Construction of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes

P. Montolio and J. Rifà

***Abstract*—This work deals with Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes, which are binary codes after a Gray map from a subgroup of the direct product of $\mathbb{Z}_2$, $\mathbb{Z}_4$ and Q_8 groups, where Q_8 is the non-commutative quaternion group. These kind of codes have five types ("shapes") and the values or range of values of several characteristic parameters is analyzed. Specifically, we show that all these codes can be represented in a standard form from a set of generators, as well as using the parameters of dimension of the kernel and rank. In addition, we present several methods that allow, given some preselected values of these parameters, the construction of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes fulfilling them.**

***Index Terms*—Dimension of the kernel, error-correcting codes, Hadamard codes, rank, $\mathbb{Z}_2\mathbb{Z}_4$-codes, $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes.**

I. Introduction

Error-correcting codes, used to correct errors in transmissions, are sequences of elements from a finite set (usually binary elements, or bits) which contain an enclosed message and allow to retrieval this message even when some of the transmitted elements are lost or corrupted. In order to achieve this objective, any two words in the set of sequences disagree on several coordinates.

Hadamard codes are a family of error-correcting codes that enforces their capability to recover a strongly corrupted message using a high level of redundancy. Hadamard codes has been extensively used in real world applications, being the most famous the NASA space probe Mariner 9 in 1971, where the code was used to transmit photos of Mars back to earth. In addition, they are also used in cryptography, mainly in stenography. Hadamard codes are named after the French mathematician Jacques Hadamard (1865-1963) and also known under the name of Walsh codes or Walsh-Hadamard codes, in recognition of the American mathematician Joseph Leonard Walsh (1895-1973).

Non-linear groups (like $\mathbb{Z}_2\mathbb{Z}_4$ or $\mathbb{Z}_2\mathbb{Z}_4Q_8$) have received an increased attention from the Hammons and Kumar work [1] that shows that most of these codes are ideals in polynomial rings using $\mathbb{Z}_4$, the ring of integers mod 4. In the author's own words "this new point of view should completely transform the study of cyclic codes". The codes this paper deals with can be characterized as the image of a subgroup, by a suitable Gray map, of an algebraic group like the direct product of $\mathbb{Z}_2$, $\mathbb{Z}_4$ and Q_8, the quaternion group of order 8 [2]. Hence it makes sense to call these codes as $\mathbb{Z}_2\mathbb{Z}_4$-codes or $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes.

In this paper we analyze codes that have both properties, being Hadamard and $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes. We will see their algebraic structure, their classification in several types ("shapes") and the values or range of values of several parameters, like the dimension of the kernel and rank. Specifically, we focus on showing how all these codes can be represented in a standard form using a set of generators and the value of the dimension of the kernel and rank.

In addition, we present methods that allow, given some preselected values of the above parameters, the construction of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes fulfilling them.

The structure of the paper is as follows: Section II introduces the notation and preliminary concepts; Section III shows the standard form of generators that allows to represent any Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code in a unique way; Section IV gives several methods of constructing codes given a prefixed value for the dimension of the kernel and/or rank. The paper finishes with conclusions and bibliographic references.

P. Montolio is with the Computing, Multimedia and Telecommunication Studies, Universitat Oberta de Catalunya, Spain.

J. Rifà is with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, Spain.

II. Preliminaries

Almost all the definitions and concepts bellow can be found in [3].

Let $\mathbb{Z}_2$ and $\mathbb{Z}_4$ denote the binary field and the ring of integers modulo 4, respectively. Let Q_8 be the *quaternion group* on eight elements. The following equalities provides a presentation and the list of elements of Q_8:

$$Q_8 = \langle \mathbf{a}, \mathbf{b} : \mathbf{a}^4 = \mathbf{a}^2\mathbf{b}^2 = \mathbf{1}, \mathbf{b}\mathbf{a}\mathbf{b}^{-1} = \mathbf{a}^{-1} \rangle = \{\mathbf{1}, \mathbf{a}, \mathbf{a}^2, \mathbf{a}^3, \mathbf{b}, \mathbf{a}\mathbf{b}, \mathbf{a}^2\mathbf{b}, \mathbf{a}^3\mathbf{b}\}.$$

Given three exponents k_1, k_2 and k_3, denote as $\mathcal{G}$ the group $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$. Any element of $\mathcal{G}$ can be expressed as a vector where the first k_1 components belong to $\mathbb{Z}_2$, the next k_2 components belong to $\mathbb{Z}_4$ and the last k_3 components belong to Q_8.

We will use multiplicative notation for $\mathcal{G}$ and denote $\mathbf{e}$ the identity element of the group and $\mathbf{u}$ the element of order two: $\mathbf{e} = (0, \overset{k_1+k_2}{\ldots}, 0, \mathbf{1}, \overset{k_3}{\ldots}, \mathbf{1})$ and $\mathbf{u} = (1, \overset{k_1+k_2}{\ldots}, 1, \mathbf{a}^2, \overset{k_3}{\ldots}, \mathbf{a}^2)$.

We will call *Gray map* the function Φ:

$$\Phi : \mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3} \longrightarrow \mathbb{Z}_2^{k_1+2k_2+4k_3},$$

acting componentwise in such a way that over the binary part is the identity, over the quaternary part acts as the usual Gray map, so $0 \to (00)$, $1 \to (01)$, $2 \to (11)$, and over the quaternionic part acts in the following way:

$\mathbf{1} \to (0,0,0,0)$, $\mathbf{b} \to (0,1,1,0)$,
$\mathbf{a} \to (0,1,0,1)$, $\mathbf{ab} \to (1,1,0,0)$,
$\mathbf{a}^2 \to (1,1,1,1)$, $\mathbf{a}^2\mathbf{b} \to (1,0,0,1)$,
$\mathbf{a}^3 \to (1,0,1,0)$, $\mathbf{a}^3\mathbf{b} \to (0,0,1,1)$.

Note that $\Phi(\mathbf{e})$ is the all-zeroes vector and $\Phi(\mathbf{u})$ is the all-ones vector.

We are interested in Hadamard binary codes $C = \Phi(\mathcal{C})$ where $\mathcal{C}$ is a subgroup of $\mathcal{G}$. All through the paper we are assuming it.

We denote as $T(\mathcal{C}) = \{z \in \mathcal{C} : z^2 = \mathbf{e}\}$ the subgroup of elements of order two in $\mathcal{C}$.

Two elements a and b of $\mathcal{C}$ commutes if and only if $ab = ba$. As an extension of this concept, the *commutator* of a and b is defined as the element $[a, b]$ such that $ab = [a, b]ba$. Note that all commutators belong to $T(\mathcal{C})$ and any element of $T(\mathcal{C})$ commutes with all elements of $\mathcal{C}$.

We say that two elements a and b of $\mathcal{C}$ *swap* if and only if $\Phi(ab) = \Phi(a) + \Phi(b)$. As an extension of this concept, define the *swapper* of a and b as the element $(a : b)$ such that $\Phi((a : b)ab) = \Phi(a) + \Phi(b)$. Note that all swappers belong to $T(\mathcal{G})$ but they can be out of $\mathcal{C}$.

Both, commutators and swappers can be obtained as a component-wise expression, if $a = (a_1, \ldots, a_l)$ and $b = (b_1, \ldots, b_l)$ then $(a : b) = ((a_1 : b_1), \ldots, (a_l : b_l))$ and $[a, b] = ([a_1, b_1], \ldots, [a_l, b_l])$. Table I and Table II describes the values of all swappers and commutators, respectively, in $\mathbb{Z}_4$ and Q_8 (the value in $\mathbb{Z}_2$ is always 0).

	0,2	1,3
0,2	0	0
1,3	0	2

	$\mathbf{1}$,$\mathbf{a}^2$	$\mathbf{a}$,$\mathbf{a}^3$	$\mathbf{b}$,$\mathbf{a}^2\mathbf{b}$	$\mathbf{ab}$,$\mathbf{a}^3\mathbf{b}$
$\mathbf{1}$,$\mathbf{a}^2$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$
$\mathbf{a}$,$\mathbf{a}^3$	$\mathbf{1}$	$\mathbf{a}^2$	$\mathbf{a}^2$	$\mathbf{1}$
$\mathbf{b}$,$\mathbf{a}^2\mathbf{b}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{a}^2$	$\mathbf{a}^2$
$\mathbf{ab}$,$\mathbf{a}^3\mathbf{b}$	$\mathbf{1}$	$\mathbf{a}^2$	$\mathbf{1}$	$\mathbf{a}^2$

TABLE I
SWAPPERS IN $\mathbb{Z}_4$ AND Q_8

	0,2	1,3
0,2	0	0
1,3	0	0

	$\mathbf{1}$,$\mathbf{a}^2$	$\mathbf{a}$,$\mathbf{a}^3$	$\mathbf{b}$,$\mathbf{a}^2\mathbf{b}$	$\mathbf{ab}$,$\mathbf{a}^3\mathbf{b}$
$\mathbf{1}$,$\mathbf{a}^2$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$
$\mathbf{a}$,$\mathbf{a}^3$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{a}^2$	$\mathbf{a}^2$
$\mathbf{b}$,$\mathbf{a}^2\mathbf{b}$	$\mathbf{1}$	$\mathbf{a}^2$	$\mathbf{1}$	$\mathbf{a}^2$
$\mathbf{ab}$,$\mathbf{a}^3\mathbf{b}$	$\mathbf{1}$	$\mathbf{a}^2$	$\mathbf{a}^2$	$\mathbf{1}$

TABLE II
COMMUTATORS IN $\mathbb{Z}_4$ AND Q_8

Using these tables it could be easily checked that, for any $a, b, c \in \mathcal{G}$:

1) $[a, b] = [b, a]$. Note it is not always true that $(a : b) = (b : a)$.
2) $(ab : c) = (a : c)(b : c)$ and $(c : ab) = (c : a)(c : b)$
3) $[ab, c] = [a, c][b, c]$.
4) $(a : b)(b : a) = [a, b]$

The *kernel* of a binary code C of length n is $K(C) = \{z \in \mathbb{Z}_2^n : C + z = C\}$. It is known [3] the following relationship between swappers and the kernel. For any element a of $\mathcal{C}$ we have $\Phi(a) \in K(C)$ if and only if all the swappers$(a : b) \in \mathcal{C}$ for every $b \in \mathcal{C}$.

The dimension of $K(C)$ is denoted by $k(C)$ or simply k.

The *rank* of a binary code C is the dimension of the linear span of C. It is denoted by $r(C)$ or simply r.

It is known [3] that the linear span of C can be seen as $\Phi(\langle \mathcal{C} \cup S(\mathcal{C}) \rangle)$, where $\langle \mathcal{C} \cup S(\mathcal{C}) \rangle$ is the group generated by $\mathcal{C}$ and $S(\mathcal{C})$ the swappers of the elements of $\mathcal{C}$.

Definition II.1. *Define $M(x)$ over $x \in T(\mathcal{G})$ as the set of coordinates positions where the value of x is the element of order two, $\varnothing \subseteq M(x) \subseteq M(\mathbf{u})$.*

Example: let $x = (1, a^2, a^2, 1, 1, a^2)$ then $M(x) = \{1, 2, 5\}$, where the first component is 0.

Lemma II.2. *Let $x, y \in \mathcal{G}$, then*

1) *$M((x : y)) \subseteq M(x^2) \cap M(y^2)$ and $M([x, y]) \subseteq M(x^2) \cap M(y^2)$. In the specific case when $[x, y] = \mathbf{e}$ we have $M((x : y)) = M(x^2) \cap M(y^2)$ and $M([x, y]) = \varnothing$.*
2) *if $[x, y] = \mathbf{e}$ then $\mathrm{wt}((xy)^2) = \mathrm{wt}(x^2y^2) = \mathrm{wt}(x^2) + \mathrm{wt}(y^2) - 2\mathrm{wt}((x : y))$.*

Proof. Both items follow straightforwardly from Tables I and II. □

Lemma II.3. *Let $\mathcal{C}$ be a subgroup of $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$ such that $\Phi(\mathcal{C})$ is a Hadamard code. Let $a, b, c \in \mathcal{C} \setminus T(\mathcal{C})$.*

1) *either $a^2 = \mathbf{u}$ or $[a, b] = [b, a] = \mathbf{e}$ or $[a, b] = [b, a] = a^2$.*
2) *if $a^2 = u$ and $b^2 = c^2 = [b, c] \notin \{\mathbf{e}, \mathbf{u}\}$ then $[a, b] = \mathbf{e}$ or $[a, c] = \mathbf{e}$ or $[a, bc] = \mathbf{e}$.*
3) *if $b^2 = c^2 = [b, c]$ and $[a, b] = [a, c] = \mathbf{e}$ then $(ab)^2 = (ac)^2 = \mathbf{u}$ and a^2, b^2, c^2 are not equal to $\mathbf{u}$.*

Proof. The first item was already proven in [3, Lemma IV.6].

For the second item we will assume that the first two possibilities of the conclusion are false. Using the first item in this Lemma we have $[a, b] = [a, c] = b^2 = c^2$, so $[a, bc] = [a, b][a, c] = b^2c^2 = e$. This proves the second item.

For the third item note that $(bc)^2 = b^2c^2[b, c] = b^2 = c^2$, thus $M(b^2) = M(c^2) = M((bc)^2)$. Taken into account that $[a, b] = [a, c] = [a, bc] = \mathbf{e}$, by Lemma II.2 we have $M((a : b)) = M((a : c)) = M((a : bc))$. Hence, $(a : b) = (a : c) = (a : bc)$. Moreover, $(a : bc) = (a : b)(a : c) = (a : b)^2 = \mathbf{e}$ and so $(a : b) = (a : c) = \mathbf{e}$. Now, using again Lemma II.2, $\mathrm{wt}(a^2b^2) = \mathrm{wt}(a^2) + \mathrm{wt}(b^2) - 2\mathrm{wt}((a : b)) = \mathrm{wt}(a^2) + \mathrm{wt}(b^2)$. As we are working with elements of a Hadamard code, the weights must be equal to n, $n/2$ or 0. The last possibility has been discarded when we state that they do not belong to $T(\mathcal{C})$, and so the only remainder possibility is $\mathrm{wt}(a^2) = \mathrm{wt}(b^2) = \mathrm{wt}(c^2) = n/2$ and $\mathrm{wt}(a^2b^2) = n$, proving in this way that a^2, b^2, c^2 are not equal to $\mathbf{u}$ and $a^2b^2 = \mathbf{u}$. The same argumentation lead to $a^2c^2 = \mathbf{u}$. □

III. THE STANDARD FORM FOR THE GENERATING SET OF A HADAMARD $\mathbb{Z}_2\mathbb{Z}_4Q_8$-CODE

In [3] there was given a classification of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes from an algebraic point of view. As a consequence each Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code, seen as a subgroup $\mathcal{C} < \mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$ is of one shape among the five possible. To decide the shape of a given subgroup we need to know a normalized generating set of $\mathcal{C}$. Now, in this section we present a new point of view which lead to us to construct a standard generating set which will allow to decide the classification of a given subgroup in a more efficient way.

In the next theorem we show that a subgroup $\mathcal{C}$, which gives a Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code, has an abelian maximal subgroup $\mathcal{A}$ which is normal in $\mathcal{C}$ and $\mathcal{C}/\mathcal{A}$ is an abelian group of order 2^a, for $a \in \{0, 1, 2\}$. We begin by a technical lemma.

Lemma III.1. *Let $\mathcal{C}$ be a subgroup of $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$ such that $\phi(\mathcal{C}) = C$ is a Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code. Let $\mathcal{A}$ be a subgroup of $\mathcal{C}$ containing $T(\mathcal{C})$, the subgroup of the elements of order two in $\mathcal{C}$. Then $\mathcal{A}$ is normal in $\mathcal{C}$.*

Proof. We want to show that $c^{-1}ac \in \mathcal{A}$ for every $a \in \mathcal{A}, c \in \mathcal{C}$. We have $c^{-1}ac = a[a,c]$ and all commutators belong to $T(\mathcal{C}) \subseteq \mathcal{A}$, so the statement follows. □

Theorem III.2. *Let $\mathcal{C}$ be a subgroup of $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$ such that $\phi(\mathcal{C}) = C$ is a Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code. Then $\mathcal{C}$ has an abelian maximal subgroup $\mathcal{A}$ which is normal in $\mathcal{C}$ and $|\mathcal{C}/\mathcal{A}| \in \{1,2,4\}$.*

Proof. The proof will be based on the already known normalized generating sets introduced in [3]. On that paper, five possible shapes for subgroups $\mathcal{C}$ such that $\phi(\mathcal{C})$ is Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code are described as well as how they are the elements in their respective normalized generators sets.

A normalized generator set in [3] has the form $\mathcal{C} = \langle x_1, \ldots, x_\sigma;\ y_1, \ldots, y_\delta;\ z_1,\ \ldots, z_\rho \rangle$, where x_i are elements of order two that generates $T(\mathcal{C}) = \langle x_1 ... x_\sigma \rangle$ and $Z(\mathcal{C}) = \langle x_1, \ldots, x_\sigma;\ y_1, \ldots, y_\delta \rangle$ is the center of $\mathcal{C}$. Throughout this proof we will use a new generator set for $\mathcal{C}$, which will be called *standardized generator set*: $\mathcal{C} = \langle x_1, \ldots, x_\sigma, r_1, \ldots, r_\tau, s_1, \ldots, s_\upsilon \rangle$ and we always define the subgroup $\mathcal{A}$ as $\mathcal{A} = \langle x_1, \ldots, x_\sigma, r_1, \ldots, r_\tau \rangle$, which is normal in $\mathcal{C}$ by Lemma III.1.

For the case when $\mathcal{C}$ is of shape 1 we have that the whole group $\mathcal{C}$ is abelian, so $\mathcal{A} = \mathcal{C}$ and $|\mathcal{C}/\mathcal{A}| = 1$.

For the case when $\mathcal{C}$ is of shape 2 we have [3] $\delta = 0$, $z_1^2 = z_2^2 = [z_1, z_2] = \mathbf{u}$, $[z_i, z_j] = z_j^2$ and $[z_j, z_k] = \mathbf{e}$ for every $i \in \{1,2\}$ and $3 \leq j,k \leq \rho$. We define the standardized generator set taking $x_1, \ldots, x_\sigma$; $r_1 = z_1 z_2$, $r_i = z_{i+1}$ for every $2 \leq i \leq \tau$; $s_1 = z_1$. Now we want to show that $\mathcal{A}$ is abelian and maximal in $\mathcal{C}$ and $\mathcal{C}/\mathcal{A} = \langle s_1 \rangle$. Indeed, for every $2 \leq i,j \leq \tau$, $[r_1, r_i] = [z_1 z_2, z_{i+1}] = [z_1, z_{i+1}][z_2, z_{i+1}] = z_{i+1}^2 z_{i+1}^2 = \mathbf{e}$ and $[r_i, r_j] = [z_{i+1}, z_{j+1}] = \mathbf{e}$. Hence $\mathcal{A}$ is abelian. To prove the maximality of $\mathcal{A}$ in $\mathcal{C}$ we show that $[s_1, r_1] = [z_1, z_1 z_2] = [z_1, z_2] = \mathbf{u} \neq \mathbf{e}$. In addition, for further use, we see that $r_1^2 = (z_1 z_2)^2 = z_1^2 z_2^2 [z_1 : z_2] = \mathbf{u}$ and $s_1^2 = z_1^2 = \mathbf{u}$.

For the case when $\mathcal{C}$ is of shape 3 we have [3] $\delta = 0$, $z_1^2 = \mathbf{u} \notin \langle z_2^2, \ldots, z_\rho^2 \rangle$, $[z_1, z_i] = z_i^2$ and $[z_i, z_j] = \mathbf{e}$, for every $i \neq j$ in $\{2, \ldots, \rho\}$. We define the standardized generator set taking $r_i = z_{i+1}$ for every $1 \leq i \leq \tau = \rho - 1$; $s_1 = z_1$. Now we want to show that $\mathcal{A}$ is abelian and maximal in $\mathcal{C}$ and $\mathcal{C}/\mathcal{A} = \langle s_1 \rangle$. Indeed, for every $1 \leq i,j \leq \tau$, $[r_i, r_j] = [z_{i+1}, z_{j+1}] = \mathbf{e}$. Hence $\mathcal{A}$ is abelian. To prove the maximality of $\mathcal{A}$ in $\mathcal{C}$ we show that $[s_1, r_1] = [z_1, z_2] = z_2^2 \neq \mathbf{e}$. In addition, we note that $\mathbf{u} \notin \langle r_1^2 \ldots r_\tau^2 \rangle$ and $s_1^2 = z_1^2 = \mathbf{u}$.

For the case when $\mathcal{C}$ is of shape 4 with $\delta = 0$ we have $\delta = 0$, $\rho = 2$ and $z_1^2 = z_2^2 = [z_1, z_2] \notin \{\mathbf{e}, \mathbf{u}\}$. We define the standardized generator set taking $r_1 = z_1$, $s_1 = z_2$ and define $\mathcal{A} = \langle x_1, \ldots, x_\sigma; r_1 \rangle$. Note that with this definition $\upsilon = 1$. As all generators belong to $T(\mathcal{C})$ except one, it is immediate that $\mathcal{A}$ is abelian and $\mathcal{C}/\mathcal{A} = \langle s_1 \rangle$. For the maximality, see that $[r_1, s_1] = [z_1, z_2] = z_1^2 \neq \mathbf{e}$. Note $r_1^2 = s_1^2 \neq \mathbf{u}$.

For the case when $\mathcal{C}$ is of shape 4 with $\delta = 1$ we have $\rho = 2$ and $z_1^2 = z_2^2 = [z_1, z_2] \notin \{\mathbf{e}, \mathbf{u}\}$. The element y_1 commutes with both z_1, z_2 and so, by item 3 of Lemma II.3 we have $y_1^2 \neq \mathbf{u}$ and $(y_1 z_1)^2 = (y_1 z_2)^2 = \mathbf{u}$. We define the standardized generator set taking $r_1 = y_1 z_1$, $r_2 = z_1$, $s_1 = z_2$. Note that with this definition $\upsilon = 1$. We have $[r_1, r_2] = [y_1 z_1, z_1] = \mathbf{e}^2 = \mathbf{e}$ and so $\mathcal{A}$ is abelian. For the maximality, see that $[r_1, s_1] = [y_1 z_1, z_2] = [z_1, z_2] = z_1^2 \neq \mathbf{e}$. In addition, $r_1^2 = (y_1 z_1)^2 = \mathbf{u} \neq r_2^2 = z_1^2$ and $s_1^2 = z_2^2 \neq \mathbf{u}$

For the case when $\mathcal{C}$ is of shape 5 we have $\delta = 0$ and $\rho = 4$. We have: $z_1^2 = z_2^2 = [z_1, z_2] = \mathbf{u} \neq z_3^2 = z_4^2 = [z_3, z_4]$ and $[z_i, z_j] \in \langle z_j^2 \rangle$ for every $i \in \{1,2\}$ and $j \in \{3,4\}$. We define the standardized generator set taking $r_1 = z_1$, $r_2 = f(z_1)$, $s_1 = z_2$, $s_2 = f(z_2)$, where:

$$f(z) = \begin{cases} z_3 & \text{if } [z, z_3] = e, \\ z_4 & \text{if } [z, z_4] = e, \\ z_3 z_4 & \text{otherwise.} \end{cases}$$

From Lemma II.3 it is easy to check that in the following matrix

$$\begin{pmatrix} [z_1, z_3] & [z_1, z_4] & [z_1, z_3 z_4] \\ [z_2, z_3] & [z_2, z_4] & [z_2, z_3 z_4] \\ [z_1 z_2, z_3] & [z_1 z_2, z_4] & [z_1 z_2, z_3 z_4] \end{pmatrix}$$

there is one and only one element in each row or column equal to e, being the other two elements equals to $z_3^2 = z_4^2$. Therefore, $[z_1, f(z_1)] = [z_2, f(z_2)] = \mathbf{e}$ and $[z_1, f(z_2)] = [z_2, f(z_1)] = [f(z_1), f(z_2)] = z_3^2 = z_4^2$.

We have $\mathcal{A} = \langle r_1, r_2 \rangle$ and $\mathcal{C}/\mathcal{A} = \langle s_1, s_2 \rangle$. In particular $[r_1, r_2] = [z_1, f(z_1)] = \mathbf{e}$, hence $\mathcal{A}$ is abelian. For the maximality, see that $[r_1, s_1] = [z_1, z_2] \neq \mathbf{e}$ and $[r_2, s_2] = [f(z_1), f(z_2)] \neq \mathbf{e}$. In addition, note $r_1^2 = s_1^2 = \mathbf{u} \neq r_2^2 = s_2^2$. □

The next corollary summarize the most relevant properties of the standardized set of generators we just defined.

Corollary III.3. *Let $\mathcal{C}$ be a subgroup of $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$ such that $C = \Phi(\mathcal{C})$ is a Hadamard code and let $\{x_1, \ldots, x_\sigma;\ r_1, \ldots, r_\tau;\ s_1, s_\upsilon\}$ be a standard set of generators of $\mathcal{C}$.*

- *The elements x_i are of order two and generate $T(\mathcal{C})$, $T(\mathcal{C}) = \langle x_1 ... x_\sigma \rangle$.*
- *The elements r_i are of order four that commute to each other, $[r_i, r_j] = e$ for every $1 \leq i,j \leq \tau$.*
- *When $\mathbf{u} \in \langle r_1 \ldots r_\tau \rangle$ we will take $\mathbf{u} = r_1^2$ and we have $r_1^2 = \mathbf{u} \notin \langle r_2^2 ... r_\tau^2 \rangle$.*
- *The cardinal υ of the set $\{s_1, s_\upsilon\}$ is in $\{0,1,2\}$ and when $\upsilon = 2$ we have $s_1^2 = \mathbf{u} \neq s_2^2 = [s_1, s_2]$. Moreover, when $r_1^2 = s_1^2 = \mathbf{u}$ then $[r_1, s_1] = \mathbf{u}$.*
- *Any element $c \in \mathcal{C}$ can be written in a unique way as*

$$c = \prod_{i=1}^{\sigma} x_i^{a_i} \prod_{j=1}^{\tau} r_j^{b_j} \prod_{k=1}^{\upsilon} s_k^{c_k}, \text{ where } a_i, b_j, c_k \in \{0,1\}.$$

The following table summarizes the main characteristics of each shape and allows their recognition using a standardized set of generators:

shape	τ	υ	$\mathbf{u} \in \langle r_1^2 ... r_\tau^2 \rangle$	$\mathbf{u} \in \langle s_1^2, s_\upsilon^2 \rangle$
1	≥ 0	0	Y/N	N
2	≥ 1	1	Y	Y
3	≥ 1	1	N	Y
4 ($\delta = 0$)	1	1	N	N
4 ($\delta = 1$)	2	1	Y	N
5	2	2	Y	Y

Quaternion group Q_8 is not a semidirect product of $\mathbb{Z}_4$ and $\mathbb{Z}_2$ but it can be seen as a quotient $Q_8 = \mathbb{Z}_4 \rtimes \mathbb{Z}_4 / \langle (\mathbf{a}^2, \mathbf{a}^2) \rangle$, where $\mathbf{a}$ is the generator of the multiplicative group $\mathbb{Z}_4$

and the semidirect product is defined by $(\mathbf{a}^i, \mathbf{a}^j)(\mathbf{a}^k, \mathbf{a}^s) = (\mathbf{a}^{i+(-1)^k}, \mathbf{a}^{j+s})$. The element $(\mathbf{a}^2, \mathbf{a}^2)$ is in the center of $\mathbb{Z}_4 \rtimes \mathbb{Z}_4$.

In the same way, $\mathcal{C}$ is not (in general) a semidirect product, but a quotient $\mathcal{C} = \mathcal{A} \rtimes \mathbb{Z}_4/\langle(\epsilon, \varepsilon)\rangle$ (respectively, $\mathcal{C} = \mathcal{A} \rtimes (\mathbb{Z}_4 \times \mathbb{Z}_4)/\langle(\epsilon, \varepsilon)\rangle$), where $\epsilon \in \mathcal{A}$, $\varepsilon \in \mathbb{Z}_4$(respectively, $\varepsilon \in \mathbb{Z}_4 \times \mathbb{Z}_4$), are of order two. Group $\mathcal{A}$ is normal and the maximal abelian inside $\mathcal{C}$. We can write it as $\mathcal{A} = \mathbb{Z}_2^{\sigma-\tau} \times \mathbb{Z}_4^{\tau}$.

The exact formulation of this quotient is specified in the next corollary.

Corollary III.4. *Let $\mathcal{C}$ be a subgroup of $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$ such that $C = \Phi(\mathcal{C})$ is a Hadamard code and let $\{x_1, \ldots, x_\sigma;\ r_1, \ldots, r_\tau;\ s_1, s_\upsilon\}$ be a standard set of generators of $\mathcal{C}$. Let $\mathcal{A} = \mathbb{Z}_2^{\sigma-\tau} \times \mathbb{Z}_4^{\tau}$ the maximal abelian and normal subgroup of $\mathcal{C}$ as we shown in Theorem III.2 and let $\{x_1, \ldots, x_\sigma;\ r_1, \ldots, r_\tau;\ s_1, s_\upsilon\}$ be a standardized generator set of $\mathcal{C}$.*

Then $\mathcal{C}$ is one of the following cases, where $Z_4 \times \mathbb{Z}_4 = \langle s_1, s_2\rangle$ in the last case and $\mathbb{Z}_4 = \langle s_1\rangle$ for the rest of cases.

Shape	$\mathcal{C}$	*comment*
1	$\mathcal{A}$	
2	$\mathcal{A} \rtimes \mathbb{Z}_4/(\mathbf{u}, s_1^2)$	$r_1^2 = \mathbf{u}$
3	$\mathcal{A} \rtimes \mathbb{Z}_4/(\mathbf{u}, s_1^2)$	$r_1^2 \neq \mathbf{u}$
$4(\delta = 0)$	$\mathcal{A} \rtimes \mathbb{Z}_4/(r_1^2, s_1^2)$	$r_1^2 \neq \mathbf{u}$
$4(\delta = 1)$	$\mathcal{A} \rtimes \mathbb{Z}_4/(r_2^2, s_1^2)$	$r_1^2 = \mathbf{u}$
5	$\mathcal{A} \rtimes (\mathbb{Z}_4 \times \mathbb{Z}_4)/(r_1^2, s_1^2)(r_2^2, s_2^2)$	$r_1^2 = \mathbf{u}$

IV. Construction of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes

In this section we describe a method to construct Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes with a preselected dimension of the kernel and rank.

In the next subsections we will see the conditions that s_1 and s_2 must fulfill in order to compose a code with specific values for the dimension of the kernel and the rank. Then, we will see how to create a subgroup $\mathcal{A}(\mathcal{C})$ a, finally, we construct codes $\mathcal{C}$ from the previous subgroup $\mathcal{A}(\mathcal{C})$ by adding the generators s_1 and, optionally, s_2.

A. Rules for s_1 and s_2

In the proof of Theorem III.2 we saw that $r_1^2 = \mathbf{u}$ (shape 2, shape 4 with $\delta = 1$, shape 5 and some cases of shape 1) and $\mathbf{u} \notin \langle r_1^2 \ldots r_\tau^2\rangle$ for the other shapes. Let $\mathcal{A} = \langle x_1, \ldots, x_\sigma, r_1, \ldots, r_\tau\rangle$ and let $\mathcal{R}$ be defined by

$$\begin{cases} \mathcal{R} = \langle x_1 \ldots x_\sigma, r_2 \ldots r_\tau\rangle; & \text{if } r_1^2 = \mathbf{u} \\ \mathcal{R} = \mathcal{A}; & \text{if } r_1^2 \neq \mathbf{u} \end{cases}$$

Let $\bar{\tau} = \tau - 1$ when $r_1^2 = \mathbf{u}$ and $\bar{\tau} = \tau$ when $r_1^2 \neq \mathbf{u}$.

with this definition, we can enunciate and proof the following lemma:

Lemma IV.1. *Let $a, b \in \mathcal{R}(\mathcal{C})\backslash T(\mathcal{C})$ which are not in the same coset of $T(\mathcal{C})$, so $b \neq aT(\mathcal{C})$ then:*

1) *$a^2, b^2, (ab)^2 \notin \{\mathbf{e}, \mathbf{u}\}$ and $\mathrm{wt}(a^2) = \mathrm{wt}(b^2) = \mathrm{wt}((ab)^2) = n/2$.*
2) *$\mathrm{wt}((a : b)) = n/4$ and so $((a : b)) \notin \mathcal{C}$.*
3) *With the same hypothesis as for a, b, let a', b' a different pair, such that the different elements in $\{a, b, a', b'\}$ are pairwise not in the same coset of $T(\mathcal{C})$. Then $(a : b) \neq (a' : b')$.*

Proof.

- Elements a, b are not in $T(\mathcal{C})$ so their square is not $\mathbf{e}$. Also, the construction of $\mathcal{R}$ explicitly excludes any element with square equal to $\mathbf{u}$. The product ab is also an element of $\mathcal{R}$, thus their square can not be $\mathbf{u}$. Moreover, if $(ab)^2 = \mathbf{e}$ then $a = bT(\mathcal{C})$ which contradicts the hypothesis. This proves the first item.
- As the elements a, b commute, we have from Lemma II.2 $n/2 = \mathrm{wt}((ab)^2) = \mathrm{wt}(a^2b^2) = \mathrm{wt}(a^2) + \mathrm{wt}(b^2) - 2\mathrm{wt}((a : b)) = n/2 + n/2 - 2\mathrm{wt}((a : b))$. Hence, $\mathrm{wt}((a : b)) = n/4$. This proves the second item.
- Suppose $(a : b) = (a' : b')$. Since $\mathrm{wt}((a : b)) = \mathrm{wt}((a' : b')) = n/4$ there are some positions (for a total weight of $n/8$) where all a, b, a', b' share a component of order four. The rest of components of order four (for a total weight of $n/8$) in each a, b, a', b' is not shared at all, since the elements are pairwise not in the same coset of $T(\mathcal{C})$. This situation is not possible in the case where all a, b, a', b' are different, for we obtain a vector of length $5n/4$. If, without loss of generality, we suppose $b = a'$ we obtain $a^2b^2b'^2 = \mathbf{u} \in \mathcal{R}$, a contradiction.

□

We can now enumerate and proof the different rules that s_1 and s_2 (if exists) must fulfill to reach a code with some kernel dimension and rank:

Lemma IV.2. *Let $\mathcal{C}$ be a subgroup of $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$ such that $C = \Phi(\mathcal{C})$ is a Hadamard code generated by $\langle \mathcal{A}(\mathcal{C}), s_1 \ldots s_\upsilon\rangle$. The values of the rank and kernel dimension depends on the characteristics of $\mathcal{A}(\mathcal{C})$, s_1 and s_2 (if exists) according to the following rules:*

1) *In the case $\upsilon = 0$ (Abelian $\mathbb{Z}_2\mathbb{Z}_4$-code) we have that if $\overline{\tau} \leq 1$ the code is linear $k = r = \sigma + \tau + \upsilon$; if $\overline{\tau} > 1$ then $k = \sigma + 1$, $r = \sigma + \tau + \upsilon + \binom{\tau-1}{2}$ when $r_1^2 = \mathbf{u}$ or $k = \sigma$, $r = \sigma + \tau + \upsilon + \binom{\tau}{2}$ when $r_1^2 \neq \mathbf{u}$*
2) *In the case $\tau = 1, \upsilon = 1$ we have that if $(s_1 : r_1) \in \mathcal{C}$ the code is linear; otherwise $k = \sigma$ and $r = \sigma + \tau + \upsilon + 1$.*
3) *In the case $\tau = 2, \overline{\tau} = 1, \upsilon = 1$ we have that if all swappers are in $\mathcal{C}$ then $k = r = \sigma + 3$. If some swappers, but not all, are in $\mathcal{C}$ then $k = \sigma + 1$, $r = \sigma + \tau + \upsilon + 1$. If none of the swappers is in $\mathcal{C}$ then $k = \sigma, r = \sigma + \tau + \upsilon + 2$.*
4) *In the case $\tau \geq \overline{\tau} \geq 2, \upsilon = 1$ we have four excluding possibilities: if $(s_1 : a) \in \mathcal{C}$ for all $a \in A(\mathcal{C})$, then $k = \sigma + \tau - \overline{\tau} + 1$, $r = \sigma + \tau + \upsilon + \binom{\overline{\tau}}{2}$; otherwise if $(s_1 r_a : a) \in \mathcal{C}$ for all $a \in A(\mathcal{C})$ and some $r_a \in \mathcal{R}(\mathcal{C})$ then $k = \sigma + \tau - \overline{\tau} + 1$, $\sigma + \tau + \upsilon + \binom{\overline{\tau}}{2} \leq r \leq \sigma + \tau + \upsilon + \binom{\overline{\tau}+\upsilon}{2}$; otherwise if $(r_1 : s_1) \in \mathcal{C}$ where r_1^2 then $k = \sigma + 1$, $\sigma + \tau + \upsilon + \binom{\overline{\tau}}{2} \leq r \leq \sigma + \tau + \upsilon + \binom{\overline{\tau}+\upsilon}{2}$; otherwise $k = \sigma$, $\sigma + \tau + \upsilon + \binom{\overline{\tau}}{2} \leq r \leq \sigma + \tau + \upsilon + \binom{\tau+\upsilon}{2}$*
5) *In the case $\tau = 2$ and $\upsilon = 2$ if both swappers $(s_2 : r_2)$ and $(s_1 s_2 : r_1 r_2)$ are in $\mathcal{C}$ then we have the linear case; when only one of these swappers belongs to $\mathcal{C}$ we have*

$k = \sigma + 2, r = \sigma + \tau + \upsilon + 1$*; and when none of them belongs to* $\mathcal{C}$ *we have* $k = \sigma, r = \sigma + \tau + \upsilon + 2$

Proof.

1) In the case $\upsilon = 0$ we have an abelian code, shape=1.
If $r_1^2 = \mathbf{u}$, any element $c \in \mathcal{C}$ can be written as $c = xr_1^i r$ with $x \in T(\mathcal{C})$, $r \in R(\mathcal{C})$ and $i \in \{0, 1\}$. It belongs to $K(\mathcal{C})$ if the swapper of c with every element in $\mathcal{C}$ are still in $\mathcal{C}$. Hence, $c \in K(\mathcal{C})$ if and only if $(c : r_1) \in \mathcal{C}$ (always true); $(c : r) \in \mathcal{C}$ (always true); and for all $\overline{r} \in R(\mathcal{C}) : (r : \overline{r}) \in \mathcal{C}$. From Lemma IV.1, we known this last condition implies $r = \mathbf{e}$, thus $K(\mathcal{C}) =< T(\mathcal{C}), r_1 >$. Moreover, from Lemma IV.1 we known all swappers of two elements in $R(\mathcal{C})$ are different, $r = \sigma+\tau+\upsilon+\binom{\tau-1}{2}$
If $r_1^2 \neq \mathbf{u}$, any element $c \in \mathcal{C}$ can be written as $c = xr$ with $x \in T(\mathcal{C})$ and $r \in R(\mathcal{C})$. In a totally equivalent way to previous one, we conclude $K(\mathcal{C}) = T(\mathcal{C})$ and $r = \sigma + \tau + \upsilon + \binom{\tau}{2}$.
2) The case $\tau = 1$ and $\upsilon = 1$ is a direct application of the definitions.
3) In the case $\tau = 2$ and $\upsilon = 1$ and $\overline{\tau} = 1$ the code $\mathcal{C}$ is of shape 2 with $r_1^2 = s_1^2 = \mathbf{u} \neq r_2^2$ or is of shape 4 with $r_1^2 = \mathbf{u} \neq s_1^2 = r_2^2$. Any element $c \in \mathcal{C}$ can be written as $c = xr_1^i r_2^j s_1^k$ where $x \in T(\mathcal{C})$ and $i, j, k \in \{0, 1\}$. It belongs to $K(\mathcal{C})$ if the swapper of c with every element in $\mathcal{C}$ are still in $\mathcal{C}$. Hence, $c \in K(\mathcal{C})$ if and only if $(s_1^k : r_1), (s_1^k : r_2) \in \mathcal{C}$ (recall that if $(s_1 : r_1) \in \mathcal{C}$ and $(s_1 : r_2) \in \mathcal{C}$ then also $(s_1 : r_1 r_2) \in \mathcal{C}$). If all the above swappers are in $\mathcal{C}$ the code $\mathcal{C}$ is linear and $K(\mathcal{C}) = \langle T(\mathcal{C}), r_1, r_2, s_1 \rangle$. Also note that, from Lemma II.2, if $s_1^2 \neq \mathbf{u}$ then $(s_1 : r_1 r_2) \in \mathcal{C}$.
If some swapper does not belong to $\mathcal{C}$, for instance, $(s_1 : r_1) \in \mathcal{C}$ and $(s_1 : r_2) \notin \mathcal{C}$ then $(s_1 : r_1 r_2) = (s_1 : r_1)(s_1 : r_2) \notin \mathcal{C}$, hence $K(\mathcal{C}) = \langle T(\mathcal{C}), r_1 \rangle$. The same argumentation works for the other instances proving the statement.
If none of the swappers belong to $\mathcal{C}$ then $K(\mathcal{C}) = T(\mathcal{C})$. Note that if $s_1^2 \neq \mathbf{u}$ then $M((r_1 r_2)^2) \cap M(s_1^2) = \varnothing$, thus, by Lemma II.2, $(r_1 r_2 : s_1) = \mathbf{e}$

4) In the case $\tau \geq \overline{\tau} \geq 2$ and $\upsilon = 1$ the code is of shape 2 with $r_1^2 = s_1^2 = \mathbf{u}$ or is of shape 3 with $s_1^2 = \mathbf{u} \notin \langle r_1^2 \dots r_\tau^2 \rangle$.
When shape=3 any element $c \in \mathcal{C}$ can be written as $c = xrs_1^i$ where $x \in T(\mathcal{C})$, $r \in R(\mathcal{C})$ and $i \in \{0, 1\}$. It belongs to $K(\mathcal{C})$ if the swapper of c with every element in $\mathcal{C}$ are still in $\mathcal{C}$. Hence, $c \in K(\mathcal{C})$ if and only if for all $\overline{r} \in R(\mathcal{C}) : (c : \overline{r}) \in \mathcal{C} \Leftrightarrow (rs_1^{ks} : \overline{r}) \in \mathcal{C}$ (condition "a") and $(c : s_1) \in \mathcal{C}$ iff $(r : s_1) \in \mathcal{C}$ (condition "b"). We need to remark that if a and b are two elements of $R(\mathcal{C}) \backslash T(\mathcal{C})$ and $(a : s_1) \in \mathcal{C}$ and $(bs_1 : a) \in \mathcal{C}$, then $(b : a) \in \mathcal{C}$ and, from Lemma IV.1, one of the following must be true: $a = e$ or $b = e$ or $a = b$. In other words, there are no two non zero and different elements of $R(\mathcal{C})$ that fulfills conditions "a" and "b". If $(s_1 : \overline{r}) \in \mathcal{C}$ for all $\overline{r} \in R(\mathcal{C})$ then, by previous fact, $r = e$, thus $K(\mathcal{C}) =< T(\mathcal{C}), s_1 >$. If there are at least two elements r_a and r_b that $(s_1 : r_a) \in \mathcal{C}$ and $(s_1 : r_b) \in \mathcal{C}$ but at least one elements r_c that $(s_1 : r_b) \notin \mathcal{C}$, then $r = e$, ks=0, thus $K(\mathcal{C}) = T(\mathcal{C})$. If there are only one element r_a that $(s_1 : r_a) \in \mathcal{C}$ and $(r_a s_1 : \overline{r})$ for all $\overline{r} \in R(\mathcal{C})$, then $(ks = 0$ and $r = \mathbf{e})$ or $(ks = 1 and r = r_a)$, thus $K(\mathcal{C}) =< T(\mathcal{C}), r_a s_1 >$. If none element of $R(\mathcal{C})$ fulfills $(r : s_1) \in \mathcal{C}$ then we have the trivial case $K(\mathcal{C}) = T(\mathcal{C})$.
When shape=2 any element $c \in \mathcal{C}$ can be written as $c = xr_1^{k1} r s_1^{ks}$, where $x \in T(\mathcal{C})$ and $r \in R(\mathcal{C})$. It belongs to $K(\mathcal{C})$ if the swapper of c with every element in $\mathcal{C}$ are still in $\mathcal{C}$. Hence, $c \in K(\mathcal{C})$ if and only if $(s_1^{ks} : r_1) \in \mathcal{C}$; $(s_1^{ks} : r) \in \mathcal{C}$; for all $\overline{r} \in R(\mathcal{C}) : (rs_1^{ks} : \overline{r}) \in \mathcal{C}$; and $(r_1^{k1} r : s_1) \in \mathcal{C}$. Note that if $(r_1, s_1) \in \mathcal{C}$, these conditions becomes the same than previous case, the conclusions still applicable adding r_1 to $K(\mathcal{C})$. If $(r_1, s_1) \notin \mathcal{C}$ it is immediate that $ks = k1 = 0$ and $r = \mathbf{e}$.
5) In the case $\tau = 2$ and $\upsilon = 2$ the code $\mathcal{C}$ is of shape 5 with $r_1^2 = s_1^2 = \mathbf{u} \neq r_2^2 = s_2^2$.
Starting from the standard generator set, define a new generator set where $\overline{r}_1 = r_1 r_2$ and $\overline{s}_1 = s_1 s_2$. Note that $\overline{r}_1^2 = \overline{s}_1^2 = ur_2^2 = us_2^2$. In this way, we have a redefined generator set composed by two pairs of elements with equal square different from u. This fact implies that $M(\overline{r}_1^2) = M(\overline{s}_1^2)$ and $M(r_2^2) = M(s_2^2)$ form a partition of the components. For this reason, $(\overline{r}_1 : r_2) = (\overline{r}_1 : s_2) = (\overline{s}_1 : r_1) = (\overline{s}_1 : r_2) = e$. Any element $c \in \mathcal{C}$ can be written as $c = xr_1^i r_2^j s_1^k$ where $x \in T(\mathcal{C})$ and $i, j, k \in \{0, 1\}$. It belongs to $K(\mathcal{C})$ if the swapper of c with every element in $\mathcal{C}$ are still in $\mathcal{C}$. Hence, $c \in K(\mathcal{C})$ if and only if $(\overline{s}_1^{k3} : \overline{r}_1) \in \mathcal{C}$; $(s_2^{k4} : r_2) \in \mathcal{C}$; $(\overline{r}_1^{k1} : \overline{s}_1) \in \mathcal{C}$; and $(r_2^{k2} : s_2) \in \mathcal{C}$. It is immediate to see that when both $(\overline{r}_1 : \overline{s}_2) \in \mathcal{C}$ and $(r_2 : s_2) \in \mathcal{C}$ are true we have a linear case $K(\mathcal{C}) = \mathcal{C}$; if only one of these swappers belongs to $\mathcal{C}$ we have the case where $k = \sigma + 1$; and if none of these swappers belongs to $\mathcal{C}$ we have $k = \sigma$.

□

B. Construction of $A(\mathcal{C})$

Start by a Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-code $\mathcal{D}$, that could be constructed using the methods described at [7] or [6]. This code will have σ generators of order two and τ generators of order four. In addition, an element with square equal to $\mathbf{u}$ could or not be include on it.

Now, we will create the subgroup $A(\mathcal{C})$ mapping the components of all the elements in the initial code in the following way: if the original component belongs to $\mathbb{Z}_2$ and has value x, the new component is a $\mathbb{Z}_4$ one of value $2x$; if the original component belongs to $\mathbb{Z}_4$, the new component is a Q_8 one of value a^x. Note that in the binary space both operations are equivalent to repeat twice the binary sequence, A is a repetition code of $\mathcal{D}$.

C. Construction of $\mathcal{C}$

After construction of $A(\mathcal{C})$ following previous previous subsection steps, we need to choice one or two more generators, s_1 and s_2. These generators must not commute with $A(\mathcal{C})$, thus, we will choice its components of order four in

$\{b,ab,a^2b,a^3b\}$. As we have see, rank and kernel of the final code depends on the choice of s_1 and s_2.

The following table resumes the values of kernel dimension and rank in each one of the previous cases (except the Abelian ones) when $r_1^2 = \mathbf{u}$:

$k-\sigma$	$r-\sigma-\tau-\upsilon^{[rule]}$			
0	$1^{[2b]}$	$2^{[3c]}$	$\binom{\tau-1}{2}\ldots\binom{\tau+1}{2}^{[4d]}$	$-$
1	$-$	$1^{[3b]}$	$\binom{\tau-1}{2}\ldots\binom{\tau}{2}^{[4c]}$	$-$
2	$0^{[2a]}$	$-$	$\binom{\tau-1}{2}\ldots\binom{\tau}{2}^{[4a,4b]}$	$-$
3	$-$	$0^{[3a]}$	$-$	$-$
4	$-$	$-$	$-$	$-$

The following table resumes the values of kernel dimension and rank in each one of the previous cases (except the Abelian ones) when $r_1^2 \neq \mathbf{u}$:

$k-\sigma$	$r-\sigma-\tau-\upsilon^{[rule]}$			
0	$1^{[2b]}$	$-$	$\binom{\tau}{2}\ldots\binom{\tau+1}{2}^{[4d]}$	$2^{[5c]}$
1	$-$	$-$	$\binom{\tau}{2}\ldots\binom{\tau+1}{2}^{[4a,4b]}$	$-$
2	$0^{[2a]}$	$-$	$-$	$1^{[5b]}$
3	$-$	$-$	$-$	$-$
4	$-$	$-$	$-$	$0^{[5a]}$

Example IV.3. *Start with the Abelian code generated by:*

$$r_1 = (1,\ a,\ a^2,\ a^3,\ 1,\ a,\ a^2,\ a^3,\ 1,\ a,\ a^2,\ a^3,\ 1,\ a,\ a^2,\ a^3)$$

with $\sigma = 1, \tau = 1, \upsilon = 0$, rank $r = 2$ and dimension of the kernel $k = 2$.

A linear code with $k = r = \sigma + \tau + \upsilon = 3$ can be constructed applying rule [2a]. This rule request that $(s_1 : r_1) \in \mathcal{C}$. In addition, we have already said that s_1^2 must belong to the original code. By example, if we choice $s_1 = (1, b, a^2, b, a^2, b, 1, b, 1, b, a^2, b, a^2, b, 1, b)$, the new code has $\sigma = 1, \tau = 1, \upsilon = 1$, rank $r = 3$ and dimension of the kernel $k = 3$.

A linear code with $k = \sigma = 1$ and $r = \sigma + \tau + \upsilon + 1 = 4$ can be constructed applying rule [2b]. This rule request that $(s_1 : r_1) \notin \mathcal{C}$. In addition, we have already said that s_1^2 must belong to the original code. By example, if we choice $s_1 = (1, b, a^2, b, a^2, ab, 1, ab, 1, b, a^2, b, a^2, ab, 1, ab)$, the new code has $\sigma = 2, \tau = 2, \upsilon = 1$, dimension of the kernel $k = 1$ and $r = 4$.

V. Conclusion

In summary, we have analyzed some error-correcting codes via algebraic methods, giving a with central relevance to Hadamard error-correcting codes and $\mathbb{Z}_2$, $\mathbb{Z}_4$ and Q_8 algebraic groups.

The first sections, the ntroduction and the preliminaries, show how the codes of this kind can be taken, by a suitable Gray map, as the image of a subgroup of a direct product of $\mathbb{Z}_2$, $\mathbb{Z}_4$ and Q_8, the quaternion group of order 8 [2]. The main invariant parameters and other useful characteristics are defined.

In Section III, it has been presented the analysis of the structure and main properties (dimension of the kernel, rank,...) of Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-codes or $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes. We have presented a new standardized form for the generator set of these codes. This standardized form is unique (except trivial equivalences) and allows an easy recognition of the shape of the code, together with the computation of some remarkable values and bounds, like the ones for dimension of the kernel and rank.

Next section IV gives a method to construct Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-codes starting with preselected values for the dimension of the kernel and rank. The method uses a detailed table of the conditions that a code must fulfill, as well as exact bounds for all possible values of the dimension of the kernel and rank. After looking this table up, the conditions are settled and the construction method shows how to obtain a generator set accomplishing these restrictions.

Examples of the construction are provided. The paper finish with bibliographic references to the main works on this topic.

References

[1] A. R. Hammons Jr, P. V. Kumar, A. R. Calderbank, N. J. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals, and related codes," *IEEE Trans. Inform. Theory.*, vol. 40, no. 2, pp. 301–319, 1994.

[2] J. Rifà and J. Pujol, "Translation-invariant propelinear codes," *IEEE Trans. Inform. Theory.*, vol. 43, no. 2, pp. 590–598, 1997.

[3] A. del Rio and J. Rifà, "Families of hadamard $\mathbb{Z}_2\mathbb{Z}_4q_8$-codes," *IEEE Trans. Inform. Theory.*, pp. 5140–5151, 2012.

[4] E. F. Assmus and J. D. Key, *Designs and their Codes*. Cambridge University Press, 1992, vol. 103.

[5] J. Borges, C. Fernández, and J. Rifà, "Every $\mathbb{Z}_{2k}$-code is a binary propelinear code," *COMB*, vol. 1, pp. 100–102, 2001.

[6] K. T. Phelps, J. Rifà, and M. Villanueva, "On the additive ($\mathbb{Z}_2\mathbb{Z}_4$-linear and non-$\mathbb{Z}_2\mathbb{Z}_4$-linear) hadamard codes: rank and kernel," *IEEE Trans. Inform. Theory.*, vol. 52, no. 1, pp. 316–319, 2006.

[7] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. Villanueva, "$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality," *Designs, Codes and Cryptography*, vol. 54, no. 2, pp. 167–179, 2010.

[8] J. Borges and J. Rifà, "A characterization of 1-perfect additive codes," *IEEE Trans. Inform. Theory.*, vol. 45, no. 5, pp. 1688–1697, 1999.

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

[10] J. Doyen, X. Hubaut, and M. Vandensavel, "Ranks of incidence matrices of steiner triple systems," *Mathematische Zeitschrift*, vol. 163, no. 3, pp. 251–259, 1978.

[11] C. Fernández-Córdoba, J. Pujol, and M. Villanueva, "$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel," *Designs, Codes and Cryptography*, vol. 56, no. 1, pp. 43–59, 2010.

[12] D. Krotov, "$\mathbb{Z}_4$-linear hadamard and extended perfect codes," *arXiv preprint arXiv:0710.0199*, 2007.

[13] F. F. J. MacWilliams and N. N. J. A. Sloane, *The Theory of Error-correcting Codes: Part 2*. Elsevier, 1977, vol. 16.

[14] K. T. Phelps, J. Rifà, and M. Villanueva, "Rank and kernel of binary hadamard codes," *IEEE Trans. Inform. Theory.*, vol. 51, no. 11, pp. 3931–3937, 2005.

[15] J. Rifà, J. M. Basart, and L. Huguet, "On completely regular propelinear codes," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*. Springer, 1989, pp. 341–355.

[16] L. Teirlinck, "On projective and affine hyperplanes," *Journal of Combinatorial Theory, Series A*, vol. 28, no. 3, pp. 290–306, 1980.