 \text{ and } g_1 = m(1) = a.$$

Therefore $\Gamma = \Gamma(\mathcal{C}) = \{(i_1, i_2) \in \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \text{ such that } f_2 \leq i_2 < f_1, 0 \leq i_1 < g_1\}$.

Finally, by Theorem 9, Γ is a set of check positions for $\mathcal{C}$, and then $T^{-1}(\Gamma)$ is a set of check positions for $R^*(m-2, m)$. So, $\{0, \alpha^i \mid i \in T^{-1}(\Gamma))\}$ is a set of check positions for $R(m-2, m)$ (see Remark 29). Since $R(m-2, m) = R(1, m)^{\perp}$ we are done. □

Examples 35. *The first value for m that satisfies the required conditions is $m = 4$. In this case, $n = 2^4 - 1 = 15, r_1 = 3, r_2 = 5, \mathrm{Ord}_3(2) = 2$. So, let us give an information set for $R(1, 4)$. By Theorem 34 we have that*

$$\Gamma = \{(i_1, i_2) \in \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \mid 0 \leq i_1 < 2, 0 \leq i_2 < 2\} = \{(0,0), (1,0), (0,1), (1,1)\}.$$

Then, by taking the isomorphism given by the Chinese Remainder Theorem, we have that $T^{-1}(\Gamma) = \{0, 1, 6, 10\}$ and then $\{0, 1, \alpha, \alpha^6, \alpha^{10}\}$ is an information set for $R(1, 4)$. Moreover $\{\alpha^i \mid i \neq 0, 1, 6, 10\}$ is an information set for $R(2, 4)$. Table I shows the different information sets that we can get by using all the possible isomorphisms from $\mathbb{Z}_{15}$ to $\mathbb{Z}_3 \times \mathbb{Z}_5$; the first column includes the image of $1 \in \mathbb{Z}_{15}$ which determines the corresponding isomorphism, while the second column gives the set of exponents I such that $\{0, \alpha^i \mid i \in I\}$ is an information set for $R(1, 4)$.

T(1)	I
(1,1)	{0,1,6,10}
(2,1)	{0,3,5,8}
(1,2)	{0,3,10,13}
(2,2)	{0,6,8,10}
(1,3)	{0,7,10,12}
(2,3)	{0,2,5,12}
(1,4)	{0,4,9,10}
(2,4)	{0,5,9,14}

TABLE I
INFORMATION SETS FOR R(1,4)

The next value for m is $m = 6$. In this case, $n = 2^6 - 1 = 63, r_1 = 7, r_2 = 9, a = 3$. So

$$\Gamma = \{(i_1, i_2) \in \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \text{ such that } 0 \leq i_1 < 3, 0 \leq i_2 < 2\} = \{(0,0), (1,0), (2,0), (0,1), (1,1), (2,1)\}.$$

Since $T^{-1}(\Gamma) = \{0, 1, 9, 28, 36, 37\}$ one has that $\{0, 1, \alpha, \alpha^9, \alpha^{28}, \alpha^{36}, \alpha^{37}\}$ is an information set for $R(1, 6)$ and $\{\alpha^i \mid i \neq 0, 1, 9, 28, 36, 37\}$ is an information set for $R(4, 6)$. Again, we have taken the isomorphism given by the Chinese Remainder Theorem

Finally, let us see the case $m = 8$, that is, the Reed-Muller codes of length 256. This is an interesting case because we have three possible decompositions of $n = 2^8 - 1 = 255$, namely, $(r_1 = 3, r_2 = 85)$, $(r_1 = 5, r_2 = 51)$ and $(r_1 = 15, r_2 = 17)$. Table II shows the sets $T^{-1}(\Gamma)$ obtained for each decomposition; in all cases we are considering the isomorphism given by the Chinese Remainder Theorem.

r_1	r_2	a	$T^{-1}(\Gamma)$
3	85	2	{0,1,3,85,87,88,171,172}
5	51	4	{0,1,51,52,102,103,153,205}
15	17	4	{0,1,17,18,120,136,137,153}

TABLE II
INFORMATION SETS FOR R(6,8)

To finish this section, we include Table III which shows the suitable values of m up to length 2048. The values $m = 2, 3, 5, 7$ yield a prime number for $n = 2^m - 1$.

VII. INFORMATION SETS FOR SECOND-ORDER REED-MULLER CODES

In this section we deal with second-order Reed-Muller codes. As in the previous section, we shall apply the results of Section IV, so we need to assume that there exist integers r_1, r_2 such that $n = 2^m - 1 = r_1 \cdot r_2$ and $\gcd(r_1, r_2) = 1, r_1, r_2 > 1$. Once more, we fix a primitive n-th root of unity α and $T : \mathbb{Z}_n \to \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$ an arbitrary isomorphism of groups.

In a similar way to the case of $R(1, m)$, we have two possibilities to get an information set for the code $R^*(2, m)$. Again, we prefer to develop the results in terms of $R^*(m-3, m)$ which yields an information set for $R(m-3, m) = R(2, m)^{\perp}$.

$\mathbf{m}$	$\mathbf{n}$	$\mathbf{r_1}$	$\mathbf{r_2}$	$\mathbf{a}$
4	15	3	5	2
6	63	7	9	3
8	255	3	85	2
8	255	15	17	4
8	255	5	51	4
9	511	7	73	3
10	1023	3	341	2
10	1023	11	93	10
10	1023	31	33	5
11	2047	23	89	11

TABLE III
PARAMETERS FOR FIRST ORDER RM CODES UP TO LENGTH 2048

Throughout this section we denote $\mathcal{C}^* = R^*(m-3, m)$. In this case we have that

$$\mathcal{D}^* = \Omega(1) \cup \Omega(2)$$

where $\Omega(1) = \{2^t \mid 0 \leq t < m\}$ and $\Omega(2) = \{2^{t_1} + 2^{t_2} \mid 0 \leq t_1 < t_2 < m\}$. Let $\overline{\mathcal{D}^*} \subseteq \mathcal{D}^*$ be a suitable set of representatives and take $\mathcal{U} \subseteq \overline{\mathcal{D}^*}$ a complete set of representatives of the equivalence classes modulo r_1 (see (7)). We will always assume that $1 \in \mathcal{U} \subseteq \overline{\mathcal{D}^*}$ (recall that $\Omega(1) = C_n(1)$).

To get the expressions (8) we need to compute the cardinalities $|C_n(e)|$, for all $e \in \overline{\mathcal{D}^*}$, and $|C_{r_1}(u)|$ for any element u in the fixed set $\mathcal{U}$. As we have seen in the previous section, these computations can be made directly in the case of elements in $\Omega(1)$, however, they turn to be much more complicated when we work with the set $\Omega(2)$. So, we impose some conditions on r_1 in order to make the mentioned computations possible, namely, all throughout we also assume that $r_1 = 2^a - 1$, with a an integer. Then, we can sum up the restrictions on the paremeters as follows

$$n = 2^m - 1 = r_1 \cdot r_2, \text{ where } r_1 = 2^a - 1 \text{ and } \gcd(r_1, r_2) = 1, r_1, r_2 > 1. \tag{13}$$

Note that from these conditions it follows that $a = \mathrm{Ord}_{r_1}(2)$ and so the notation is consistent with that used in Theorem 34. In what follows we write $m = ab$.

The first lemma, probably a well-known result, shows that the value of the cardinalities $|C_n(e)|$ and $|C_{r_1}(e)|$ can be easily computed for the elements in $\Omega(2)$ of the form $1 + 2^t$.

Lemma 36. *Let μ, ν integers such that $\mu = 2^\nu - 1$. Then $|C_\mu(1)| = \nu$ and for any natural number $0 < t \leq \nu - 1$*

$$\left|C_\mu\left(1 + 2^t\right)\right| = \begin{cases} \dfrac{\nu}{2} & \textit{in case} \quad t = \dfrac{\nu}{2} \\ \\ \nu & \textit{otherwise} \end{cases}$$

Proof. The equality $|C_\mu(1)| = \nu$ is clear. To see the second one, denote $\delta = |C_\mu(1 + 2^t)|$. Then $2^\delta \cdot (1+2^t) = 2^\delta + 2^{\delta+t} \equiv 1 + 2^t$ modulo μ. So, either $\delta = \nu$ (and $\delta + t \equiv t \bmod \nu$) or $\delta + t = \nu$ and $\delta = t$. The second condition implies $\delta = t = \nu/2$. □

As we have observed in the previous section the elements in the suitable set $\overline{\mathcal{D}^*}$ might not satisfy condition (10). However, we can relate any element in $\overline{\mathcal{D}^*}$ with another one in the same 2-cyclotomic coset modulo n that satisfies that condition (see Theorem 32). The following result details this relationship.

Proposition 37. *Let $\overline{\mathcal{D}^*}$ be a suitable set of representatives. There exists a bijection $\varepsilon : \overline{\mathcal{D}^*} \setminus \{1\} \longrightarrow \{s \in \mathbb{Z} \mid 1 \leq s \leq \lfloor \frac{m}{2} \rfloor\}$ where, for any $e \in \overline{\mathcal{D}^*} \setminus \{1\}$, $\varepsilon(e)$ is the unique integer such that $1 + 2^{\varepsilon(e)}$ belongs to $C_n(e)$ and satisfies condition (10).*

Proof. By Theorem 32, for any $e \in \overline{\mathcal{D}^*} \setminus \{1\}$ there exists $e' = 1 + 2^s$, where $0 < s \leq \lfloor \frac{m}{2} \rfloor$, such that $C_n(e') = C_n(e)$. We define $\varepsilon(e) = s$ and we are going to prove that e' is unique in $C_n(e)$ satisfying condition (10).

Suppose that exists $e'' = 1 + 2^{s'} \in C_n(e)$, $e'' \neq e'$, satisfying the required condition. Then there must exist $v \in \{1, \ldots, m-1\}$ such that $e'' \equiv 2^v e' \equiv 2^v + 2^{v+s} \bmod n$. Necessarily this implies $v + s = m, v = s'$. So, $s' = m - s \geq m - \lfloor m/2 \rfloor \geq \lfloor m/2 \rfloor$; since $e'' \neq e'$ then $s' > \lfloor m/2 \rfloor$, a contradiction. So, we can say that ε is well-defined. Now, for any $s \in \{1, \ldots, \lfloor \frac{m}{2} \rfloor\}$ the element $1 + 2^s$ belongs to $\Omega(2)$ and so there exists $e \in \overline{\mathcal{D}^*} \setminus \{1\}$ such that $C_n(e) = C_n(1 + 2^s)$. Moreover, if $e \neq e' \in \overline{\mathcal{D}^*}$ then $C_n(e) \neq C_n(e')$ and so $\varepsilon(e) \neq \varepsilon(e')$. This implies that ε is a bijection. □

Remark 38. *Observe that for all $e = 2^{t_1} + 2^{t_2} \in \Omega(2)$ one has that $1 + 2^\delta$, with $\delta = \min\{t_2 - t_1, m - t_2 + t_1\}$, belongs to $C_n(e)$ and verifies (10), therefore $\varepsilon(e) = \min\{t_2 - t_1, m - t_2 + t_1\}$.*

Under the notation introduced by Proposition 37 we can say that for any $e \in \Omega(2)$ the element $1 + 2^{\varepsilon(e)}$ is the unique element in $C_n(e)$ satisfying condition (10).

Now, from Proposition 37 and Lemma 36 we obtain the next result which gives us the desired cardinalities.

Proposition 39. *Let $n = 2^m - 1 = r_1 \cdot r_2$ satisfying (13), that is, $m = ab$, with a such that $r_1 = 2^a - 1$ and $(r_1, n/r_1) = 1$. For any $e \in \Omega(2)$ one has that*

1) $|C_n(e)| = \begin{cases} \dfrac{m}{2} & \text{in case} \quad \varepsilon(e) = \dfrac{m}{2} \\ m & \text{otherwise} \end{cases}$

2) $|C_{r_1}(e)| = \begin{cases} \dfrac{a}{2} & \text{in case} \quad \varepsilon(e) \equiv \dfrac{a}{2} \bmod a \\ a & \text{otherwise} \end{cases}$

Proof. Let $e = 2^{t_1} + 2^{t_2} \in \Omega(2)$ and $e' = 1 + 2^{\varepsilon(e)}$. Then $C_n(e) = C_n(e')$. Moreover $\varepsilon(e) = t_2 - t_1$ or $\varepsilon(e) = m - (t_2 - t_1)$ (see Remark 38). By Lemma 36 $|C_n(e')| = m/2$ if $\varepsilon(e) = m/2$ and $|C_n(e')| = m$ otherwise, which yields *1)*.

To prove *2)* note that there exists an integer $v \in \{0, \ldots, m-1\}$ such that $e' \equiv 2^v e$ modulo n. Since $n = r_1 \cdot r_2$ we have that $e' \equiv 2^v e$ modulo r_1. Then $C_{r_1}(e) = C_{r_1}(e')$ and so $|C_{r_1}(e)| = |C_{r_1}(e')|$. Note also that $e' \equiv 1 + 2^\mu \bmod r_1$ where μ is the residue of $\varepsilon(e)$ modulo a. By Lemma 36 $|C_{r_1}(e')| = a/2$ if $\varepsilon(e) \equiv a/2 \bmod a$ and $|C_{r_1}(e')| = a$ otherwise. Finally, observe that if $\varepsilon(e) \equiv 0 \bmod a$ then $e' \in C_{r_1}(1)$ and so $|C_{r_1}(e')| = |C_{r_1}(1)| = a$. This finishes the proof. □

Now, all that is required to obtain the expressions (8) is the description of the sets $\mathcal{O}(u)$ with $u \in \mathcal{U}$, that is, $\mathcal{O}(1)$ and $\mathcal{O}(e)$ with $e \in \Omega(2) \cap \mathcal{U}$. The next results solve this problem. The first one gives the information we need about $\mathcal{O}(1)$. Recall that all throughout $\overline{\mathcal{D}^*}$ denotes a suitable set of representatives.

Proposition 40. *1)* $\mathcal{O}(1) = \{1\} \cup \{e \in \overline{\mathcal{D}^*} \mid \varepsilon(e) = \lambda a$ *with* $1 \leq \lambda \leq \lfloor \frac{b}{2} \rfloor\}$.
2) $|\mathcal{O}(1)| = 1 + \lfloor b/2 \rfloor$.
3) If b is even then $\varepsilon^{-1}(m/2) \in \mathcal{O}(1)$, $\left|C_n(\varepsilon^{-1}(m/2))\right| = m/2$, *and* $|C_n(e)| = m$ *for any* $e \in \mathcal{O}(1) \setminus \{\varepsilon^{-1}(m/2)\}$.
4) If b is odd then $|C_n(e)| = m$ *for any* $e \in \mathcal{O}(1)$.

Proof. Let $e \in \overline{\mathcal{D}^*}, e \neq 1$, such that $e \equiv 1 \bmod r_1$. Then $C_{r_1}(1 + 2^{\varepsilon(e)}) = C_{r_1}(e) = C_{r_1}(1)$. Let μ be the residue of $\varepsilon(e)$ modulo a, then $C_{r_1}(1 + 2^{\varepsilon(e)}) = C_{r_1}(1 + 2^\mu) = C_{r_1}(1)$. So $1 + 2^\mu$ and 1 are different elements in $\{1, \ldots, r_1 - 1\}$ that belongs to the same 2-cyclotomic coset modulo r_1; this is only possible in the case $\mu = 0$. Therefore $\varepsilon(e) \equiv 0 \bmod a$. Let $\varepsilon(e) = \lambda a$ with λ a natural number. It is easy to see that this implies $1 \leq \lambda \leq \lfloor \frac{b}{2} \rfloor$ because $\varepsilon(e) \leq \lfloor \frac{m}{2} \rfloor$ (recall that $n = 2^m - 1$ where $m = ab$). Conversely, if $e \in \overline{\mathcal{D}^*}$ and $\varepsilon(e) = \lambda a$ then $C_{r_1}(e) = C_{r_1}(1 + 2^{\lambda a}) = C_{r_1}(2) = C_{r_1}(1)$. Since $\overline{\mathcal{D}^*}$ is a suitable set of representatives we conclude that $e \equiv 1$ modulo r_1. This proves *1)*.

Statement *2)* is immediate from *1)* and Proposition 37.

Now, suppose that b is even. Then $\frac{m}{2} = a \cdot \frac{b}{2}$, so $\varepsilon^{-1}(m/2) \in \mathcal{O}(1)$ by *1)*. The last part of *3)* follows from Proposition 39.

Finally, suppose that b is odd. Then, in case m even, $\frac{m}{2} \equiv \frac{a}{2}$ modulo a, so $\varepsilon^{-1}(m/2) \notin \mathcal{O}(1)$. Therefore, $|C_n(e)| = m$ for any $e \in \mathcal{O}(1)$ by Proposition 39. This finishes the proof. □

Remark 41. *As we have already seen we assume that $1 \in \mathcal{U} \subseteq \overline{\mathcal{D}^*}$. Furthermore, depending on the parity of a and b we will take the following elements in $\mathcal{U}$ by convention:*

1) If m is even we also assume that $\varepsilon^{-1}(m/2) \in \mathcal{U}$ unless $\varepsilon^{-1}(m/2) \in \mathcal{O}(1)$.
2) If a is even we assume that $\varepsilon^{-1}(a/2) \in \mathcal{U}$ unless $\varepsilon^{-1}(a/2) \in \mathcal{O}(\varepsilon^{-1}(m/2))$. Observe that $\varepsilon^{-1}(a/2)$ never belongs to $\mathcal{O}(1)$.

The next result yields the description of the set $\mathcal{O}(e)$ for any $e \in \mathcal{U} \setminus \{1\}$. Let us observe that $e \in \mathcal{U} \setminus \{1\}$ implies $e \in \mathcal{U} \cap \Omega(2)$.

Proposition 42. *Let $e \in \mathcal{U} \setminus \{1\}$. Then* $\mathcal{O}(e) = \{e' \in \overline{\mathcal{D}^*} \mid \varepsilon(e') \equiv \varepsilon(e)$ *mod* a or $\varepsilon(e') \equiv a - \varepsilon(e)$ *mod* $a\}$.

Proof. Let $e' \in \overline{\mathcal{D}^*}$ such that $e' \equiv e \bmod r_1$. Then $C_{r_1}(1 + 2^{\varepsilon(e)}) = C_{r_1}(1 + 2^{\varepsilon(e')})$. Let μ and μ' be the residues of $\varepsilon(e)$ and $\varepsilon(e')$ modulo a respectively. So $C_{r_1}(1 + 2^\mu) = C_{r_1}(1 + 2^{\mu'})$, that is, $1 + 2^\mu$ and $1 + 2^{\mu'}$ are elements in $\{1, \ldots, r_1 - 1\}$ that belong to the same 2-cyclotomic coset modulo r_1. This is only possible in the cases $\mu = \mu'$ or $\mu = a - \mu'$.

Conversely, suppose that $e' \in \overline{\mathcal{D}^*}$ and $\varepsilon(e') \equiv \varepsilon(e)$ modulo a. Then, $C_{r_1}(e) = C_{r_1}(1 + 2^{\varepsilon(e)}) = C_{r_1}(1 + 2^{\varepsilon(e')}) = C_{r_1}(e')$. Since $\overline{\mathcal{D}^*}$ is a suitable set of representatives this implies $e' \equiv e$ modulo r_1. Finally if $e' \in \overline{\mathcal{D}^*}$ and $\varepsilon(e') \equiv a - \varepsilon(e)$ modulo a we have the following sequence of equalities: $C_{r_1}(e') = C_{r_1}(1 + 2^{\varepsilon(e')}) = C_{r_1}(1 + 2^{a - \varepsilon(e)}) = C_{r_1}(1 + 2^{\varepsilon(e)}) = C_{r_1}(e)$. Again, we conclude that $e' \equiv e$ modulo r_1. So we are done. □

The following propositions complete the information about the sets $\mathcal{O}(e)$, with $e \in \mathcal{U} \setminus \{1\}$, by making a distinction between the cases b even and b odd ($m = ab$).

Proposition 43. *Let $e \in \mathcal{U} \setminus \{1\}$ and suppose that b is even. Then*

1) For any $e' \in \mathcal{O}(e)$ one has that $|C_n(e')| = m$.
2) If a is odd then $|\mathcal{O}(e)| = b$ and $|C_{r_1}(e)| = a$.
3) If a is even then in case $e = \varepsilon^{-1}(a/2)$ one has that $|\mathcal{O}(e)| = b/2$, $|C_{r_1}(e)| = a/2$ and otherwise $|\mathcal{O}(e)| = b$, $|C_{r_1}(e)| = a$.

Proof: First of all note that since b is even then $\frac{m}{2} \equiv a$ modulo a which implies $\varepsilon^{-1}(m/2) \in \mathcal{O}(1)$ (see Proposition 40), so $e' \neq \varepsilon^{-1}(m/2)$ for all $e' \in \mathcal{O}(e)$. This proves *1)* by Proposition 39.

In the rest of proof we denote by μ the residue of $\varepsilon(e)$ modulo a. Observe that $\mu \neq 0$ because $e \in \mathcal{U} \setminus \{1\}$. Let us define $A = \{e' \in \overline{\mathcal{D}^*} \mid \varepsilon(e') \equiv \varepsilon(e) \bmod a\}$ and $B = \{e' \in \overline{\mathcal{D}^*} \mid \varepsilon(e') \equiv a - \varepsilon(e) \bmod a\}$. By Proposition 42, $\mathcal{O}(e) = A \cup B$. Note also that $A \cap B \neq \emptyset$ if and only if $\mu = a/2$, that is, if and only if $\mathcal{O}(e) = A = B = A \cap B$.

Now we write $A = \{e' \in \overline{\mathcal{D}^*} \mid \varepsilon(e') = \lambda a + \mu, \text{ with } \lambda \text{ a natural number}\}$. To get the cardinality of A we need to study the range of values of λ. By definition of ε one has that $1 \leq \varepsilon(e') \leq \left\lfloor \frac{m}{2} \right\rfloor$, and since

$$\frac{b}{2}a + \mu = \frac{m}{2} + \mu > \frac{m}{2} \geq \left\lfloor \frac{m}{2} \right\rfloor$$

and

$$\left(\frac{b}{2} - 1\right)a + \mu = \frac{m}{2} - a + \mu < \frac{m}{2},$$

we conclude that $|A| = \left|\{\lambda \in \mathbb{Z} \mid 0 \leq \lambda < \frac{b}{2}\}\right| = b/2$. An analogous argument yields $|B| = b/2$.

To prove *2)* we assume that a is odd. Then, $|\mathcal{O}(e)| = |A| + |B|$, that is, $|\mathcal{O}(e)| = \frac{b}{2} + \frac{b}{2} = b$. The equality $|C_{r_1}(e)| = a$ follows from Proposition 39.

Finally, we suppose that a is even. Then $\varepsilon^{-1}(a/2) \in \mathcal{U}$ (see Remark 41). If $e = \varepsilon^{-1}(a/2)$ then $|\mathcal{O}(e)| = |A| = b/2$ and $|C_{r_1}(e)| = a/2$. If $e \neq \varepsilon^{-1}(a/2)$ then, by repeating the arguments of the previous paragraph, we obtain $|\mathcal{O}(e)| = b$ and $|C_{r_1}(e)| = a$. ■

Proposition 44. *Let $e \in \mathcal{U} \setminus \{1\}$ and suppose that b is odd. Then $|C_n(e')| = m$ for all $e' \in \mathcal{O}(e) \setminus \{e\}$ and*

1) If a is odd then $|\mathcal{O}(e)| = b$, $|C_{r_1}(e)| = a$ and $|C_n(e)| = m$.
2) If a is even then
  a) If $e = \varepsilon^{-1}(m/2)$ then $|\mathcal{O}(e)| = (b+1)/2$, $|C_n(e)| = m/2$ and $|C_{r_1}(e)| = a/2$.
  b) If $e \neq \varepsilon^{-1}(m/2)$ then $|\mathcal{O}(e)| = b$, $|C_n(e')| = m$ and $|C_{r_1}(e)| = a$.

Proof:

We denote by μ the residue of $\varepsilon(e)$ modulo a ($\mu > 0$). We are going to use a similar technique to that was used in the proof of the previous proposition. We define $A = \{e' \in \overline{\mathcal{D}^*} \mid \varepsilon(e') \equiv \varepsilon(e) \bmod a\}$ and $B = \{e' \in \overline{\mathcal{D}^*} \mid \varepsilon(e') \equiv a - \varepsilon(e) \bmod a\}$. Then $\mathcal{O}(e) = A \cup B$. Observe that $A \cap B \neq \emptyset$ if and only if $\mu = a/2$ if and only if $\mathcal{O}(e) = A = B = A \cap B$. Then

$$\left\lfloor \frac{b}{2} \right\rfloor a + \mu = \frac{b-1}{2}a + \mu = \frac{m}{2} - \frac{a}{2} + \mu \ ;$$

this value is less than or equal to $\left\lfloor \frac{m}{2} \right\rfloor$ if and only if $\mu \leq \left\lfloor \frac{a}{2} \right\rfloor$. So $|A| = \left|\{0 \leq \lambda \leq \left\lfloor \frac{b}{2} \right\rfloor\}\right| = \left\lfloor \frac{b}{2} \right\rfloor + 1$ in case $\mu \leq \left\lfloor \frac{a}{2} \right\rfloor$ and $|A| = \left|\{0 \leq \lambda < \left\lfloor \frac{b}{2} \right\rfloor\}\right| = \left\lfloor \frac{b}{2} \right\rfloor$ otherwise.

To compute the cardinality of B we observe that

$$\left\lfloor \frac{b}{2} \right\rfloor a + a - \mu = \frac{b-1}{2}a + a - \mu = \frac{m}{2} + \frac{a}{2} - \mu.$$

It is easy to see that this value is less than or equal to $\left\lfloor \frac{m}{2} \right\rfloor$ if and only if $\mu \geq \left\lceil \frac{a}{2} \right\rceil$. Then $|B| = \left\lfloor \frac{b}{2} \right\rfloor + 1$ in case $\mu \geq \left\lceil \frac{a}{2} \right\rceil$ and $|B| = \left\lfloor \frac{b}{2} \right\rfloor$ otherwise.

Now, suppose that a is odd. Then

$$\left\lceil \frac{a}{2} \right\rceil = \frac{a}{2} + \frac{1}{2}, \ \left\lfloor \frac{a}{2} \right\rfloor = \frac{a}{2} - \frac{1}{2}$$

and so $\mu \leq \left\lfloor \frac{a}{2} \right\rfloor$ if and only if $\mu < \left\lceil \frac{a}{2} \right\rceil$. Therefore, $|\mathcal{O}(e)| = |A| + |B| = 2\left\lfloor \frac{b}{2} \right\rfloor + 1 = b$. On the other hand, since a and m are odd, for all $e' \in \mathcal{O}(e)$ one has that $|C_n(e')| = m, |C_{r_1}(e')| = a$, by Proposition 39. This proves *1)*.

Finally, suppose that a is even. Note that since b is odd we have $\frac{m}{2} \equiv \frac{a}{2}$ modulo a, so $\varepsilon^{-1}(m/2) \in \mathcal{U}$ and $\varepsilon^{-1}(a/2) \in \mathcal{O}(\varepsilon^{-1}(m/2))$ (see Remark 41 and Proposition 42).

First, assume that $e = \varepsilon^{-1}(m/2)$. Then $\mu = a/2$ and $|\mathcal{O}(e)| = |A| = |B| = \left\lfloor \frac{b}{2} \right\rfloor + 1 = (b+1)/2$. Moreover, we have $|C_{r_1}(e)| = a/2, |C_n(e)| = m/2$ and $|C_n(e')| = m$ for any $e' \in \mathcal{O}(e) \setminus \{e\}$. This proves *2 a)*.

In the case $e \neq \varepsilon^{-1}(m/2)$ we have that $\mu \neq \frac{a}{2}$ because $e, \varepsilon^{-1}(m/2) \in \mathcal{U}$ and they satisfy $C_{r_1}(e) = C_{r_1}(1 + 2^{\mu})$ and $C_{r_1}(\varepsilon^{-1}(m/2)) = C_{r_1}(1 + 2^{a/2})$. Note that $\mu \neq \frac{a}{2}$ implies again $\mu \leq \left\lfloor \frac{a}{2} \right\rfloor = \frac{a}{2}$ if and only if $\mu < \left\lceil \frac{a}{2} \right\rceil = \frac{a}{2}$. So $|\mathcal{O}(e)| = |A| + |B| = 2\left\lfloor \frac{b}{2} \right\rfloor + 1 = b$. In addition, $|C_{r_1}(e)| = a$ and $|C_n(e')| = m$ for all $e' \in \mathcal{O}(e)$. ■

The last result we need before enunciating our main theorem gives us the cardinality of any choice of the set $\mathcal{U}$. It uses the mentioned concept of 2-weight of an integer (see paragraph before Definition 27). We talk about the 2-weight of a 2-cyclotomic coset when one of its elements (and so all of them) has that 2-weight.

Lemma 45. *For any election of the set of representatives $\mathcal{U}$ one has that*

$$|\mathcal{U}| = 1 + |\{C_{r_1}(e) \mid e \in \mathcal{U} \cap \Omega(2)\}| = 1 + \lfloor a/2 \rfloor .$$

Proof. First of all, as we have noted in Remark 41 we always assume that $1 \in \mathcal{U}$, so we restrict our attention to the cardinality of $\mathcal{U} \setminus \{1\}$. We define a map

$$\varphi : \mathcal{U} \setminus \{1\} \to \{C_{r_1}(e) \mid e \in \mathcal{U} \cap \Omega(2)\}$$

given by $\varphi(e) = C_{r_1}(e)$. We are going to see that φ is a bijection.

Let $e \in \mathcal{U} \setminus \{1\}$. Then $C_{r_1}(e) = C_{r_1}(1+2^{\varepsilon(e)})$. Note that, by Proposition 40, the case $\varepsilon(e) \equiv 0$ modulo a implies $e \in \mathcal{O}(1)$ which yields a contradiction, so $C_{r_1}(e)$ is a coset of weight 2 and φ is well-defined.

Now, let $e', e \in \mathcal{U} \setminus \{1\}, e \neq e'$. By the definitions of suitable set of representatives and $\mathcal{U}$ we have that $C_{r_1}(e) \neq C_{r_1}(e')$, so φ is injective. Take $C_{r_1}(e)$ such that $e \in \mathcal{U} \cap \Omega(2)$. Then $e \neq 1$ because $e \in \Omega(2)$, so $C_{r_1}(e) = \varphi(e)$ which implies that φ is surjective.

Finally, to see the right hand equality take any integer $s \in \{1, \ldots, \lfloor \frac{a}{2} \rfloor\}$. Then $1+2^s \in \Omega(2) \subset \mathcal{D}^*$. Since $T_1(1+2^s) = 1+2^s$ and $T(\overline{\mathcal{D}^*})$ is a restricted set of representatives, there exists $e \in \overline{\mathcal{D}^*} \cap \Omega(2)$ such that $C_{r_1}(e) = C_{r_1}(1+2^s)$; moreover, in case $e \notin \mathcal{U}$, there must exist $u \in \mathcal{U} \setminus \{1\}$ such that $u \equiv e \bmod r_1$ and then $C_{r_1}(u) = C_{r_1}(e) = C_{r_1}(1+2^s)$. Finally, if $u \in \mathcal{U} \cap \Omega(2)$ then there exists $s_u \in \{1, \ldots, \lfloor \frac{a}{2} \rfloor\}$ such that $1 + 2^{s_u} \in C_{r_1}(u)$, and if $u \neq u'$ then $s_u \neq s_{u'}$ because $T(\overline{\mathcal{D}^*})$ is a restricted set of representatives. This finishes the proof. □

Now, we can present the main result for second-order Reed-Muller codes.

Theorem 46. *Let $\mathcal{C}^* = R^*(m-3, m)$. Suppose that $n = 2^m - 1 = r_1 \cdot r_2$, where $m = ab$, $r_1 = 2^a - 1$ and $\gcd(r_1, r_2) = 1, r_1, r_2 > 1$. Let $\mathcal{D}^* \subseteq \mathbb{Z}_n$ be the defining set of $\mathcal{C}^*$, with respect to α, a primitive n-th root of unity, and $\mathcal{C} \subseteq \mathbb{A}(r_1, r_2)$ the abelian code with defining set $D(\mathcal{C}) = T(\mathcal{D}^*)$. Then, the values of f_i and g_i from (3) and (5) are*

$$f_1 = b^2, f_2 = \frac{b(b+1)}{2} \quad \text{and} \quad g_1 = \frac{a(a-1)}{2}, g_2 = \frac{a(a+1)}{2},$$

respectively.

Therefore the set $T^{-1}(\Gamma)$ where $\Gamma = \Gamma(\mathcal{C}) = \{(i_1, i_2) \in \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$ such that

$$\left.\begin{array}{l} 0 \leq i_1 < \dfrac{a(a-1)}{2} \ \text{ and } \ 0 \leq i_2 < b^2 \\ \\ \text{or} \\ \\ \dfrac{a(a-1)}{2} \leq i_1 < \dfrac{a(a+1)}{2} \ \text{ and } \ 0 \leq i_2 < \dfrac{b(b+1)}{2} \end{array}\right\}$$

is a set of check positions for $R^*(m-3, m)$. Furthermore, $\{0, \alpha^i \mid i \in T^{-1}(\Gamma)\}$ is an information set for $R(2, m)$ and $\{\alpha^i \mid i \notin T^{-1}(\Gamma)\}$ is an information set for $R(m-3, m)$.

Proof: Let $\mathcal{C} \subseteq \mathbb{A}(r_1, r_2)$ be the abelian code with defining set $D(\mathcal{C}) = T(\mathcal{D}^*)$. In order to get the set $\Gamma(\mathcal{C})$ we are going to compute the sequences (3) and (5) by using the expressions (8). To do that we have to study different cases depending on the parity of a and b respectively. As we will see, in any case we will obtain the same set of check positions.

- Case m odd (a, b odd).

  Take $1 \in \mathcal{U}$. By applying Proposition 40 we have that

  $$M(1) = \frac{1}{|C_{r_1}(1)|} \sum_{v \in \mathcal{O}(1)} |C_n(v)| = \frac{1}{a} \sum_{v \in \mathcal{O}(1)} |C_n(v)| = \frac{1}{a} \cdot m \cdot \left(\left\lfloor \frac{b}{2} \right\rfloor + 1 \right) = b \cdot \frac{b+1}{2} = \frac{b(b+1)}{2}.$$

  For any $e \in \mathcal{U} \setminus \{1\}$ we use Proposition 44 *1)* and we obtain

  $$M(e) = \frac{1}{|C_{r_1}(e)|} \sum_{v \in \mathcal{O}(e)} |C_n(v)| = \frac{1}{a} \cdot m \cdot b = b^2.$$

  Therefore $f_1 = b^2 > f_2 = \frac{b(b+1)}{2}$. By definition, the sequence $g_1 < g_2$ is obtained as follows

  $$g_1 = \sum_{M(v) = f_1} |C_{r_1}(v)| = a \cdot |\mathcal{U} \setminus \{1\}| = a \cdot \left\lfloor \frac{a}{2} \right\rfloor = a \cdot \frac{a-1}{2},$$

and

$$g_2 = \sum_{M(v)\geq f_2} |C_{r_1}(v)| = a\cdot|\mathcal{U}| = a\cdot\frac{a+1}{2},$$

where we have used Lemma 45.

- Case a odd and b even. In this case $\varepsilon^{-1}(m/2)\in\mathcal{O}(1)$ (see Proposition 40 *4)*).
Take $1\in\mathcal{U}$. By Proposition 40

$$\begin{aligned} M(1) &= \frac{1}{|C_{r_1}(1)|}\sum_{v\in\mathcal{O}(1)}|C_n(v)| = \frac{1}{a}\left(\left|C_n(\varepsilon^{-1}(m/2))\right| + \sum_{v\in\mathcal{O}(1)\setminus\{\varepsilon^{-1}(m/2)\}}|C_n(v)|\right) = \\ &= \frac{1}{a}\left(\frac{m}{2}+\frac{b}{2}\cdot m\right) = \frac{b}{2}+\frac{b^2}{2} = \frac{b(b+1)}{2}. \end{aligned}$$

On the other hand, for any $e\in\mathcal{U}\setminus\{1\}$ one has that

$$M(e) = \frac{1}{|C_{r_1}(e)|}\sum_{v\in\mathcal{O}(e)}|C_n(v)| = \frac{1}{a}\cdot b\cdot m = b^2.$$

Therefore, $f_1 = b^2 > f_2 = \frac{b(b+1)}{2}$. The sequence $g_1 < g_2$ is

$$g_1 = \sum_{M(v)=f_1}|C_{r_1}(v)| = \sum_{u\in\mathcal{U}\setminus\{1\}}|C_{r_1}(u)| = \frac{a-1}{2}\cdot a = \frac{a(a-1)}{2},$$

$$g_2 = g_1 + |C_{r_1}(1)| = \frac{a(a-1)}{2} + a = \frac{a(a+1)}{2},$$

- Case a and b even.
Take $1\in\mathcal{U}$. Then $M(1)$ is computed exactly as in the previous case, so $M(1) = \frac{b(b+1)}{2}$.
Now, consider $\varepsilon^{-1}(a/2)\in\mathcal{U}$. Then, by Proposition 43 *3)*

$$M(\varepsilon^{-1}(a/2)) = \frac{1}{|C_{r_1}(\varepsilon^{-1}(a/2))|}\sum_{v\in\mathcal{O}(\varepsilon^{-1}(a/2))}|C_n(v)| = \frac{2}{a}\cdot\frac{b}{2}\cdot m = b^2.$$

Finally, for any $e\in\mathcal{U}\setminus\{1,\varepsilon^{-1}(a/2)\}$ one has

$$M(e) = \frac{1}{|C_{r_1}(e)|}\sum_{v\in\mathcal{O}(e)}|C_n(v)| = \frac{1}{a}\cdot b\cdot m = b^2.$$

We conclude $f_1 = b^2 > f_2 = \frac{b(b+1)}{2}$. The values g_1, g_2 are

$$g_1 = \sum_{M(v)=f_1}|C_{r_1}(v)| = a\cdot(|\mathcal{U}|-2) + \left|C_{r_1}(\varepsilon^{-1}(a/2))\right| = a\cdot\left(\frac{a}{2}-1\right)+\frac{a}{2} = \frac{a(a-1)}{2},$$

and

$$g_2 = g_1 + |C_{r_1}(1)| = \frac{a(a-1)}{2} + a = \frac{a(a+1)}{2},$$

- Case a even and b odd. In this case $\varepsilon^{-1}(m/2)\notin\mathcal{O}(1)$ and $\varepsilon^{-1}(m/2)\in\mathcal{U}$ (see Remark 41). Observe that $\varepsilon^{-1}(a/2)\in\mathcal{O}(\varepsilon^{-1}(m/2))$ and so $\varepsilon^{-1}(a/2)\notin\mathcal{U}$.
For $1\in\mathcal{U}$ we have

$$M(1) = \frac{1}{|C_{r_1}(1)|}\sum_{v\in\mathcal{O}(1)}|C_n(v)| = \frac{1}{a}\cdot|\mathcal{O}(1)|\cdot m = \frac{1}{a}\cdot\frac{b+1}{2}\cdot m = \frac{b(b+1)}{2}.$$

Now consider $\varepsilon^{-1}(m/2)\in\mathcal{U}$. Then, by Proposition 44 *2) a)*

$$M(\varepsilon^{-1}(m/2)) = \frac{1}{|C_{r_1}(\varepsilon^{-1}(m/2))|}\sum_{v\in\mathcal{O}(\varepsilon^{-1}(m/2))}|C_n(v)| = \frac{2}{a}\cdot\left[\left(\frac{b+1}{2}-1\right)\cdot m+\frac{m}{2}\right] = (b-1)\cdot b + b = b^2.$$

Finally, for any $e\in\mathcal{U}\setminus\{1,\varepsilon^{-1}(m/2)\}$ we use Proposition 44 *2) b)* and we obtain $M(e) = \frac{1}{a}\cdot b\cdot m = b^2$. Therefore, as in all the previous cases $f_1 = b^2 > f_2 = \frac{b(b+1)}{2}$, and once more

$$g_1 = \left|C_{r_1}(\varepsilon^{-1}(m/2)\right| + \left(\frac{a}{2}-1\right)\cdot a = \frac{a}{2}+\frac{a-2}{2}\cdot a = \frac{a(a-1)}{2}$$

and

$$g_2 = g_1 + |C_{r_1}(1)| = \frac{a(a-1)}{2} + a = \frac{a(a+1)}{2}.$$

In conclusion, all the cases yield the same sequences $f_1 > f_2$, $g_1 < g_2$. Finally, by Theorem 9, $\Gamma(\mathcal{C})$ is a set of check positions for $\mathcal{C}$, and then $T^{-1}(\Gamma)$ is a set of check positions for $R^*(m-3,m)$. So, $\{0, \alpha^i \mid i \in T^{-1}(\Gamma))\}$ is a set of check positions for $R(m-3,m)$ (see Remark 29). Since $R(m-3,m) = R(2,m)^{\perp}$ we are done.

■

Examples 47. *The first value for m that satisfies conditions (13) is $m = 4$. In this case, $n = 2^4 - 1 = 15, r_1 = 3, r_2 = 5, a = b = 2$. So, let us give an information set for $R(2,4)$. By Theorem 46 we have that*

$$\Gamma = \{(0,0),(1,0),(2,0),(0,1),(1,1),(2,1),(0,2),(1,2),(2,2),(0,3)\}.$$

Then, by taking the isomorphism given by the Chinese Remainder Theorem, we have that $T^{-1}(\Gamma) = \{0,1,2,3,5,6,7,10,11,12\}$. So $\{0, \alpha^i \mid i \in T^{-1}(\Gamma)\}$ is an information set for $R(2,4)$ and $\{\alpha^i \mid i \notin T^{-1}(\Gamma)\}$ is an information set for $R(1,4)$. In the same sense than in the previous section, Table IV shows the different information sets that we can get by using all the possible isomorphisms from $\mathbb{Z}_{15}$ to $\mathbb{Z}_3 \times \mathbb{Z}_5$; the first column includes the image of $1 \in \mathbb{Z}_{15}$ which determines the corresponding isomorphism, while the second column gives the set of exponents I such that $\{0, \alpha^i \mid i \in I\}$ is an information set for $R(2,4)$. From these information sets we can obtain the corresponding ones for $R(1,4)$; the reader may check that we get four new information sets with respect to that obtained in Table I.

T(1)	I
(1,1)	{0,1,2,3,5,6,7,10,11,12}
(2,1)	{0,1,2,3,5,6,7,10,11,12}
(1,2)	{0,1,3,5,6,8,9,10,11,13}
(2,2)	{0,1,3,5,6,8,9,10,11,13}
(1,3)	{0,2,4,5,6,7,9,10,12,14}
(2,3)	{0,2,4,5,6,7,9,10,12,14}
(1,4)	{0,3,4,5,8,9,10,12,13,14}
(2,4)	{0,3,4,5,8,9,10,12,13,14}

TABLE IV
INFORMATION SETS FOR R(2,4)

The next value for m is $m = 6$. In this case, $n = 2^6 - 1 = 63, r_1 = 7, r_2 = 9, a = 3$ and $b = 2$. So

$$\begin{aligned}\Gamma \;=\; & \{(0,0),(1,0),(2,0),(3,0),(4,0),(5,0),(0,1),(1,1),(2,1),(3,1),(4,1),(5,1),(0,2),(1,2),(2,2),(3,2),(4,2),\\ & (5,2),(0,3),(1,3),(2,3)\}.\end{aligned}$$

By taking as isomorphism that given by the Chinese Remainder Theorem, we obtain

$$T^{-1}(\Gamma) = \{0,1,2,9,10,11,18,19,21,28,29,30,36,37,38,45,46,47,54,56,57\},$$

so we have that $\{0, \alpha^i \mid i \in T^{-1}(\Gamma)\}$ is an information set for $R(2,6)$ and $\{\alpha^i \mid i \notin T^{-1}(\Gamma)\}$ is an information set for $R(3,6)$.

Finally, we see the case $m = 8$. In this case, there are two decompositions of $n = 2^8 - 1 = 255$ that satsify conditions (13), namely, $(r_1 = 3, r_2 = 85)$ and $(r_1 = 15, r_2 = 17)$. Table V shows the sets $T^{-1}(\Gamma)$ obtained for each decomposition; in both cases we are considering the isomorphism given by the Chinese Remainder Theorem.

r_1	r_2	a	$T^{-1}(\Gamma)$
3	85	2	{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 15, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 96, 99, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 183 }
15	17	4	{ 0, 1, 2, 3, 17, 18, 19, 20, 34, 35, 36, 51, 52, 53, 68, 69, 105, 120, 121, 122, 136, 137, 138, 139, 153, 154, 155, 170, 171, 172, 187, 188, 189, 204, 240, 241}

TABLE V
INFORMATION SETS FOR R(5,8)

To finish our explanation, we include the following table which shows the suitable values of m up to length 4096. The values $m = 2, 3, 5, 7$ yield a prime number for $n = 2^m - 1$, while the value $m = 11$ only admits a decomposition $(r_1 = 23, r_2 = 89)$ that does not satisfy the conditions (13).

m	n	r_1	r_2	a	b
4	15	3	5	2	2
6	63	7	9	3	2
8	255	3	85	2	4
8	255	15	17	4	2
9	511	7	73	3	3
10	1023	3	341	2	5
12	4095	7	585	3	4
12	4095	63	65	6	2

TABLE VI
PARAMETERS FOR SECOND ORDER RM CODES UP TO LENGTH 4096

VIII. CONCLUSIONS

We have described information sets for Reed-Muller codes of first and second-order respectively. We have seen them as group codes and we have constructed those information sets from their defining sets; that is, from an intrinsical characteristic of this family of algebraic codes. This supposes a relevant difference with regard to other approaches to the same problem, such as those proposed from a geometrical point of view ([12], [13], [18]). Moreover, the definition of the information sets turn be very simple in the end and it is given only in terms of their basic parameters.

It is also pertinent to wonder about the benefits that our results may imply in relation to the applicability of certain decoding algorithms such as the permutation decoding algorithm, which is especially appropriate for abelian codes. In [5] we showed a generic study of this algorithm for abelian codes starting from the information sets introduced in [4]. Therefore, since the present work manage to adapt the results in [4] to Reed-Muller codes, it is reasonable to believe that the results in [5]can also be apply to them. Furthermore, the vision of Reed-Muller codes as affine-invariant codes allows us to search for a PD-set within the group of all affine transformations, beyond the translations. For all these reasons, the application of the permutation decoding algorithm to Reed-Muller codes, starting from the results obtained in this work instead of the geometric point of view, supposes an interesting open problem.

REFERENCES

[1] W. C. Huffman, "Codes and Groups", in *Handbook of Coding Theory*, vol II, V. S. Pless, W. C. Huffman and R. A. Brualdi Eds. Amsterdam. North-Holland, 1998.

[2] E. F. Assmus Jr and J. D. Key, "Polynomial codes and Finite Geometries", in *Handbook of Coding Theory*, vol II, V. S. Pless, W. C. Huffman and R. A. Brualdi Eds. Amsterdam. North-Holland, 1998.

[3] S. D. Berman, "Semisimple cyclic and Abelian codes", *Cybernetics*, vol. 3, no. 3, pp. 21-30, 1967.

[4] J. J. Bernal and J. J. Simón, "Information sets from defining sets in abelian codes", *IEEE Trans. Inform. Theory*, vol. 57, no. 12, pp. 7990-7999, 2011.

[5] J. J. Bernal and J. J. Simón, "Partial permutation decoding for abelian codes", *IEEE Trans. Inform. Theory*, vol. 59, no. 8, pp. 5152-5170, 2013.

[6] J. J. Bernal and J. J. Simón, Reed-Muller codes: Information sets from defining sets, Coding Theory and Applications, Proceedings of 5th International Castle Meeting ICMTCA 2017, A. Barbero, V. Skachek and O. Ytrehus eds, LNCS vol. 10495, Springer, 2017, pp. 30-47.

[7] J. J. Bernal, Códigos de grupo. Conjuntos de información. Decodificación por permutación. Ph. D. Thesis, 2011.

[8] A. Blokhuis, G. E. Moorhouse, "Some p-ranks related to orthogonal spaces", *J. Algebraic Combin.* vol. 4, pp. 295-316, 1995.

[9] P. Charpin, Codes cycliques etendus invariants sous le group affine. These de Doctorat d'Etat, Universite Pars VII, 1987.

[10] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge, 2003.

[11] H. Imai, "A theory of two-dimensional cyclic codes", *Inform. and Control*, vol34, pp. 1.21, 1977.

[12] J. D. Key, T. P. McDonough, V. C. Mavron, "Partial permutation decoding for codes from finite planes", *Eur. Journal of Combin.* vol 26, pp. 665-682, 2005.

[13] J. D. Key, T. P. McDonough, V. C. Mavron, "Information sets and partial permutation decoding for codes from finite geometries", *Finite Fields Appl.* vol 12, pp. 232-247, 2006.

[14] F.J. MacWilliams, N. J. A. Sloane, The theory of error-correcting codes, North-Holland, Amsterdam, 1983.

[15] D. E. Muller, "Application of boolean algebra to switching circuit design and to error detection", *IEEE Trans. Comput.* vol. 3, pp. 6-12, 1954.

[16] G. E. Moorhouse, "Bruck nets, codes and characters of loops", *Des. Codes Cryptogr.* vol. 1, pp. 7-29, 1991.

[17] I. S. Reed, "A class of multiple-error-correcting codes and the decoding scheme", *IRE Trans. Inform. Theory,* IT-4, pp 38-49, 1954.

[18] P. Seneviratne, "Permutation decoding for the first-order Reed-Muller codes", *Discrete Math.* vol.309, pp. 1967-1970, 2009