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

Á. del Rio†, J. Rifà, ‡

Abstract

A $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code is the binary image, after a Gray map, of a subgroup of $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$, where Q_8 is the quaternion group on eight elements. Such $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes are translation invariant propelinear codes as are the well known $\mathbb{Z}_4$-linear or $\mathbb{Z}_2\mathbb{Z}_4$-linear codes.

In the current paper, we show that there exist "pure" $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes, that is, codes that do not admit any abelian translation invariant propelinear structure. We study the dimension of the kernel and rank of the $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes, and we give upper and lower bounds for these parameters. We give tools to construct a new class of Hadamard codes formed by several families of $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes; we classify such codes from an algebraic point of view and we improve the upper and lower bounds for the rank and the dimension of the kernel when the codes are Hadamard.

1 Introduction

The discovery of the existence of a quaternary structure in some relevant families with better parameters than any linear code has raised the interest in the study of these codes [8] and more generally on codes with a group structure. From the Coding Theory perspective it is desired that the group operation preserves the Hamming distance. This is the case, for example, of the $\mathbb{Z}_2\mathbb{Z}_4$-linear codes which has been intensively studied during the last years. More generally, the propelinear codes and, specially those which are translation invariant, are particularly interesting because both left and right product preserves the Hamming distance. Translation invariant propelinear codes has been characterized as the image of a subgroup by a suitable Gray map of a direct product of $\mathbb{Z}_2$, $\mathbb{Z}_4$ and Q_8, the quaternion group of order 8 [14]. Hence it makes sense to call this codes as $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes. The aim of this paper is to study the structure and main properties of $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes with special focus on those that are Hadamard codes as well.

Section 2 has been reserved for notation and preliminaries.

As far a we know there is not any example in the literature of a proper $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code, i.e., one which is not equivalent to a $\mathbb{Z}_2\mathbb{Z}_4$-linear code. The first

*This work has been partially supported by the Spanish Government under Grants MTM2009-08435 and MTM2012-35240, including funds from ERDF, and by the Catalan AGAUR and Fundación Séneca of Murcia under Grants 2009SGR1224 and 04555/GERM/06, respectively.

†Á. del Río is with the Department of Mathematics, Universidad de Murcia, Spain.

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

result of this paper consists in providing such an example. This result appears in Section 3, where we also study the group-theoretical properties of the $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes and the relation of this structure with its rank and the dimension of its kernel. This structure suggests associating three numerical parameters to the group. We will show that these parameters provide bounds for the rank and dimension of the kernel. Moreover, our example of a proper $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code shows that these bounds are tight.

Section 4 is dedicated to Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. The Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-linear codes as well as the (extended) 1-perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes are well known [4, 9, 12]. The Hadamard linear codes are dual of extended 1-perfect codes. However we will show that the extended 1-perfect codes, involving at least one quaternionic component do not exist for length $n \geq 8$. For every $n = 2^m$ there is a unique Hadamard linear code, up to equivalence. If $m \leq 3$ this is the unique Hadamard code. However, there are five inequivalent Hadamard codes of length 16. One of them is linear, another is a $\mathbb{Z}_2\mathbb{Z}_4$-linear code and the other three cannot be realized as $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. We will show that exactly one of these three can be realized as a $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code, more specifically, as a pure Q_8-code. This provides another example of such codes. In Theorem 4.11 we provide a precise description of the possible group structures of a Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes and in Corollary 4.12 we obtain bounds for the rank of a Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code which are better than those for general $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes.

In the last section of the paper we introduce two constructions of $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes which allow to construct many Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes.

2 Preliminaries

Let $\mathbb{Z}_2$ and $\mathbb{Z}_4$ denote the binary field and the ring of integers modulo 4, respectively. Let $\mathbb{Z}_2^n$ denote the set of all binary vectors of length n and let $\mathbb{Z}_4^n$ be the set of all n-tuples over the ring $\mathbb{Z}_4$. The all-zero vector in $\mathbb{Z}_2^n$ is denoted by $\mathbf{0}$. Let $\mathrm{wt}(v)$ denote the *Hamming weight* of a vector $v \in \mathbb{Z}_2^n$ (i.e., the number of its nonzero coordinates), and let $d(v,u) = \mathrm{wt}(v+u)$, the *Hamming distance* between two vectors $v, u \in \mathbb{Z}_2^n$.

Any non-empty subset of $\mathbb{Z}_2^n$ is called a binary code and a linear subspace of $\mathbb{Z}_2^n$ is called a *binary linear code* or a $\mathbb{Z}_2$*-linear code*. Similarly, any non-empty subset of $\mathbb{Z}_4^n$ is a quaternary code and a subgroup of $\mathbb{Z}_4^n$ is called a *quaternary linear code* [8]. Quaternary codes can be viewed as binary codes under the Gray map defined as

$$\varphi(0) = (0,0),\ \varphi(1) = (0,1),\ \varphi(2) = (1,1),\ \varphi(3) = (1,0),$$

which is extended coordinatewise to a bijection $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$. If $\mathcal{C}$ is a quaternary linear code of length n, then the binary code $C = \varphi(\mathcal{C})$ is said to be a $\mathbb{Z}_4$*-linear code* of binary length $2n$ [8].

Let Q_8 be the *quaternion group* on eight elements. The following equalities provides a presentation and the list of elements of Q_8:

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

A *quaternionic code* $\mathcal{C}$ is a non-empty subgroup of Q_8^n. Quaternionic codes can also be seen as binary codes under the following Gray map: $\phi : Q_8 \longrightarrow \mathbb{Z}_2^4$, such that

$$\begin{array}{ll} \phi(\mathbf{1}) = (0,0,0,0), & \phi(\mathbf{b}) = (0,1,1,0), \\ \phi(\mathbf{a}) = (0,1,0,1), & \phi(\mathbf{ab}) = (1,1,0,0), \\ \phi(\mathbf{a}^2) = (1,1,1,1), & \phi(\mathbf{a}^2\mathbf{b}) = (1,0,0,1), \\ \phi(\mathbf{a}^3) = (1,0,1,0), & \phi(\mathbf{a}^3\mathbf{b}) = (0,0,1,1). \end{array} \tag{1}$$

We will also denote by ϕ the componentwise extended map from Q_8^n to $\mathbb{Z}_2^{4n}$. If $\mathcal{C}$ is a quaternionic code, then we will say that $C = \phi(\mathcal{C})$ is a Q_8-*code* of binary length $4n$.

Binary linear codes, $\mathbb{Z}_4$-linear codes and Q_8-codes can be seen as particular cases of a more general family of codes. More specifically, given non-negative integers k_1, k_2 and k_3 we can define the generalized Gray map

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

such that if $x \in \mathbb{Z}_2^{k_1}$, $y \in \mathbb{Z}_4^{k_2}$ and $z \in Q_8^{k_3}$ then

$$\Phi(x, y, z) = (x, \varphi(y), \phi(z)).$$

A $\mathbb{Z}_2\mathbb{Z}_4Q_8$-*code* is a binary code C of the form $C = \Phi(\mathcal{C})$ where $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$.

Notice that if $k_1 > 0$ and $k_2 = k_3 = 0$ then C is a binary linear or $\mathbb{Z}_2$-linear code. If $k_2 > 0$ and $k_1 = k_3 = 0$, then C is a $\mathbb{Z}_4$-linear code. If $k_3 > 0$ and $k_1 = k_2 = 0$, then C is a Q_8-code. Finally, if $k_3 = 0$, then C is called a $\mathbb{Z}_2\mathbb{Z}_4$-linear code [3] (hence, including the cases $\mathbb{Z}_2$-linear and $\mathbb{Z}_4$-linear). We also remark that $\mathcal{C}$ is abelian if and only if C is a $\mathbb{Z}_2\mathbb{Z}_4$-linear code.

We use additive notation for $\mathbb{Z}_2$ and $\mathbb{Z}_4$ and multiplicative notation for Q_8. Therefore, $(0, \overset{k_1+k_2}{\ldots}, 0, \mathbf{1}, \overset{k_3}{\ldots}, \mathbf{1})$ is the identity of $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$. We denote this element as $\mathbf{e}$. We also denote it $\mathbf{e}_{k_1,k_2,k_3}$ or $\mathbf{e}_l$, with $l = k_1 + k_2 + k_3$, when we want to emphasize the ambient space of $\mathbf{e}$. Note that each one of the groups $\mathbb{Z}_2$, $\mathbb{Z}_4$ and Q_8 have exactly one element of order 2. So there is a unique element $\mathbf{u}$ of $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$ which has the element of order 2 in each coordinate. This element is also determined by the fact that $\Phi(\mathbf{u})$ is the all one vector. As for $\mathbf{e}$, we also denote $\mathbf{u}$ by $\mathbf{u}_{k_1,k_2,k_3}$ or $\mathbf{u}_l$, with $l = k_1+k_2+k_3$ if we want to emphasize its ambient space.

If $h \in \mathbb{Z}$ and $w = (x, y, z) \in \mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$, where $x \in \mathbb{Z}_2^{k_1}$, $y \in \mathbb{Z}_4^{k_2}$ and $z \in Q_8^{k_3}$, then

$$w^h = (hx, hy, z^h).$$

The order of w is the smallest positive integer h such that $w^h = \mathbf{e}$.

Let $\mathcal{S}_n$ denote the symmetric group of permutations on the set $\{1, \ldots, n\}$. For any $\pi \in \mathcal{S}_n$ and any vector $v = (v_1, \ldots, v_n) \in \mathbb{Z}_2^n$, we write $\pi(v)$ to denote the vector $(v_{\pi^{-1}(1)}, \ldots, v_{\pi^{-1}(n)})$.

Two binary codes C_1 and C_2 of length n are said to be *isomorphic* if there is a coordinate permutation $\pi \in \mathcal{S}_n$ such that $C_2 = \{\pi(x) : x \in C_1\}$. They are said to be *equivalent* if there is a vector $y \in \mathbb{Z}_2^n$ and a coordinate permutation $\pi \in \mathcal{S}_n$ such that $C_2 = \{y + \pi(x) : x \in C_1\}$. Although the two definitions above stand for two different concepts, two binary linear codes are equivalent if and only if they are isomorphic.

A binary code C of length n is said to be *propelinear* [13] if for any codeword $x \in C$ there exists $\pi_x \in \mathcal{S}_n$ satisfying the following properties for all $v \in \mathbb{Z}_2^n$ and $x, y \in C$:

1. $x + \pi_x(y) \in C$ and
2. $\pi_x(\pi_y(v)) = \pi_z(v)$, where $z = x + \pi_x(y)$.

Let C be a propelinear code and for every $x \in C$ let $\pi_x \in S_n$ satisfy the above conditions. For all $x \in C$ and $y \in \mathbb{Z}_2^n$ let $xy = x + \pi_x(y)$. This endows C with a group structure, which is not abelian in general. Therefore, the vector $\mathbf{0}$ is always a codeword and $\pi_{\mathbf{0}}$ is the identity permutation I. Hence, $\mathbf{0}$ is the identity element in C and $x^{-1} = \pi_x^{-1}(x)$ for all $x \in C$ [13]. Notice that a binary code may have several structures of propelinear code with different group structures.

The following lemma is straightforward [13, 14, 4].

Lemma 2.1. *Let C be a propelinear code of length n. Then,*

$$d(u, v) = d(xu, xv) \text{ for all } x \in C \text{ and } u, v \in \mathbb{Z}_2^n.$$

This means that left multiplication in a propelinear code is *Hamming compatible* [2] in the sense that $d(xz, x) = \mathrm{wt}(z)$ for all $x \in C$ and $z \in \mathbb{Z}_2^n$.

Definition 2.2. *A propelinear code C of length n is said to be* translation invariant *if*

$$d(x, y) = d(xu, yu) \text{ for all } x, y \in C \text{ and } u \in \mathbb{Z}_2^n.$$

In [14], it is proven that a binary code is translation invariant propelinear if and only if it is a $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code. Then, a translation invariant propelinear binary code is isomorphic to $C = \Phi(\mathcal{C})$ for a subgroup of $\mathcal{G} = \mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$. The permutation π_x associated to each element of $\mathcal{G}$ is obtained by concatenation of permutations in each $\mathbb{Z}_4$ or Q_8 block, such that the permutation in a component of order at most 2 is the identity; the permutation of a $\mathbb{Z}_4$-coordinate of order 4 is the transposition of the binary components and of a Q_8-coordinate of order 4 is a product of two disjoint transpositions of the four binary components. More precisely, if $w = (x_1, \ldots, x_{k_1}, y_1, \ldots, y_{k_2}, z_1, \ldots, z_{k_3})$ and $w' = \Phi(w)$ then $\pi_{w'} = \sigma_1 \ldots \sigma_{k_2} \delta_1 \ldots \delta_{k_3}$ where

$$\sigma_i = \begin{cases} I, & \text{if } y_i \in \{0, 2\}; \\ (k_1 + 2i - 1, k_1 + 2i), & \text{if } y_i \in \{1, 3\}. \end{cases}$$

and if $t = k_1 + 2k_2$ then

$$\delta_i = \begin{cases} I, & \text{if } z_i \in \{\mathbf{1}, \mathbf{a}^2\}; \\ (s_i - 3, s_i - 2)(s_i - 1, s_i), & \text{if } z_i \in \{\mathbf{a}, \mathbf{a}^3\}; \\ (s_i - 3, s_i - 1)(s_i - 2, s_i), & \text{if } z_i \in \{\mathbf{b}, \mathbf{a}^2\mathbf{b}\}; \\ (s_i - 3, s_i)(s_i - 2, s_i - 1), & \text{if } z_i \in \{\mathbf{ab}, \mathbf{a}^3\mathbf{b}\}, \end{cases}$$

where $s_i = t + 4i$.

The *rank* of a binary code C is the dimension of the binary vector space generated by its codewords. We denote the rank of C with $r(C)$ or simply r. The *kernel* of a binary code C of length n is

$$K(C) = \{z \in \mathbb{Z}_2^n \,:\, C + z = C\}.$$

If C contains the all-zero vector, then $K(C)$ is a linear subcode of C. The dimension of $K(C)$ is denoted with $k(C)$ or simply k. These two parameters, the rank and dimension of the kernel, can be used to classify binary codes, since if two binary codes have different ranks or dimensions of the kernel, they are non-equivalent. Note that if C is a propelinear code and $x \in C$ is such that $\pi_x = I$ then $x \in K(C)$.

The binary code C can be partitioned by $K(C)$-cosets and therefore $|C|$ is a multiple of $|K(C)|$. Since the union of $K(C)$ and anyone of its cosets is again linear, it is clear that either C is linear or $|C| > 2|K(C)|$.

If C is not linear and $\overline{C}$ is the linear span of C then $|K(C)|$ divides $|\overline{C}|$ and $|\overline{C}| > |C|$. Therefore, $|\overline{C}| \geq 4|K(C)|$ and $r = \log_2(|\overline{C}|) \geq \log_2(4|K(C)|) = k+2$. If moreover C is a $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code then $|C|$ is a power of 2 and therefore, if C is not linear then $|C| \geq 4|K(C)|$. Hence, $|\overline{C}| \geq 8|K(C)|$ and $r \geq k+3$. We summarize this in the following lemma.

Lemma 2.3. *If C is a non-linear binary code then $r(C) \geq k(C)+2$. If moreover C is a $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code then $r(C) \geq k(C)+3$.*

A *Hadamard matrix* of order n is a matrix of size $n \times n$ with entries ± 1, such that $HH^T = nI$. We can easily see that any two rows (columns) of a Hadamard matrix agree in precisely $n/2$ coordinates. If $n > 2$ then any three rows (columns) agree in precisely $n/4$ coordinates. Thus, if $n > 2$ and there is a Hadamard matrix of orden n then n is multiple of 4. It is conjectured that the converse holds, i.e., if n es multiple of 4 then there are Hadamard matrices of order n [1].

Two *Hadamard matrices* are *equivalent* if one can be obtained from the other by permuting rows and/or columns and multiplying rows and/or columns by -1. With the last operations we can change the first row and column of H into $+1$'s and we obtain an equivalent Hadamard matrix which is called normalized. If $+1$'s are replaced by 0's and -1's by 1's, the initial Hadamard matrix is changed into a (binary) Hadamard matrix and, from now on, we will refer to it when we deal with Hadamard matrices. The binary code consisting of the rows of a (binary) Hadamard matrix and their complements is called a (binary) *Hadamard code*, which is of length n, with $2n$ codewords, and minimum distance $n/2$.

A perfect one error correcting binary code (1-perfect code) is a binary code of length $2^m - 1$, minimum distance 3, and 2^{n-m} codewords. Linear 1-perfect codes (Hamming codes) exist for all $m > 1$ and also there exist $\mathbb{Z}_2Z_4$-linear 1-perfect codes for all admissible $n \geq 15$. If C is a binary 1-perfect code, the extended code C^* by a parity check coordinate is a code of length 2^m and minimum distance 4. When code C^* is linear or $\mathbb{Z}_2\mathbb{Z}_4$-linear there exist the dual code $(C^*)^\perp$, which is a Hadamard code.

In general, by the dual of the (non necessarily linear) code C, which will be denoted by $C^\perp$, we mean the dual of the subspace spanned by C.

3 Properties of $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes. Rank and dimension of the kernel.

In this section we study some of the group theoretical properties of $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes. We also present an example of a pure Q_8-code, i.e., a Q_8-code which is

not equivalent to a $\mathbb{Z}_2\mathbb{Z}_4$-linear code.

All throughout $\mathcal{G} = \mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$. We also fix a non-trivial subgroup $\mathcal{C}$ of $\mathcal{G}$ and let $C = \Phi(\mathcal{C})$. Then, the length of C is $n = k_1 + 2k_2 + 4k_3$ and we set $l = k_1 + k_2 + k_3$.

We use the notation below for $x, y \in \mathcal{G}$:

$$\begin{aligned} x^y &= y^{-1}xy, \text{ conjugate of } x \in \mathcal{C} \text{ by } y \in \mathcal{C}, \\ [x,y] &= x^{-1}y^{-1}xy, \text{ commutator of } x, y \in \mathcal{C}, \\ \mathcal{C}' &= \langle [x,y] : x, y \in \mathcal{C} \rangle, \text{ commutator subgroup of } \mathcal{C}, \\ Z(\mathcal{C}) &= \{z \in \mathcal{C} : zx = xz, x \in \mathcal{C}\}, \text{ the center of } \mathcal{C}, \\ T(\mathcal{C}) &= \{z \in \mathcal{C} : z^2 = \mathbf{e}\}. \end{aligned}$$

Note that

$$\mathcal{C}' \subseteq T(\mathcal{C}) \subseteq Z(\mathcal{C}) \tag{2}$$

and hence, both $\mathcal{C}'$ and $T(\mathcal{C})$ are central subgroups of $\mathcal{C}$. This implies that

$$[x,y] = [y,x] \text{ and } [xy,z] = [x,z][y,z] \tag{3}$$

for every $x, y, z \in \mathcal{C}$.

Definition 3.1. *We say that $\mathcal{C}$ is of type (σ, δ, ρ) if $|T(\mathcal{C})| = 2^\sigma$, $[Z(\mathcal{C}) : T(\mathcal{C})] = 2^\delta$ and $[\mathcal{C} : Z(\mathcal{C})] = 2^\rho$.*

For instance, if $\delta = \rho = 0$ then C is a linear code and if C is a $\mathbb{Z}_2\mathbb{Z}_4$-linear code then $\mathcal{C} \cong \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ for some non-negative integers γ and δ. In the latter case $\sigma = \gamma + \delta$ and $\rho = 0$. Note that the type depends on the group $\mathcal{C}$ rather than on the binary code C. For example, if $\mathcal{C} = \mathbb{Z}_4$ then the type of $\mathcal{C}$ is $(1,1,0)$. However the corresponding binary code is $\mathbb{Z}_2^2$ and henceforth, it is also the binary code of a subgroup of $\mathbb{Z}_2^2$ of type $(2,0,0)$. Similarly, if $\mathcal{C} = Q_8$ then $\mathcal{C}$ has type $(1,0,2)$ but C is linear and hence it is also the binary code of a group of type $(3,0,0)$.

Assume that $\mathcal{C}$ is of type (σ, δ, ρ). Clearly $T(\mathcal{C}) \cong \mathbb{Z}_2^\sigma$. Moreover, as every element of $\mathcal{G}$ has order 1, 2 or 4, we have that $x^2 \in T(\mathcal{C})$ for every $x \in \mathcal{C}$ and, therefore, $\mathcal{C}/T(\mathcal{C}) \cong \mathbb{Z}_2^{\delta+\rho}$, $Z(\mathcal{C})/T(\mathcal{C}) \cong \mathbb{Z}_2^\delta$ and $\mathcal{C}/Z(\mathcal{C}) \cong \mathbb{Z}_2^\rho$.

Furthermore, $\sigma \geq \delta$ and $\mathcal{C}$ is generated by $\sigma + \delta + \rho$ elements: $x_1, \ldots, x_\sigma$; $y_1, \ldots, y_\delta$; $z_1, \ldots, z_\rho$ with $T(\mathcal{C}) = \langle x_1 \rangle \times \cdots \times \langle x_\sigma \rangle$ and
$Z(\mathcal{C}) = \langle x_1, \ldots, x_\sigma, y_1, \ldots, y_\delta \rangle \cong \mathbb{Z}_2^{\sigma-\delta} \times \mathbb{Z}_4^\delta$.

Using (2) it easily follows that any element $c \in \mathcal{C}$ can be written in a unique way as

$$c = \prod_{i=1}^{\sigma} x_i^{\alpha_i} \prod_{j=1}^{\delta} y_j^{\beta_j} \prod_{k=1}^{\rho} z_k^{\gamma_k},$$

where $\alpha_i, \beta_j, \gamma_k \in \{0,1\}$. Note that the elements $z_1, \ldots, z_\rho$ do not commute among them, but we interpret $\prod_{k=1}^{\rho} z_k^{\gamma_k}$ as $z_1^{\gamma_1} \cdots z_\rho^{\gamma_\rho}$. Moreover, $c \in T(\mathcal{C})$ if and only if $\beta_j = 0$ for every j and $\gamma_k = 0$ for every k; and $c \in Z(C)$ if and only if $\gamma_k = 0$ for every k. In particular, the y_j's and z_k's have order 4.

In the remainder of the paper when we write

$$\mathcal{C} = \langle x_1, \ldots, x_\sigma;\ y_1, \ldots, y_\delta;\ z_1, \ldots, z_\rho\ \rangle \tag{4}$$

we are assuming that $x_1, \ldots, x_\sigma; y_1, \ldots, y_\delta;\ z_1, \ldots, z_\rho$ is a generating set of $\mathcal{C}$ satisfying the above conditions.

Lemma 3.2. *Let $a, b \in \mathcal{C} \setminus T(\mathcal{C})$.*

1. *If $[a,b] = \mathbf{e}$ and $a^2 = b^2$ then $ab \in T(\mathcal{C})$.*
2. *a^2, b^2 and $[a,b]$ coincide in each non-trivial coordinate of $[a,b]$. In particular, $\mathrm{wt}(\Phi([a,b]) \leq \mathrm{wt}(\Phi(a^2))$.*
3. *If $\mathcal{C}$ is of type (σ, δ, ρ) then $\sigma \geq \delta + \min\{1, \rho\}$.*

Proof. 1. Assume that $a^2 = b^2$ and $[a,b] = \mathbf{e}$. As $a^4 = \mathbf{e}$, we have $b^2 = a^2 = a^{-2}$ and hence $(ab)^2 = a^2b^2 = \mathbf{e}$.

2. Let $a = (a_1, \ldots, a_l)$ and $b = (b_1, \ldots, b_l)$. If the commutator $[a_i, b_i]$ is non-trivial then a_i and b_i are two non-commuting elements of Q_8 and hence $[a_i, b_i] = a_i^2 = b_i^2$.

3. We know $\sigma \geq \delta$. Thus, if $\rho = 0$ then the desired inequality is clear. Assume otherwise that $\rho \neq 0$ and $z_1^2 \in \langle y_1^2, \ldots, y_\delta^2 \rangle$ then, by item 1, $y_1^{\alpha_1} \ldots y_\delta^{\alpha_\delta} z_1 \in T(\mathcal{C})$ for some integers $\alpha_1, \ldots, \alpha_\delta$, contradicting the construction of the generating set. Thus $\langle y_1^2, \ldots, y_\delta^2, z_1^2 \rangle$ is a subgroup of $T(\mathcal{C})$ isomorphic to $\mathbb{Z}_2^{\delta+1}$ and hence $\sigma \geq \delta + 1$. □

Definition 3.3. *The* swapper *of $x, y \in \mathcal{G}$ is*

$$(x : y) = \Phi^{-1}(\Phi(x) + \Phi(y) + \Phi(xy)).$$

We define the swapper of $\mathcal{C}$ as the set,

$$S(\mathcal{C}) = \{(x : y) : x, y \in \mathcal{C}\}.$$

Note that if $x = (x_1, \ldots, x_l), y = (y_1, \ldots, y_l) \in \mathcal{C}$ then

$$(x : y) = ((x_1 : y_1), \ldots, (x_l : y_l)). \tag{5}$$

Therefore, to compute a swapper in $\mathcal{G}$ it is enough to compute the swapper in $\mathbb{Z}_2$, $\mathbb{Z}_4$ and Q_8. Clearly $(x : y) = \mathbf{e}$ for $x, y \in \mathbb{Z}_2$. The following tables describe the values of all the swappers in $\mathbb{Z}_4$ and Q_8:

	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 1: Swappers in $\mathbb{Z}_4$ and Q_8

In particular $(x : y) \in T(\mathcal{G})$ and this implies that

$$\Phi((x : y)\, xy) = \Phi((x : y)) + \Phi(xy) = \Phi(x) + \Phi(y), \tag{6}$$

i.e., the swapper of x and y is the element needed to pass from $\Phi(xy)$ to $\Phi(x) + \Phi(y)$.

Using (5) and the swapper tables of $\mathbb{Z}_4$ and Q_8 one can easily prove the following properties about swappers.

Lemma 3.4. *Let $x, y, z, t \in \mathcal{G}$ and let $C = \Phi(\mathcal{C})$ be a $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code.*

(a) If $z^2 = \mathbf{e}$ then $(zx : y) = (x : zy) = (x : y)$ and $(z : x) = (x : z) = \mathbf{e}$.

(b) $\left(x : x^{-1}\right) = (x : x)$.

(c) $(x : y)\,(y : x) = [x, y]$.

(d) $(x : x) = x^2$.

(e) $(x : yz) = (x : y)\,(x : z)$ and $(xy : z) = (x : z)\,(y : z)$.

(f) If $\Phi(x) \in K(C)$ then $(x : y) \in \mathcal{C}$ for any $y \in \mathcal{C}$.

The following lemma is a consequence of the definition of swapper and the above properties.

Lemma 3.5 (Lower bound for $k(C)$)**.** *Let $C = \phi(\mathcal{C})$ be a $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code of type (σ, δ, ρ). Then $\Phi(T(\mathcal{C})) \subseteq K(C)$ and hence $\sigma \leq k(C)$.*

Proof. Let $x \in T(\mathcal{C})$, where $T(\mathcal{C})$ is the subgroup of the elements $x \in \mathcal{C}$ such that $x^2 = \mathbf{e}$. We want to show that $\Phi(x) \in K(C)$. To do this, we check if $\Phi(x) + \Phi(y) \in C$ for any $y \in \Phi(\mathcal{C})$. From Lemma 3.4 (a) we have $(x : y) = (y : x) = \mathbf{e}$ and so, from (6) we have $\Phi(x) + \Phi(y) = \Phi(xy) + \Phi((x : y)) = \Phi(xy) \in C$. This proves the statement. □

Whenever we have a quotient group G/N, with G a group and N a normal subgroup of G, and the meaning is clear from the context we use the standard bar notation for the N-coset containing g, i.e., if $g \in G$ then $\overline{g} = gN$.

Lemma 3.6 (Upper bound for $r(C)$)**.** *Let $\mathcal{C}$ be a subgroup of $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q_8^{k_3}$ with $l = k_1 + k_2 + k_3$ such that $C = \Phi(\mathcal{C})$ is of type (σ, δ, ρ). Let $\mathcal{D} = \langle \mathcal{C} \cup S(\mathcal{C}) \rangle$, the group generated by $\mathcal{C}$ and the swappers of the elements of $\mathcal{C}$. Then*

1. *$\Phi(\mathcal{D})$ is the binary linear span of C;*
2. *$r(C) = \sigma + \delta + \rho + h$ with $h \leq \min\left\{\binom{\delta+\rho}{2}, l - \sigma\right\}$;*

Proof. By (6), it is clear that $\Phi(\mathcal{D})$ is included in the linear span of C. To prove the inverse it is enough to show that $\Phi(\mathcal{D})$ is closed under addition. To see this let $x_1, x_2 \in \mathcal{D}$. As all the swappers have order at most 2 we have $x_1 = b_1c_1$ and $x_2 = b_2c_2$ with $b_1, b_2 \in \mathcal{C}$ and $c_1, c_2 \in \langle (c : c') : c, c' \in \mathcal{C} \rangle$. Then, by (6) and Lemma 3.4(a), we have $\Phi(x_1) + \Phi(x_2) = \Phi(x_1x_2\,(x_1 : x_2)) = \Phi(b_1b_2c_1c_2\,(b_1 : b_2)) \in \Phi(\mathcal{D})$. Item 1 is proved.

Let $\mathcal{C} = \langle K(\mathcal{C}), a_1, \ldots, a_t \rangle$, where t is minimal and $K(\mathcal{C})) = \Phi^{-1}(K(C))$. Since $T(\mathcal{C}) \subseteq K(\mathcal{C})$, we have $a_i^2 \in K(\mathcal{C})$ for every i and $t \leq \delta + \rho$. Let $c, c' \in \mathcal{C}$. Then, using (2) it follows that $c = xa_1^{\alpha_1} \cdots a_t^{\alpha_t}$ and $c' = x'a_1^{\beta_1} \cdots a_t^{\beta_t}$ with $x, x' \in K(\mathcal{C})$ and each $\alpha_i, \beta_i \in \{0, 1\}$. Using Lemma 3.4 we have

$$(c : c') \quad = \quad (x : x') \prod_{i=1}^{t} (x : a_i)^{\beta_i} \, (a_i : x')^{\alpha_i} \prod_{1 \leq i,j \leq t} (a_i : a_j)^{\alpha_i\beta_j} .$$

Again, by Lemma 3.4 (f), all $(x : x'), (x : a_i), (a_i : x')$ belong to $\mathcal{C}$ and we can conclude that $\mathcal{D} \subseteq \langle \mathcal{C}, (a_i : a_j) : 1 \leq i < j \leq t \rangle$. The reverse inclusion is obvious, hence $\mathcal{D} = \langle \mathcal{C} \cup \{(a_i : a_j) : 1 \leq i < j \leq t\} \rangle$.

Now, having in mind that $|S(\mathcal{C})| \leq |T(\mathcal{G})| \leq 2^{k_1+k_2+k_3} = 2^l$ we have that $\mathcal{D}$ is of type $(\sigma + h, \delta, \rho)$ and, from Lemma 3.5, $r(C) = \sigma + \delta + \rho + h$ with $h \leq \binom{t}{2} \leq \binom{\delta+\rho}{2}$ and $h \leq l - \sigma$. This proves item 2.

□

Lemma 3.7. *Let C be a $\mathbb{Z}_2\mathbb{Z}_4$-linear code. If $|C| \leq 8$, then C is also a $\mathbb{Z}_2$-linear code.*

Proof. Assume that $\mathcal{C}$ is of type (σ, δ, ρ). As $\mathcal{C}$ is commutative $\rho = 0$. If C is not linear then $8 \geq 2^{\sigma+\delta} = |C| > 2|K(C)| = 2^{k(C)+1}$. Hence, by Lemma 3.5, we have $\delta \leq \sigma \leq k(C) \leq 1$ and so $\sigma + \delta \leq 2$. Thus, $k(C) + 1 < \delta + \sigma \leq 2$ and so $k(C) = \delta = \sigma = 0$, a contradiction. Hence, C is $\mathbb{Z}_2$-linear. □

We now present a "pure" Q_8-code.

Proposition 3.8. *Let $\mathcal{C}$ be the quaternionic code $\mathcal{C} = \langle(\mathbf{a}, \mathbf{a}), (\mathbf{ab}, \mathbf{b})\rangle \leq Q_8^2$. Let $C = \Phi(\mathcal{C})$ be the corresponding Q_8-code. Then, C is not a $\mathbb{Z}_2\mathbb{Z}_4$-linear code.*

Proof. $\mathcal{C}$ has eight elements, namely $\mathcal{C} = \{(\mathbf{1}, \mathbf{1}), (\mathbf{a}, \mathbf{a}),$
$(\mathbf{a}^2, \mathbf{a}^2), (\mathbf{a}^3, \mathbf{a}^3), (\mathbf{ab}, \mathbf{b}), (\mathbf{a}^2\mathbf{b}, \mathbf{ab}), (\mathbf{a}^3\mathbf{b}, \mathbf{a}^2\mathbf{b}), (\mathbf{b}, \mathbf{a}^3\mathbf{b})\}$.

The swapper $((\mathbf{a}, \mathbf{a}) : (\mathbf{ab}, \mathbf{b})) = (\mathbf{a}^2, \mathbf{1}) \notin \mathcal{C}$ and hence, by Lemma 3.6, C is not linear. Finally, by Lemma 3.7, C is not $\mathbb{Z}_2\mathbb{Z}_4$-linear. □

Remark 3.9. The type of the group $\mathcal{C}$ of Proposition 3.8 is $(\sigma, \delta, \rho) = (1, 0, 2)$. Let $C = \Phi(\mathcal{C})$ and let $k = k(C)$ and $r = r(C)$. By Lemma 2.3 we have $r \geq k+3$; by Lemma 3.5 we have $k \geq \sigma = 1$; by Lemma 3.6 we have $r \leq \sigma+\delta+\rho+\binom{\delta+\rho}{2} = 4$ and by statement 3 of Lemma 3.2 we have $\sigma \geq \delta + \min\{1, \rho\} = 1$. In this example the previous bounds on σ, the rank and the dimension of the kernel are absolutely tight, we have $\sigma = k = 1$ and $r = 4$.

4 Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes

In this section we focus on Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes. But, first of all, we shall begin seeing that the usual companions of the Hadamard codes, that is the (extended) 1-perfect codes which are $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes, do not exist for binary length $n > 8$, except for those which are $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. However we will present a number of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes. The main result of this section is Theorem 4.11 which provides a classification of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes in terms of its structure. For Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes we also refine the upper bound for the rank given in Lemma 4.10 for arbitrary $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes. As an application we classify the Hadamard codes of length 16 which are $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes. More precisely, for any $n = 2^m$, there is an unique (up to isomorphism) extended Hamming code of length n and, since the dual of an extended Hamming code is a Hadamard code [10], for the same length n it always exists a unique Hadamard binary linear code. But, there are much more non isomorphic Hadamard codes. As an example, there are exactly five non isomorphic Hadamard codes of length 16 [1]. One of them is the linear Hadamard code. The other four have the following parameters for the rank r and the dimension of the kernel k: $(r, k) \in \{(6, 3), (7, 2), (8, 2), (8, 1)\}$ [11]. The Hadamard code with parameters $(r, k) = (6, 3)$ is a $\mathbb{Z}_2\mathbb{Z}_4$-linear code, and the other three non-linear Hadamard codes are not $\mathbb{Z}_2\mathbb{Z}_4$-linear [12]. In Proposition 4.5, we show

that the one with parameters $(r,k)=(7,2)$ is a Q_8-code. Moreover, we will see that the remaining two codes, the ones with parameters $(8,2)$ and $(8,1)$, are not $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes (see Example 4.14). This is a consequence of an analysis of the structure, type and parameters of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes.

It is well known that there exist $\mathbb{Z}_2\mathbb{Z}_4$-linear extended 1-perfect codes and $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes [4, 9], but now we are interested in extended 1-perfect $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes where the quaternion group is involved.

Lemma 4.1. *Let $\mathcal{C}$ be a subgroup of $\mathbb{Z}_2^{k_1}\times\mathbb{Z}_4^{k_2}\times Q_8^{k_3}$ with $k_3\neq 0$ and $C=\Phi(\mathcal{C})$. Then, the dual code $C^{\perp}$ has a codeword of weight 4.*

Proof. We can assume that the last coordinate of any vector in $\mathcal{C}$ correspond to an element in Q_8. Since the binary image of all the elements in Q_8 is even, we conclude that $(0,\ldots,0,1,1,1,1)\in C^{\perp}$. □

The next lemma was stated for Steiner triple systems [6] and, later, for Steiner quadruple systems [15]. We give a version for perfect and extended perfect codes which is useful for Theorem 4.3.

Lemma 4.2. *[6, 15] The dual of a 1-perfect code C of length 2^m-1 (respectively, an extended 1-perfect code C^* of length 2^m) is a subcode of the dual of a Hamming code of length 2^m-1 (respectively, linear Hadamard code of length 2^m).*

Theorem 4.3. *Let $C=\Phi(\mathcal{C})$, where $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^{k_1}\times\mathbb{Z}_4^{k_2}\times Q_8^{k_3}$, with $k_3>0$ and $n=k_1+2k_2+4k_3$.*

1. *If C is a 1-perfect code then $n=7$ and $(k_1,k_2,k_3)=(3,0,1)$.*
2. *If C is an extended 1-perfect code then either $n=8$ and $(k_1,k_2,k_3)\in\{(4,0,1),(0,2,1),(0,0,2)\}$, or $n=4$ and $(k_1,k_2,k_3)=(0,0,1)$.*

Proof. Although item 1 about 1-perfect codes was already proven in [4] we give a new proof which includes both items.

By Lemma 4.2 all the codewords in $C^{\perp}$ (respectively, $C^{*\perp}$) should have weight 2^{m-1} (respectively, should have weight 2^m or 2^{m-1}) and by Lemma 4.1 this is only possible when $2^{m-1}=4$ (respectively, when $2^m=4$ or $2^{m-1}=4$). Hence, the non existence of 1-perfect $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes (respectively, extended 1-perfect $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes) is proved for codes of length $n>7$ (respectively, $n>8$).

To finish the proof, let us go to the specific codes of length 7 (respectively, length 8 for the extended case). The extended Hamming code of length 8 can not have the parameters $(k_1,k_2,k_3)=(2,1,1)$, otherwise, after puncturing, there would exist a 1-perfect code with parameters $(k_1,k_2,k_3)=(1,1,1)$ which does not exist. Indeed, vector with quaternionic coordinate $a_j\in\{\mathbf{a}^3,\mathbf{ab},\mathbf{a}^2\mathbf{b}\}\subset Q_8$ (1) and all the other coordinates equal to zero should be at distance one apart from the code, so we obtain three codewords v_1,v_2,v_3, depending on the value of a_j . The distance from v_iv_i to other v_jv_j $(i,j\in\{1,2,3\})$ is zero or two, a contradiction. Therefore, the extended Hamming code of length 8 can be constructed as a $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code $C=\Phi(\mathcal{C})$ in the following three ways: taking $\mathcal{C}$ as the subgroup of $\mathbb{Z}_2^4\times Q_8$ generated by $(1,1,0,0,\mathbf{a}^3)$, $(1,0,1,0,\mathbf{a}^2\mathbf{b})$ and $(1,1,1,1,\mathbf{a}^2)$; taking $\mathcal{C}$ as the subgroup of $\mathbb{Z}_4^2\times Q_8$ generated by $(2,0,\mathbf{a}^3),(1,3,\mathbf{a}^2\mathbf{b})$ and $(2,2,\mathbf{a}^2)$; and taking $\mathcal{C}$ as the subgroup of Q_8^2 generated by $(\mathbf{a},\mathbf{a}),(\mathbf{b},\mathbf{b})$ and $(\mathbf{1},\mathbf{a}^2)$. Puncturing the first one in the first coordinate we obtain the Hamming

code of length 7 which is the binary code associated to the subgroup of $\mathbb{Z}_2^3 \times Q_8$ generated by $(1,0,0,\mathbf{a}^3)$, $(0,1,0,\mathbf{a}^2\mathbf{b})$ and $(1,1,1,\mathbf{a}^2)$. The extended Hamming code of length 4 can be constructed as the binary code of the subgroup of Q_8 generated by $\mathbf{a}^2$. □

Remark 4.4. From Lemma 4.1 a binary code with no codewords of weight 4 in its dual can not be $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes with $k_3 > 0$. There are good binary codes without the dual weight 4. For instance, the extended Preparata-like code and its additive dual, the Kerdock-like code, are $\mathbb{Z}_4$-linear codes but they are not $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes with $k_3 \neq 0$. Indeed, the minimum distance of both codes is greater than 4. Also note that it was already proven in [5] that both codes are not $\mathbb{Z}_2\mathbb{Z}_4$-linear codes with $k_1 \neq 0$.

In the following, we use the notation $N \rtimes H$ for a semidirect product, i.e., a group such that as a set $N \rtimes H = N \times H$ with multiplication given by

$$(n_1, h_1)(n_2, h_2) = (n_1\alpha_{h_1}(n_2), h_1h_2)$$

where $(n_1, n_2 \in N, h_1, h_2 \in H)$ and $h \to \alpha_h$ is a group homomorphism $\alpha : H \to \mathrm{Aut}(N)$. The direct product $N \times H$ is the semidirect product with $\alpha_h = I$ for every $h \in H$.

Proposition 4.5. *Consider the quaternionic code*

$$\mathcal{C} = \langle (\mathbf{a},\mathbf{a},\mathbf{a},\mathbf{a}), (\mathbf{b},\mathbf{ab},\mathbf{b},\mathbf{ab}), (\mathbf{a}^2,\mathbf{1},\mathbf{a},\mathbf{a}^3) \rangle \leq Q_8^4 \tag{7}$$

and let $C = \Phi(\mathcal{C})$. Then $\mathcal{C}$ is of type $(2,0,3)$ and C is a Hadamard code of length 16, rank 7 and dimension of the kernel 2.

Proof. Let $a = (\mathbf{a},\mathbf{a},\mathbf{a},\mathbf{a}), b = (\mathbf{b},\mathbf{ab},\mathbf{b},\mathbf{ab})$ and $c = (\mathbf{a}^2,\mathbf{1},\mathbf{a},\mathbf{a}^3)$. Then a, b and c have order 4, $a^2b^2 = \mathbf{e}$, $a^b = a^{-1}$, $c^a = c$ and $c^b = c^{-1}$. Moreover $\langle c \rangle \cap \langle a, b \rangle = \{\mathbf{e}\}$. Therefore, $\mathcal{C}$ is a semidirect product $\langle c \rangle \rtimes \langle a, b \rangle \cong \mathbb{Z}_4 \rtimes Q_8$. Hence, $T(\mathcal{C}) = Z(\mathcal{C}) = \langle a^2, c^2 \rangle \cong \mathbb{Z}_2^2$. Thus, $\mathcal{C}$ has type $(2,0,3)$ and $G/T(\mathcal{C}) = \langle \overline{a} \rangle \times \langle \overline{b} \rangle \times \langle \overline{c} \rangle$. Furthermore, a straightforward calculation shows that $\Phi^{-1}(K(C)) = T(\mathcal{C})$ and every element of C has weight 0, 8 or 16. Therefore, C is a Hadamard code. The dimension of its kernel is 2. By Lemma 3.6 the linear span of C is $\Phi(\langle \mathcal{C}, (a:b) = (\mathbf{a}^2,\mathbf{1},\mathbf{a}^2,\mathbf{1}), (a:c) = \mathbf{e}, (b:c) = (\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{a}^2) \rangle)$. Thus, the rank of C is 7. □

Lemma 4.6. *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 $a, b, c \in \mathcal{C} \setminus T(\mathcal{C})$. Then*

1. *either $[a, b] \in \langle a^2 \rangle$ or $a^2 = \mathbf{u}$;*
2. *if $a^2 = b^2 = c^2 \neq \mathbf{u}$ then $|\langle a, b, c, T(\mathcal{C}) \rangle / T(\mathcal{C})| \leq 4$*
3. *if $a^2 = b^2 = [a, b] \neq c^2$ then $|\langle (a:c), (b:c), T(\mathcal{C}) \rangle / T(\mathcal{C})| \leq 2$.*

Proof. We know that the binary all ones vector belongs to any Hadamard code and hence $\mathbf{u} \in \mathcal{C}$.

1. If $y \in \mathcal{C} \setminus \{1, \mathbf{u}\}$ then $\mathrm{wt}(\Phi(y)) = \frac{n}{2}$. Thus, by item 2 of Lemma 3.2, if $a^2 \neq \mathbf{u}$ and $[a, b] \neq \mathbf{e}$ then $[a, b] = a^2$.

2. Assume $|\langle a,b,c,T(\mathcal{C})\rangle/T(\mathcal{C})| > 4$ and $a^2 = b^2 = c^2 = t \neq \mathbf{u}$. Then $\{ab, ac, bc, abc\} \cap T(\mathcal{C}) = \emptyset$. Therefore, by items 1 and 2 of Lemma 3.2, $[a,b] = [a,c] = [b,c] = t$. Hence $(abc)^2 = [a,b][a,c][b,c]a^2b^2c^2 = t^6 = \mathbf{e}$. Thus $abc \in T(\mathcal{C})$, a contradiction.

3. Suppose $|\langle (a:c), (b:c), T(\mathcal{C})\rangle/T(\mathcal{C})| > 2$ and $a^2 = b^2 = [a,b] \neq c^2$. Then $\langle (a:c), (b:c)\rangle$ is isomorphic to $\mathbb{Z}_2^2$ and intersects $T(\mathcal{C})$ trivially. Write $a = (a_1, \ldots, a_l), b = (b_1, \ldots, b_l)$ and $c = (c_1, \ldots, c_l)$.

Suppose $[a,c] = [b,c] = \mathbf{e}$. Then $a^2 \neq \mathbf{u}$ for otherwise $\langle a_i, b_i\rangle = Q_8$ for every i and hence c has order 2, contradicting the fact that $(a:c) \neq \mathbf{e}$. Therefore, after reordering the coordinates we may assume that $a^2 = (\mathbf{u}_{l_1} | \mathbf{e}_{l_2})$. Hence, if $i \leq l_1$ then $\langle a_i, b_i\rangle = Q_8$ and c_i has order at most two and when $i > l_1$, a_i and b_i have order at most two and c_i has order four. Then $(a:c) = \mathbf{e}$, contradicting the assumption.

Thus either $[a,c] \neq \mathbf{e}$ or $[b,c] \neq \mathbf{e}$. By symmetry we may assume that $[a,c] \neq \mathbf{e}$. If $[b,c] = \mathbf{e}$ then $[ab,c] \neq \mathbf{e}$, $(ab)^2 = a^2$ and $(ab:c) = (a:c)(b:c)$, so that $\langle (a:c), (b:c)\rangle = \langle (a:c), (ab,c:)\rangle$. Therefore, we can replace b by ab and so we may assume that $[b,c] \neq \mathbf{e}$. Then, by item 1, either $a^2 = \mathbf{u}$ and $[a,c] = [b,c] = c^2$ or $c^2 = \mathbf{u}$ and $[a,c] = [b,c] = a^2$.

Suppose that $a^2 = \mathbf{u}$. Then $\langle a_i, b_i\rangle \cong Q_8$ for every i, so that $\mathcal{G} = Q_8^l$ and $\mathrm{wt}(c^2) = 2l = \frac{n}{2}$. Then l is even and after reordering the coordinates we may assume that $c^2 = (\mathbf{u}_{\frac{l}{2}} | \mathbf{e}_{\frac{l}{2}})$. Then each a_i and b_i have order 4 and c_i has order 4 if and only if $i \leq \frac{l}{2}$. Let $A_1 = \{\mathbf{a}, \mathbf{a}^3\}$, $A_2 = \{\mathbf{b}, \mathbf{a}^2\mathbf{b}\}$ and $A_3 = \{\mathbf{ab}, \mathbf{a}^3\mathbf{b}\}$. If $r \in A_i$ and $s \in A_j$ then $[r,s] = \mathbf{e}$ if and only if $i = j$; and $(r:s) = \mathbf{e}$ if and only if $i - j \equiv 1 \mod 3$ (see Table 1). Each a_i, b_i and c_i, with $i \leq \frac{l}{2}$, belongs to some A_i and $[a_i, b_i] = [a_i, c_i] = [b_i, c_i] = \mathbf{a}^2$. Therefore a_i, b_i and c_i belong to different A_i's. This implies that for every $i \leq \frac{l}{2}$, $\{(a_i:c_i), (b_i:c_i)\} = \{1, \mathbf{a}^2\}$. On the other hand, $[a_i, c_i] = [b_i, c_i] = \mathbf{1}$ for every $i > \frac{l}{2}$. Therefore $(a:c)(b:c) = (\mathbf{u}_{\frac{l}{2}} | \mathbf{e}_{\frac{l}{2}}) = c^2 \in T(\mathcal{C})$ which yields a contradiction. A slight modification of this argument, with the roles of a and c interchanged, yields also a contradiction in the case $c^2 = \mathbf{u}$. This finishes the proof of item 3. □

The following corollary is a straightforward consequence of Lemma 3.2 and Lemma 4.6.

Corollary 4.7. *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 $x_1, \ldots, x_\sigma$; $y_1, \ldots, y_\delta$; $z_1, \ldots, z_\rho$ be a set of generators of $\mathcal{C}$.*

1. *For every $t \in T(\mathcal{C})$ with $t \neq \mathbf{u}$, the cardinality of $\{i = 1, \ldots, \rho : z_i^2 = t\}$ is at most 2.*
2. *If $[z_i, z_j] \neq \mathbf{e}$ then either $z_i^2 = \mathbf{u}$ or $[z_i, z_j] = z_i^2$.*
3. *If $[z_i, z_j] = e$ then $z_i^2 \neq z_j^2$.*

Corollary 4.7 implies that if $\mathcal{C}$ is a subgroup of $\mathcal{G}$ such that $\Phi(\mathcal{C})$ is a Hadamard code and $t \neq \mathbf{u}$ then a generating set of $\mathcal{C}$ has at most two z_i's with square equal to t. Moreover if $z_i^2 = z_j^2 \neq \mathbf{u}$ then $[z_i, z_j] = z_i^2$, by item 1 of Lemma 3.2 and item 1 of Lemma 4.6. For our purposes it is convenient to use a generating set for which this property also holds for z_i's with square $\mathbf{u}$.

Definition 4.8. *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 $x_1, \ldots, x_\sigma; y_1, \ldots, y_\delta; z_1, \ldots, z_\rho$ be a set of generators of $\mathcal{C}$. We say that this generating set is* normalized *if $z_i^2 = \mathbf{u}$ for at most two $i = 1, \ldots, \rho$ and if $z_i^2 = z_j^2 = \mathbf{u}$ with $i \neq j$ then $[z_i, z_j] = \mathbf{u}$.*

Lemma 4.9. *Every Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code C has a normalized set of generators.*

Proof. Let $x_1, \ldots, x_\sigma; y_1 \ldots, y_\tau; z_1, \ldots, z_\rho$ be a generating set of $\mathcal{C}$. We may assume without loss of generality that $z_i^2 = \mathbf{u}$ if and only if $i \leq k$ and either $[z_1, z_i] \neq \mathbf{u}$ for every $2 \leq i \leq k$ or $[z_1, z_2] = \mathbf{u}$. If $k \leq 1$ there is nothing to prove. Otherwise, for every $i = 1, \ldots, \rho$ we define

$$z_i' = \begin{cases} z_1 z_i, & \text{if } 2 \leq i \leq k \text{ and } [z_1, z_i] \neq \mathbf{u}; \\ z_2 z_i, & \text{if } 3 \leq i \leq k, [z_1, z_i] = \mathbf{u} \neq [z_2, z_i]; \\ z_1 z_2 z_i, & \text{if } 3 \leq i \leq k, [z_1, z_i] = \mathbf{u} = [z_2, z_i]; \\ z_i, & \text{otherwise.} \end{cases}$$

Then $x_1, \ldots, x_\sigma; y_1 \ldots, y_\tau; z_1', \ldots, z_\rho'$ is a generating set of $\mathcal{C}$ and we claim that it is normalized. Indeed, if $i > k$ then $z_i'^2 = z_i^2 \neq \mathbf{u}$. Assume $3 \leq i \leq k$. If $[z_1, z_i] \neq \mathbf{u}$ then $z_i'^2 = (z_1 z_i)^2 = [z_1, z_i] z_1^2 z_2^2 = [z_1, z_i] \neq \mathbf{u}$. Assume that $[z_1, z_i] = \mathbf{u}$. Then, by construction, $[z_1, z_2] = \mathbf{u}$. Therefore, if $[z_2, z_i] \neq \mathbf{u}$ then $z_i'^2 = (z_2 z_i)^2 = [z_2, z_i] z_2^2 z_i^2 = [z_2, z_i] \neq \mathbf{u}$, and if $[z_2, z_i] = \mathbf{u}$ then $z_i'^2 = (z_1 z_2 z_i)^2 = [z_1, z_2][z_1, z_i][z_2, z_i] z_1^2 z_2^2 z_i^2 = \mathbf{u}^6 = 1 \neq \mathbf{u}$. Finally, assume that $i = 2 \leq k$. If $[z_1, z_2] = \mathbf{u}$ then $z_2' = z_2$ and so $[z_1, z_2'] = \mathbf{u}$ and otherwise $z_2'^2 = (z_1 z_2)^2 = [z_1, z_2] \neq \mathbf{u}$. □

In the remainder of the section $x_1, \ldots, x_\sigma$; $y_1, \ldots, y_\delta$; $z_1, \ldots, z_\rho$ is a normalized generating set of $\mathcal{C}$. Moreover, let ϵ denote the number of pairs of different z_i's with the same squares, We reorder the z_i's in such a way that two z_i's with the same square are consecutive and placed at the beginning of the list, i.e., $z_1^2 = z_2^2, \ldots, z_{2\epsilon-1}^2 = z_{2\epsilon}^2$ and $z_2^2, z_4^2, \ldots, z_{2\epsilon}^2, z_{2\epsilon+1}^2, \ldots, z_\rho^2$ are pairwise different. Note that for each $i = 1, \ldots, \rho$ there is $j = 1, \ldots, \rho$ such that $[z_i, z_j] \neq \mathbf{e}$. In that case, either $z_i^2 = \mathbf{u}$ or $z_j^2 = \mathbf{u}$ or $z_i^2 = z_j^2$. In the last case $\{i, j\} = \{2t - 1, 2t\}$ for some $t \leq \epsilon$.

Lemma 4.10. *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 and let $x_1, \ldots, x_\sigma; y_1, \ldots, y_\delta; z_1, \ldots, z_\rho$ be a normalized set of generators of $\mathcal{C}$. Let ϵ and the z_i's be as in the previous paragraph. Then the following assertions hold:*

1. *$\epsilon \leq 2$.*
2. *If $\epsilon = 2$ then $\delta = 0$ and $\rho = 4$. In the case when z_1^2, z_3^2 and $\mathbf{u}$ are pairwise different we have $[z_i, z_j] = \mathbf{e}$ and $z_i^2 z_j^2 = \mathbf{u}$ for $i \in \{1, 2\}$, $j \in \{3, 4\}$.*
3. *If $z_i^2 = \mathbf{u}$ with $i \leq 2\epsilon$ then $\delta = 0$.*
4. *Let $V = \{y_1, \ldots, y_\delta, z_1, z_3, \ldots, z_{2\epsilon-1}, z_{2\epsilon+1}, z_{2\epsilon+2}, \ldots, z_\rho\}$, $W = \{w^2 : w \in V\}$ and $U = \{u \in V : u^2 \neq \mathbf{u}\}$. Then $|\langle W \rangle| \geq 2^{\delta+\rho-\epsilon-1}$, and hence $\sigma \geq \delta + \rho - \epsilon - 1$. If moreover $\mathbf{u} \notin \langle U \rangle$ then $|\langle W \rangle| = 2^{\delta+\rho-\epsilon}$, and hence $\sigma \geq \delta + \rho - \epsilon$.*

5. (Upper bound for $r(C)$) *If $\mathcal{D} = \langle \mathcal{C} \cup S(\mathcal{C}) \rangle$ (as in Lemma 3.6) then $\mathcal{D}$ is of type $(\sigma + h, \delta, \rho)$ and $r(C) \leq \sigma + \delta + \rho + h$ with*

$$h \leq \begin{cases} \epsilon + \binom{\delta+\rho-\epsilon}{2}, & \text{if } \epsilon \leq 1; \\ 3, & \text{if } \epsilon = 2 \end{cases}$$

Proof. Item 3. Assume $z_i^2 = \mathbf{u}$ for some $i \leq 2\epsilon$. Then we may assume without loss of generality that $z_1^2 = z_2^2 = [z_1, z_2] = \mathbf{u}$. (Recall that our generating set is normalized.) Then the projection of $\langle z_1, z_2 \rangle$ onto each coordinate is Q_8, so that $k_1 = k_2 = 0$, and no element of $\mathcal{C}$ of order 4 is central, i.e., $\delta = 0$.

For every $i = 1, \ldots, \rho$ let $X_i = \{j : \text{the } j\text{th coordinate of } z_i \text{ has order } 4\}$.

We claim that if z_i^2, z_j^2 and $\mathbf{u}$ are pairwise different for some $i, j \leq 2\epsilon$ then $k_1 = k_2 = \delta = 0$, X_i and X_j form a partition of $\{1, \ldots, l\}$, $z_i^2 z_j^2 = \mathbf{u}$ and $\{z_1^2, \ldots, z_\rho^2\} \subseteq \{z_i^2, z_j^2, \mathbf{u}\}$. For simplicity we also assume that $i = 1$ and $j = 3$. We know that $z_1^2 = z_2^2$ and $z_3^2 = z_4^2$, and, by Lemma 3.2, $[z_1, z_2] \neq \mathbf{e} \neq [z_3, z_4]$. Hence, by Corollary 4.7, $[z_1, z_2] = z_1^2 = z_2^2$ and $[z_3, z_4] = z_3^2 = z_4^2$, and the images of these elements by Φ have weight $\frac{n}{2}$. This implies that $X_1 = X_2$, the projections of z_1 and z_2 on the coordinates of X_1 generates Q_8 and $|X_1| = \frac{n}{8}$. Similarly $X_3 = X_4$, the projections of z_3 and z_4 on X_3 generate Q_8 and $|X_3| = |X_4| = \frac{n}{8}$. Moreover, by Corollary 4.7, $[z_i, z_j] = \mathbf{e}$ for $i = 1, 2$ and $j = 3, 4$. Therefore the projection of z_3 and z_4 on the coordinates of X_1 have order 2. This implies that X_1 and X_3 are disjoint. Therefore $4(|X_1| + |X_3|) = n$ and hence $k_1 = k_2 = 0$. Furthermore, no element of $\mathcal{C}$ of order 4 can commute with each z_i with $i = 1, 2, 3, 4$. This implies that $\delta = 0$ and, by item 1 of Lemma 4.6, $z_k^2 = \mathbf{u}$ for every $k \neq 1, 2, 3, 4$. This finishes the proof of the claim.

Items 1 and 2. Assume first that z_i^2, z_j^2 and $\mathbf{u}$ are pairwise different for some $i, j \leq 2\epsilon$. Observe that this holds if $\epsilon > 2$. By the claim, we may assume without loss of generality that X_1 is formed by the first $\frac{n}{8}$ coordinates and X_3 is formed by the last $\frac{n}{8}$ coordinates. Moreover, if $\rho > 5$, then by the claim $z_5^2 = \mathbf{u} = z_1^2 z_3^2$. Then there are $z_1' \in \langle z_1, z_2 \rangle$ and $z_3' \in \langle z_3, z_4 \rangle$ such that z_1' and z_5 coincide in the first coordinate and z_3' and z_5 coincide in the last coordinate. As all the coordinates of z_5 have order 4, and both the last $\frac{l}{2}$ coordinates of z_1^2 and the first $\frac{l}{2}$ coordinates of z_3^2 are $\mathbf{e}$, we deduce that the first $\frac{l}{2}$ coordinates of z_1' and the last coordinates $\frac{l}{2}$ of z_3' have order 4. Moreover $[z_1', z_5] \neq {z_1'}^2$ and $[z_3', z_5] \neq {z_3'}^2$. So, $z_1'^2 z_3'^2 = z_5^2$ and $[z_1', z_5] = [z_3', z_5] = \mathbf{e}$. Then $(z_1' z_3' z_5)^2 = z_1'^2 z_3'^2 z_5^2 = \mathbf{e}$, contradicting the fact that $z_1' z_3' z_5 \notin T(\mathcal{C})$. This finishes the proof of 1, and proves 2 in case $z_1^2 \neq \mathbf{u} \neq z_3^2$.

Suppose that $\epsilon = 2$ and $z_1^2 = \mathbf{u}$. As above, we may assume that $\langle z_3, z_4 \rangle$ projects to Q_8 in the first $\frac{n}{8}$ coordinates and projects to an element of order at most 2 in the remaining coordinates. Suppose $\rho > 4$. By Corollary 4.7, $[z_3, z_5] = [z_4, z_5] = \mathbf{e}$, so that the projection of z_5 in the first $\frac{n}{8}$ coordinates has order at most 2 and the projection on the remaining coordinates has order 4. Therefore $(z_3 z_5)^2 = (z_4 z_5)^2 = z_3^2 z_5^2 = z_4^2 z_5^2 = \mathbf{u}$. Moreover, by the same argument as in the previous paragraph, we could take $z_1' \in \langle z_1, z_2 \rangle$ and $z_3' \in \langle z_3, z_4 \rangle$ such that $[z_1', z_5] = [z_3', z_5] = [z_1', z_3'] = \mathbf{e}$. This implies that $(z_1' z_3' z_5)^2 = z_1'^2 z_3'^2 z_5^2 = \mathbf{e}$, contradicting the fact that $z_1 z_3 z_5 \notin T(\mathcal{C})$. This finishes the proof of 2.

Item 4. Let $t = |U|$ and set $U = \{u_1, \ldots, u_t\}$. Observe that $t = \delta + \rho - \epsilon - 1$ if $\mathbf{u} \in W$ and otherwise $t = \delta + \rho - \epsilon$. From item 2 of Corollary 4.7, the elements of U commute. Moreover the map $\mathbb{Z}_2^t \to \mathcal{C}/T(\mathcal{C})$ given

by $(\alpha_1,\dots,\alpha_t)\mapsto u_1^{\alpha_1}\dots u_t^{\alpha_t}T(\mathcal{C})$ is injective. Then, by item 1 of Lemma 3.2, the rule $(\alpha_1,\dots,\alpha_t)\mapsto u_1^{2\alpha_1}\dots u_t^{2\alpha_t}$ defines a bijection $\mathbb{Z}_2^t\to T(U)$. Then $|\langle W\rangle|\geq|T(\langle U\rangle)|=2^t\geq 2^{\delta+\rho-\epsilon-1}$. If $\mathbf{u}\notin\langle U\rangle$ then either $\mathbf{u}\notin W$ and hence $t=\delta+\rho-\epsilon$, $W=T(U)$ and $|W|=|T(U)|=2^{\delta+\rho-\epsilon}$ or $\langle W\rangle=\langle T(U),\mathbf{u}\rangle$ and then $|W|=2|T(U)|=2^{\delta+\rho-\epsilon}$. In both cases $|W|=2^{\delta+\rho-\epsilon}$.

Item 5. Using the argumentation in the proof of Lemma 3.6 the span of C is $\Phi(\mathcal{D})$ where $\mathcal{D}$ is the group generated $\mathcal{C}$ and the swappers of $A=\{y_1,\dots,y_\delta,z_1,\dots,z_\rho\}$, where we only take one of the two swappers $(a:b)$ or $(b:a)$ for $a\neq b\in A$. If $i\leq\epsilon$ then $|\langle(z_{2i-1}:a),(z_{2i}:a),T(\mathcal{C})\rangle/T(\mathcal{C})|\leq 2$ (Lemma 4.6), for every $a\in A\setminus\{z_{2i-1},z_{2i}\}$. Therefore, in order to generate $\mathcal{D}$ modulo $\mathcal{C}$ it is enough to take the swappers of the form $(z_j:z_k)$ with $2\epsilon<j<k\leq\rho$, the swapper $(z_{2i-1}:z_{2i})$ for each $i\leq\epsilon$ and one out of the two swappers $(z_{2i-1}:z_j)$ or $(z_{2i}:z_j)$ for each $i\leq\epsilon$ and $2i<j\leq\rho$. This gives a total of $s=\binom{\delta+\rho-2\epsilon}{2}+\epsilon+\sum_{i=1}^{\epsilon}(\delta+\rho-2i)$ swappers. Thus $r(C)=\sigma+\delta+\rho+h$ with $h\leq s$. If $\epsilon=0$ then $s=\binom{\delta+\rho}{2}$. If $\epsilon=1$ then $\alpha=1+\binom{\delta+\rho-2}{2}+(\delta+\rho-2)=1+\binom{\delta+\rho-1}{2}$. Finally, assume that $\epsilon=2$. Then $\delta=0$, $\rho=4$ and $h\leq s=4$. We claim that in this case we may assume that $z_1^2=\mathbf{u}$. Otherwise, by item 2 in this Lemma, $[z_i,z_j]=\mathbf{e}$ and $(z_iz_j)^2=\mathbf{u}$ for every $i=1,2$ and $j=3,4$, and therefore $(z_1z_3)^2=(z_2z_4)^2=\mathbf{u}$ and $[z_1z_3,z_2z_4]=[z_1,z_2][z_3,z_4]=z_1^2z_3^2=\mathbf{u}$. Thus, replacing z_1 and z_2 by z_1z_3 and z_2z_4, respectively, we obtain the desired claim. To finish the proof it remains to prove that $h\leq 3$. In this case $\mathcal{D}=\langle\mathcal{C},(z_1:z_2),(z_3:z_4),s_1,s_2\rangle$ where $\{s_1,s_2\}=\{(z_1:z_3),(z_2:z_4)\}$ or $\{s_1,s_2\}=\{(z_1:z_4),(z_2:z_3)\}$. After reordering z_3 and z_4, if necessary, one may assume that $\mathcal{D}=\langle\mathcal{C},(z_1:z_2),(z_3:z_4),(z_1:z_3),(z_2:z_4)\rangle$. By means of contradiction assume that $h=4$. This means that

$$\mathcal{A}=\langle(z_1:z_2),(z_3:z_4),(z_1:z_3),(z_2:z_4),T(\mathcal{C})\rangle/T(\mathcal{C}) \tag{8}$$

is of order 16. By $[z_1,z_2]=\mathbf{u}$ we have $k_1=k_2=0$. After a suitable reordering we may assume that $z_3^2=(\mathbf{u}_{\frac{l}{2}},\mathbf{e}_{\frac{l}{2}})$. Write $z_1=(a_1,\dots,a_l)$, $z_2=(b_1,\dots,b_l)$, $z_3=(c_1,\dots,c_l)$ and $z_4=(d_1,\dots,d_l)$. As $[a_1,b_1]=\mathbf{a}^2$ and c_1 has order 4, c_1 does not commute with either a_1 or b_1. If $[a_1,c_1]=\mathbf{1}$ then replacing z_1 by z_1z_2 we may assume that $[a_1,c_1]=[b_1,c_1]=\mathbf{a}^2$.

We argue similarly if $[b_1,c_1)]=\mathbf{e}$ to deduce that we may always assume that $[a_1,c_1)]=[b_1,c_1)]=\mathbf{a}^2$. Then $[z_1,z_3]=[z_2,z_3]=z_3^2$. For every $x\in Q_8$ of order 4 let $l(x)\in\{1,2,3\}$ with $x\in A_{l(x)}$, where $A_1=\{\mathbf{a},\mathbf{a}^3\}$, $A_2=\{\mathbf{b},\mathbf{a}^2\mathbf{b}\}$ and $A_3=\{\mathbf{ab},\mathbf{a}^3\mathbf{b}\}$. Then $\{l(a_i),l(b_i),l(c_i)\}=\{1,2,3\}$ for every $i\leq\frac{l}{2}$. As $[c_1,d_1]\neq\mathbf{1}$, $l(c_1)\neq l(d_1)$. If $l(b_1)=l(d_1)$ then $[b_1,d_1]=\mathbf{1}$ and therefore $[z_2,z_4]=\mathbf{e}$. Then $l(b_i)=l(d_i)$ for every $i\leq\frac{l}{2}$ and hence $s_4=(z_2:z_4)=(\mathbf{u}_{\frac{l}{2}},\mathbf{e}_{\frac{l}{2}})=z_3^2\in\mathcal{C}$, contradicting the assumption. Thus $l(b_1)\neq l(d_1)$ and hence $[z_2,z_4]=z_3^2$. Then $l(b_i)\neq l(d_i)$ for every $i\leq\frac{l}{2}$. So, for these indexes we have $\{l(b_i),l(c_i),l(d_i)\}=\{1,2,3\}$, hence $l(a_i)=l(d_i)$ and $(a_i:c_i)(c_i:d_i)=(a_i:c_i)(d_i:c_i)[c_i,d_i]=(a_id_i:c_i)[c_i,d_i]=[c_i,d_i]$.

We conclude with $(z_1:z_3)(z_3:z_4)=[z_3,z_4]\in T(\mathcal{C})$, a contradiction. □

Next theorem describes the group structure of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes and specify the bounds for the rank and dimension of the kernel in each case.

Theorem 4.11. *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 of length $n=2^m$ with rank $r=r(C)$ and dimension of the*

kernel $k = k(C)$. Then $\mathcal{C}$ has a normalized generating set $x_1, \ldots, x_\sigma$; $y_1, \ldots, y_\delta$; $z_1, \ldots, z_\rho$, where $m = \sigma + \delta + \rho - 1$, satisfying one of the following conditions.

1. *$\rho = 0$. Then $\mathcal{C} \cong \mathbb{Z}_2^{\sigma-\delta} \times \mathbb{Z}_4^\delta$ and C is a $\mathbb{Z}_2\mathbb{Z}_4$-linear code (which could be $\mathbb{Z}_4$-linear code or not), with length $n = 2^m$ and $m = \sigma + \delta - 1$.*
   (a) *If C is $\mathbb{Z}_4$-linear then either $\delta \in \{1, 2\}$ and C is linear, or $\delta \geq 3$, $k = \sigma + 1$; $r = \sigma + \delta + \binom{\delta-1}{2}$.*
   (b) *If C is not $\mathbb{Z}_4$-linear then $\sigma > \delta$ and either $\delta \in \{0, 1\}$ and C is linear, or $\delta \geq 2$, $k = \sigma$ and $r = \sigma + \delta + \binom{\delta}{2}$.*
2. *$\delta = 0$, $z_1^2 = z_2^2 = [z_1, z_2] = \mathbf{u}$, $[z_i, z_j] = z_j^2$ and $[z_j, z_k] = \mathbf{e}$ for every $i \in \{1, 2\}$ and $3 \leq j, k \leq \rho$. Then $\mathcal{C} \cong \mathbb{Z}_2^{\sigma-\rho+1} \times (\mathbb{Z}_4^{\rho-2} \rtimes Q_8)$, $k \geq \sigma \geq \rho - 1$ and $r \leq \sigma + \rho + 1 + \binom{\rho-1}{2}$.*
3. *$\delta = 0$, $z_1^2 = \mathbf{u} \notin \langle z_2^2, \ldots, z_\rho^2 \rangle \cong \mathbb{Z}_2^{\rho-1}$, $[z_1, z_i] = z_i^2$ and $[z_i, z_j] = \mathbf{e}$, for every $i \neq j$ in $\{2, \ldots, \rho\}$. Then $\mathcal{C} \cong \mathbb{Z}_2^{\sigma-\rho} \times (\mathbb{Z}_4^{\rho-1} \rtimes \mathbb{Z}_4)$, $k \geq \sigma \geq \rho$ and $r \leq \sigma + \rho + \binom{\rho}{2}$.*
4. *$\rho = 2$, $\delta \leq 1$ and $z_1^2 = z_2^2 = [z_1, z_2] \neq \mathbf{u}$. Then $\mathcal{C} \cong \mathbb{Z}_2^{\sigma-\delta-1} \times \mathbb{Z}_4^\delta \times Q_8$, $k \geq \sigma \geq \delta + 1$ and $r \leq \sigma + \delta + \rho + 1 \leq \sigma + 4$.*
5. *$\delta = 0$, $\rho = 4$, $z_1^2 = z_2^2 = [z_1, z_2] = \mathbf{u} \neq z_3^2 = z_4^2 = [z_3, z_4]$ and $[z_i, z_j] \in \langle z_j^2 \rangle$ for every $i \in \{1, 2\}$ and $j \in \{3, 4\}$. Then $\mathcal{C} \cong \mathbb{Z}_2^{\sigma-2} \times (Q_8 \rtimes Q_8)$ and $k \geq \sigma \geq 2$; $r \leq \sigma + 7$.*

Proof. If $\mathcal{C}$ is abelian then condition 1 holds and the values for the rank and dimension of the kernel are already known [12]. So, in the remainder of the proof we assume that $\mathcal{C}$ is non-abelian and therefore $\rho \geq 2$.

We fix a normalized generating set $x_1, \ldots, x_\sigma$; $y_1, \ldots, y_\delta$; $z_1, \ldots, z_\rho$ of $\mathcal{C}$ which will be modified throughout the proof to be adapted to one of the cases. Let ϵ be as in Lemma 4.10 and reorder the z_i's such that those with equal square are consecutive and placed at the beginning of the list. Then $z_{2i-1}^2 = z_{2i}^2 = [z_{2i-1}, z_i]$ for every $i = 1, \ldots, \epsilon$ (see the comment after Corollary 4.7). Also, as in Lemma 4.10 we set $V = \{y_1, \ldots, y_\delta, z_1, z_3, \ldots, z_{2\epsilon-1}, z_{2\epsilon+1}, z_{2\epsilon+2}, \ldots, z_\rho\}$ and $U = \{u \in V : u^2 \neq \mathbf{u}\}$.

1. Assume $\epsilon = 2$. Then $\delta = 0$ and $\rho = 4$ (Lemma 4.10). If either z_1^2 or z_3^2 equals $\mathbf{u}$ we can assume that $z_1^2 = \mathbf{u}$. If z_1^2, z_3^2 and $\mathbf{u}$ are pairwise different we can take $z_1' = z_1 z_3$ and $z_2' = z_2 z_4$ which is a new normalized generating set z_1', z_2', z_3, z_4 with ${z_1'}^2 = \mathbf{u}$. By Corollary 4.7, $[z_i, z_j] = \langle z_j^2 \rangle$, for $i = 1, 2$ and $j = 3, 4$. Hence, condition 5 holds and $\mathbf{u} \notin \langle U \rangle$, so $\sigma \geq \delta + \rho - \epsilon = 2$.
2. Assume $\epsilon = 1$ and $z_1^2 = \mathbf{u}$. Then $\delta = 0$ (Lemma 4.10).

   If $\rho = 2$ then condition 2 holds. In this case $\mathbf{u} \notin \langle U \rangle$, so $\sigma \geq \delta + \rho - \epsilon = \rho - 1$.

   Assume $\rho \geq 3$. Then $U = \{z_3, \ldots, z_\rho\}$. By Corollary 4.7, for every $3 \leq i, j \leq \rho$ we have $[z_i, z_j] = \mathbf{e}$ and therefore $\langle [z_1, z_i], [z_2, z_i] \rangle = \langle z_i^2 \rangle$. By changing the generators z_1 and z_2 if necessary, we may assume that $[z_1, z_\rho] = [z_2, z_\rho] = z_\rho^2$. The new generating set is still normalized. We have two options: $\mathbf{u} \notin \langle U \rangle$ or $\mathbf{u} \in \langle U \rangle$. In the first case, $[z_1, z_i] = z_i^2$ for every $i \geq 3$ for otherwise $[z_1, z_i z_\rho] = z_\rho^2 \notin \langle (z_i z_\rho)^2 \rangle$ in contradiction with

Lemma 4.6. Similarly $[z_2, z_i] = z_i^2$. Then condition 2 holds. We claim that in the second case, so when $\mathbf{u} \in \langle U \rangle$, we have $[z_1, z_i] = \mathbf{e}$, $[z_2, z_i] = z_i^2$ for some $i \geq 3$. Otherwise $[z_1, z_i] = [z_2, z_i] = z_i^2$ for every $i = 3, \ldots, \rho$. Then $[z_1 z_2, z_i] = \mathbf{e}$ for every $j \geq 3$. After reordering the z_i's we may assume that $(z_3 \cdots z_k)^2 = \mathbf{u}$. Then $(z_1 z_2 z_3 \cdots z_k)^2 = \mathbf{e}$ contradicting the fact that $z_1 \ldots z_k \notin T(C)$. This proves the claim. So assume that $\mathbf{u} \in \langle U \rangle$ and (after reordering the z_i's) $[z_1, z_3] = \mathbf{e}$ and $[z_2, z_3] = z_3^2$. Then $[z_1, z_3 z_\rho] = z_\rho^2 \notin \langle (z_3 z_\rho)^2 \rangle$ and therefore $(z_3 z_\rho)^2 = \mathbf{u}$. If $4 \leq i < \rho$ then $(z_i z_\rho)^2 \neq (z_3 z_\rho)^2 = \mathbf{u}$ and therefore $[z_1, z_i] = [z_2, z_i] = z_i^2$. Thus $(z_3 z_i)^2 = \mathbf{u} = (z_3 z_\rho)^2$ which is not possible. This proves that $\rho = 4$. Now we can construct a new generating set $\{z_1' = z_1 z_2, z_2' = z_2', z_3' = z_1 z_3, z_4' = z_4\}$ and it is easy to check that $z_1'^2 = z_2'^2 = [z_1', z_2'] = \mathbf{u} \neq z_3'^2 = z_4'^2 = [z_3', z_4']$ and $[z_i', z_j'] = z_3'^2$, for every $i = 1, 2$ and $j = 3, 4$. Thus, $\epsilon = 2$ which has been treated before.

3. Assume $\epsilon = 1$ and $z_1^2 \neq \mathbf{u}$. We can have $\rho \geq 3$ or $\rho = 2$.

   In the first case, so if $\rho \geq 3$ then $[z_i, z_j] = [z_j, z_k] = \mathbf{e}$ for every $i \neq 2$ and every $j, k \geq 3$ such that $z_j^2 = \mathbf{e}$, by Corollary 4.7. As each z_j is not central, $z_j^2 = \mathbf{u}$ for some $j \geq 3$ and we may assume that $z_3^2 = \mathbf{u}$. After reordering coordinates one also may assume that $\langle z_1, z_2 \rangle$ projects to Q_8 in the first $\frac{n}{8}$ coordinates. Then either $[z_1, z_3] \neq \mathbf{e}$ or $[z_2, z_3] \neq \mathbf{e}$. By symmetry we may assume that $[z_1, z_3] \neq \mathbf{e}$. If $[z_2, z_3] = \mathbf{e}$ then replacing z_2 by $z_1 z_2$, we can always assume that $[z_2, z_3] \neq \mathbf{e}$. Then $[z_i, z_3] = z_i^2$ for $i = 1, 2$, by Lemma 4.6. If it were $3 < \rho$ then z_4 projects to an element of order at most 2 in the first $\frac{n}{8}$ coordinates and to an element of order 4 in the remaining coordinates and $[z_3, z_4] = z_4^2$. Then $x_1, \ldots, x_\sigma; y_1, \ldots, y_\delta; z_1, z_2, z_3, z_4' = z_1 z_4$ is a new generating set such that $z_4'^2 = z_1^2 z_4^2 = \mathbf{u} = [z_3, z_4']$, with $\epsilon = 2$, which is out of our initial assumption about $\epsilon = 1$. Hence, we have $\rho = 3$ with $z_3^2 = \mathbf{u}$ and $[z_i, z_3] = z_i^2$ for every $i = 1, 2$. Then $[z_1 z_2 z_3, z_1] = [z_1 z_2 z_3, z_2] = [z_1 z_2 z_3, z_3] = \mathbf{e}$. Therefore $z_1 z_2 z_3 \in Z(\mathcal{C})$, a contradiction.

   In the second case, so when $\rho = 2$, assume $\delta > 1$. We can reorder the coordinates in such a way that $\langle z_1, z_2 \rangle$ projects to Q_8 in the first $\frac{n}{8}$ coordinates and then take two elements y_1, y_2 of order four which commutes with z_1 and z_2. The first $\frac{n}{8}$ coordinates of both y_i must be of order at most two and so, $y_1 y_2$ is of order two, contradicting the fact that y_1, y_2 are elements of a generating set. Hence, $\delta \leq 1$. In this case, note that if we take $\mathcal{A} = \langle x_1, \ldots, x_\sigma; y_1; z_1 \rangle$ then $A = \Phi(\mathcal{A})$ is a linear code. Indeed, the value of all swappers is $\mathbf{e}$ except for $(y_1 : y_1) = y_1^2$ and $(z_1 : z_1) = z_1^2$, which are also values belonging to $\mathcal{A}$. Code $\mathcal{C} = \langle \mathcal{A}, z_2 \rangle$ has only one possible swapper given by $(z_2 : z_1)$ and so, $r(C) \leq m + 2$. Then, condition 4 holds.

4. Finally assume $\epsilon = 0$. Necessarily $z_i^2 = \mathbf{u}$ for some i, since $[z_i, z_j] = \mathbf{e}$ if z_i^2, z_j^2 and $\mathbf{u}$ are pairwise different. We may assume that $z_1^2 = \mathbf{u}$. Then $[z_1, z_i] = z_i^2$ and $[z_i, z_j] = \mathbf{e}$ for every $i, j = 2, \ldots, \rho$. We have $U = \{z_2, \ldots, z_\rho\}$ and $\langle U \rangle$ is isomorphic to $\mathbb{Z}_2^{\rho-1}$. We have two options: $\mathbf{u} \in \langle U \rangle$ or $\mathbf{u} \notin \langle U \rangle$. In the first case, reordering $z_2, \ldots, z_\rho$, we may assume that $z_2^2 z_3^2 \ldots z_k^2 = \mathbf{u}$ for some $2 < k \leq \rho$. Then we change the set

of generators by replacing z_2 by $z_2 \dots z_k$. Observe that we have passed from a normalized generating set with $\epsilon = 0$ to a normalized one with $\epsilon = 1$ and $[z_1, z_2] = z_1^2 = z_2^2 = \mathbf{u}$. This case is already studied. If $\mathbf{u} \notin \langle U \rangle$ then $\delta = 0$ and condition 3 holds. Otherwise, there exists an element of order four, y commuting with z_1 and z_2. But $[z_1, z_2] = z_2^2 \neq \mathbf{u}$, so the coordinates of order four in z_2 should coincide with the coordinates of order at most two in y and then $y^2 z_2^2 = \mathbf{u}$ or, the same $(yz_1)^2 = z_2^2$. Then $x_1, \dots, x_\rho; y_1, \dots, y_\delta; z_1' = yz_1, z_2, z_3, \dots, z_\rho$ is a new normalized generating set with $\epsilon = 1$, and $(z_1')^2 = z_2^2 = [z_1', z_2] \neq \mathbf{u}$, a case which has been treated before. This finishes the proof.

□

If $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q^{k_3}$ such that $C = \Phi(\mathcal{C})$ is a Hadamard code and with a normalized set of generating vectors satisfying condition i ($i \in \{1, \dots, 5\}$) in Theorem 4.11 we will say that $\mathcal{C}$ is of *shape* i.

Corollary 4.12. *Let $\mathcal{C}$ be a subgroup of $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times Q^{k_3}$ of length 2^m and type (σ, δ, ρ) such that $C = \Phi(\mathcal{C})$ is a Hadamard code. Let $k = k(C)$ and $r = r(C)$. Then the following statements hold:*

1. $\left\lceil \frac{m}{2} \right\rceil \leq \sigma \leq k \leq m+1 \leq r \leq m+1+\binom{\delta+\rho}{2}$ *and* $\delta+\rho = m+1-\sigma \leq \left\lfloor \frac{m+2}{2} \right\rfloor$, *with one exception for a code with parameters $m = 5, \sigma = 2, \delta = 0, \rho = 4$.*

2. $r \leq \begin{cases} m+1+\binom{\frac{m+1}{2}}{2}, & \text{if } m \text{ is odd;} \\ m+2+\binom{\frac{m}{2}}{2}, & \text{if } m \text{ is even.} \end{cases}$

   More precisely:

$$r-(m+1) \leq \begin{cases} \binom{\frac{m-1}{2}}{2}, & \text{if } m \text{ odd, } \mathrm{sh}(\mathcal{C}) = 1; \\ 1+\binom{\frac{m-1}{2}}{2}, & \text{if } m \text{ odd, } \mathrm{sh}(\mathcal{C}) = 2; \\ \binom{\frac{m+1}{2}}{2}, & \text{if } m \text{ odd, } \mathrm{sh}(\mathcal{C}) = 3; \\ \binom{\frac{m}{2}}{2}, & \text{if } m \text{ even, } \mathrm{sh}(\mathcal{C}) = 1; \\ 1+\binom{\frac{m}{2}}{2}, & \text{if } m \text{ even, } \mathrm{sh}(\mathcal{C}) = 2; \\ \binom{\frac{m}{2}}{2}, & \text{if } m \text{ even, } \mathrm{sh}(\mathcal{C}) = 3; \\ 1, & \text{if } \mathrm{sh}(\mathcal{C}) = 4; \\ 3, & \text{if } \mathrm{sh}(\mathcal{C}) = 5. \end{cases}$$

Proof. Item 1. It is clear that $k \leq m+1 = \sigma+\delta+\rho \leq r$. From Lemma 3.5 we have $\sigma \leq k$ and Lemma 3.6 gives $r \leq m+1+\binom{\delta+\rho}{2}$. Moreover $\sigma \geq \delta+\rho-1$, except for the case $\epsilon = 2$, which is shape 5. In this last case we also have $\delta = 0$ and $\rho = 4$, so σ still fulfils the inequality $\sigma \geq \delta+\rho-1$, with the exception of $(m = 5, \sigma = 2, \delta = 0, \rho = 4)$. Hence $m+1 = \sigma+\delta+\rho \leq 2\sigma+1$ (with the above exception) and therefore $\left\lceil \frac{m}{2} \right\rceil \leq \sigma \leq k$. Then $\delta+\rho = m+1-\sigma \leq m+1-\frac{m}{2} = \frac{m+2}{2}$.

Item 2. Let $h = r-(m+1)$.

For shape 1(a), $m+1 = \sigma+\delta \geq 2\delta$, hence $\delta-1 \leq \left\lfloor \frac{m-1}{2} \right\rfloor$. Therefore, $h = r-(m+1) = (\sigma+\delta+\binom{\delta-1}{2}) - (m+1) = \binom{\delta-1}{2}$. Thus, if m is odd then $h \leq \binom{\frac{m-1}{2}}{2}$ and if m is even $h \leq \binom{\frac{m-2}{2}}{2} < \binom{\frac{m}{2}}{2}$.

For shape 1(b), $m+1 = \sigma+\delta \geq 2\delta+1$, so $\delta \leq \left\lfloor \frac{m}{2} \right\rfloor$ and $h = \binom{\delta}{2}$. Thus, if m is odd then $h \leq \binom{\frac{m-1}{2}}{2}$ and if m is even $h \leq \binom{\frac{m}{2}}{2}$.

For shape 2, $m+1=\sigma+\rho\geq 2\rho-1$, so that $\rho-1\leq\lfloor\frac{m}{2}\rfloor$, and $h\leq 1+\binom{\rho-1}{2}$. Hence, if m is odd then $h\leq 1+\binom{\frac{m-1}{2}}{2}$ and if m is even $h\leq 1+\binom{\frac{m}{2}}{2}$.

For shape 3, $\sigma\geq\rho$ and $m+1=\sigma+\rho\geq 2\rho$, so $\rho\leq\lfloor\frac{m+1}{2}\rfloor$. Moreover, $h\leq\binom{\rho}{2}$. Hence, if m is odd then $h\leq\binom{\frac{m+1}{2}}{2}$ and if m is even $h\leq\binom{\frac{m}{2}}{2}$.

For shape 4, $r\leq\sigma+\delta+\rho+1\leq m+2$. Hence, $h=r-(m+1)\leq 1$.

Finally, the bound for shape 5, comes from Lemma 4.10. □

Example 4.13 (A Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code fulfilling the exception of Corollary 4.12)**.** By item 1 in Corollary 4.12, there are no Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes of length 2^m such that neither $\lceil\frac{m}{2}\rceil<k$ nor $m+1-\sigma>\lfloor\frac{m+2}{2}\rfloor$, except perhaps for a code of parameters $(m=5,\sigma=2,\delta=0,\rho=4)$. We present one example of such a code.

Consider the subgroup $\mathcal{C}$ of Q_8^8 generated by

$$\begin{aligned} z_1 &= (\mathbf{a},\mathbf{a},\mathbf{a},\mathbf{a},\mathbf{a},\mathbf{a},\mathbf{a},\mathbf{a}),\\ z_2 &= (\mathbf{b},\mathbf{b},\mathbf{ab},\mathbf{ab},\mathbf{b},\mathbf{b},\mathbf{ab},\mathbf{ab}),\\ z_3 &= (\mathbf{a},\mathbf{a},\mathbf{a}^3,\mathbf{a}^3,\mathbf{1},\mathbf{1},\mathbf{a}^2,\mathbf{a}^2),\\ z_4 &= (\mathbf{b},\mathbf{b}^3,\mathbf{ab},\mathbf{a}^3\mathbf{b},\mathbf{1},\mathbf{a}^2,\mathbf{1},\mathbf{a}^2). \end{aligned}$$

Then $\mathcal{C}$ is of type $(2,0,4)$, z_1,z_2,z_3,z_4 is a normalized generating system of $\mathcal{C}$, which is of shape 5 and $\Phi(\mathcal{C})$ is a Hadamard code. Note that $k(C)=2=\frac{m-1}{2}<3=\lceil\frac{m}{2}\rceil$, $r(C)=8=m+3$ and $m+1-\sigma=4>3=\lfloor\frac{m+2}{2}\rfloor$.

Example 4.14 (The Hadamard codes of length 16)**.** Let C be a Hadamard code of length 16 and let $r=r(C)$ and $k=k(C)$. As it was explained at the beginning of this section $(r,k)=\{(5,5),(6,3),(7,2),(8,1),(8,2)\}$. Of course if $(r,k)=(5,5)$ then C is $\mathbb{Z}_2$-linear. If $(r,k)=(6,3)$ then C is $\mathbb{Z}_2\mathbb{Z}_4$-linear and if $(r,k)\in\{(7,2),(8,1),(8,2)\}$ then C is not a $\mathbb{Z}_2\mathbb{Z}_4$-linear linear code [12]. In Proposition 4.5 we have exhibited a Hadamard Q_8-code of length 16 with $(r,k)=(7,2)$ and from item 2 of Corollary 4.12 the upper bound for the rank of $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes of length 2^4 is 7. Hence, the Hadamard codes of length 16 and rank 8 are not $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes.

5 Recursive constructions of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes

In this section we present some methods to construct quaternionic Hadamard codes from a given Hadamard code.

The complement of a binary vector v is denoted $(v)^c$. Observe that if $x\in\mathcal{G}$ then $(\Phi(c))^c=\Phi(\mathbf{u}c)$.

5.1 From $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes to Hadamard $\mathbb{Z}_4Q_8$-codes

It is known [12] that for any m we have $\lfloor\frac{m-1}{2}\rfloor$ nonequivalent $\mathbb{Z}_4$-linear Hadamard codes of binary length $n=2^m$. These codes can be characterized by the parameter δ. Note that $\delta\in\{1,2,\ldots,\lfloor\frac{m+1}{2}\rfloor\}$, but the values $\delta=1,2$ give codes equivalent to the linear Hadamard. The $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard

codes (which are not $\mathbb{Z}_4$-codes) are described in [12]. For any m there are $\lfloor \frac{m}{2} \rfloor$ nonequivalent such codes of binary length $n = 2^m$. As with the $\mathbb{Z}_4$-linear case, these codes can be characterized by the parameter $\delta \in \{0, 1, 2, \ldots, \lfloor \frac{m}{2} \rfloor\}$ and the values $\delta = 0, 1$ give codes equivalent to the linear Hadamard.

We begin by taking a $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard code to obtain a Hadamard $\mathbb{Z}_4Q_8$-code. Let $C = \Phi(\mathcal{C})$ be a $\mathbb{Z}_2\mathbb{Z}_4$-linear code, where $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. Let $\xi_1 : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4$ be the homomorphism defined by $\xi_1(i) = 2i$ and let $\xi_2 : \mathbb{Z}_4 \longrightarrow \langle \mathbf{a} \rangle \subseteq Q_8$ be the homomorphism defined by $\xi_2(i) = \mathbf{a}^i$ and generalize those to a componentwise group homomorphism $\xi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \to \mathbb{Z}_4^\alpha \times Q_8^\beta$. Let $C_q = \Phi(\mathcal{C}_q)$ be the $\mathbb{Z}_4Q_8$-code obtained from $\mathcal{C}_q = \xi(\mathcal{C})$ of binary length $2(\alpha + 2\beta) = 2n$. Code C_q is a $\mathbb{Z}_4Q_8$-code of the same type as C.

Assume additionally that $\Phi(\mathcal{C})$ is a Hadamard code. Then the length of $\Phi(\mathcal{C}_q)$ is $2n$ and all the codewords of $\Phi(\mathcal{C}_q)$ have length 0, n or $2n$. However $\Phi(\mathcal{C}_q)$ is not a Hadamard code since $|\mathcal{C}_q| = |C| = 2n$. Hence, to obtain a Hadamard code we need to double the cardinality of this code. We do that by taking $\mathcal{C}^{(x)} = \langle \mathcal{C}_q, x \rangle$ for an appropriate element $x \in \mathbb{Z}_4^\alpha \times Q_8^\beta$ of order 2 modulo $\mathcal{C}_q$ which normalizes $\mathcal{C}_q$ and $C^{(x)} = \Phi(\mathcal{C}^{(x)})$. Then $\mathcal{C}^{(x)} = \mathcal{C}_q \cup x\mathcal{C}_q$ and to make sure that $C^{(x)}$ is a Hadamard code we must choose x so that

$$\mathrm{wt}(\Phi(xc)) = n, \text{ for every } c \in \mathcal{C} \tag{9}$$

If x has order 2 then, after reordering the coordinates we may assume that $x = (\mathbf{e}_{l_1} | \, \mathbf{u}_{l_2})$, where we separate the coordinates with value $\mathbf{e}$ and $\mathbf{u}$, respectively. Then $C^{(x)} = \Phi(\mathcal{C}_q) \cup \{(c_1|(c_2)^c) : (c_1|c_2) \in C\}$, where both c_1 and c_2 have length n. Indeed, $\mathrm{wt}(c_1|(c_2)^c) = \mathrm{wt}(c_1) + n - \mathrm{wt}(c_2)$ and so, for $C^{(x)}$ to be a Hadamard code it is necessary that $\mathrm{wt}(c_1) = \mathrm{wt}(c_2)$ for every $(c_1|c_2) \in C$.

One way to ensure that $C^{(x)}$ is a Hadamard code is taking $x = (x_1, \ldots, x_{\frac{n}{2}})$ with each $x_i \in Q_8 \setminus \langle \mathbf{a} \rangle$. Condition (9) above is satisfied because for every $c \in \mathcal{C}$, all the coordinates of xc have order 4 and therefore $\mathrm{wt}(\Phi(xc)) = n$, as desired. The rank and dimension of the kernel of $C(x)$ depends on the election of x.

Example 5.1. Take $\mathcal{C} = \langle (1,1,1,1), (2,0,1,3) \rangle \subset \mathbb{Z}_4^4$. If we choose $x = (\mathbf{b}, \mathbf{b}, \mathbf{b}, \mathbf{b})$ then $C^{(x)}$ is the (unique up to equivalence) binary linear code of length 16. If we take $x = (\mathbf{b}, \mathbf{ab}, \mathbf{b}, \mathbf{ab})$ then $\mathcal{C}^{(x)}$ is the group of Proposition 4.5 and hence $C^{(x)}$ is the Hadamard Q_8-code of length 16 with rank 7 and dimension of the kernel 2. Finally, if we choose $y = (\mathbf{b}, \mathbf{b}, \mathbf{b}, \mathbf{a}^3\mathbf{b})$ then $C^{(y)}$ is a Hadamard Q_8-code of length 16, with rank 6 and dimension of kernel 3. Hence the three Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes of length 16 can be obtained applying our construction to $\mathcal{C}$.

The following theorem shows that most Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes can be obtained with this construction.

Theorem 5.2. *Let C' be a Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code. Assume that C' is either of shape 2 or 3. Then C' is equivalent to $C^{(z)}$ for C a $\mathbb{Z}_2\mathbb{Z}_4$-linear code and some z.*

Proof. Assume that $C' = \phi(\mathcal{C}')$ with $\mathcal{C}'$ a subgroup of $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^\alpha \times Q_8^\beta$ and let $x_1, \ldots, x_\sigma$; $y_1, \ldots, y_\delta$; $z_1, \ldots, z_\rho$ a normalized generating set of $\mathcal{C}'$ satisfying either condition 2 or 3 of Theorem 4.11. As $z_1^2 = \mathbf{u}$, we have $k_1 = 0$. Moreover, for shape 2, $[z_1, z_2] = \mathbf{u}$ and therefore $\alpha = 0$. Let

$$\mathcal{C}'' = \begin{cases} \langle x_1, \ldots, x_\sigma; z_1 z_2, z_3, \ldots, z_\rho \rangle, & \text{for shape 2;} \\ \langle x_1, \ldots, x_\sigma; z_2, z_3, \ldots, z_\rho \rangle, & \text{for shape 3.} \end{cases}$$

Then $\mathcal{C}''$ is an abelian subgroup of $\mathcal{C}$ of index 2. Moreover, the projection on the $\mathbb{Z}_4$ part is contained in $\{0,2\}$. This is clear for shape 2. For shape 3, it is a consequence of $[z_1, z_i] = z_i^2$ for $i \geq 2$. After a suitable permutation on the Q_8-coordinates we may assume that $\mathcal{C} \subseteq 2\mathbb{Z}_4^\alpha \times \langle \mathbf{a} \rangle^\beta$ and therefore $\mathcal{C}'' = \xi(\mathcal{C})$ for a suitable subgroup $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ such that $C = \Phi(\mathcal{C})$ is a Hadamard code. Then $\mathcal{C}' = \langle \mathcal{C}, z_1 \rangle$ and so $C' = C^{(z_1)}$.

Note that if $\mathcal{C}'$ is of shape 2, then $\alpha = 0$ and so it is equivalent to $C^{(z_1)}$ for C a $\mathbb{Z}_4$-linear code. □

Notice that if $\mathcal{C}$ is of shape 5 then $\mathcal{C}$ has no abelian subgroup of index 2 and therefore $\mathcal{C}$ can not be obtained with this type of construction.

The $\mathbb{Z}_2\mathbb{Z}_4$-linear codes C used in Theorem 5.2 have length $n = 2^m$, where $m + 1 = \sigma + \delta$ and $\sigma > \delta$ in the case we are dealing with $\mathbb{Z}_2\mathbb{Z}_4$-linear (non $\mathbb{Z}_4$-linear) codes (see [12]). The parameters of the obtained code C' after the construction in Theorem 5.2 are $m' = m + 1$, $\rho' = \delta + 1$ and $\sigma' = \sigma$. Therefore, $m' = m + 1 = \sigma + \delta = \sigma' + \rho' - 1$. The rank of C' can be computed from the rank of C adding vector z_1 and all the swappers $(z_1 : z_i)$, where $i \in \{1, \rho\}$. Thus $r(C') \leq r(C) + 1 + \rho' = \sigma + \delta + \binom{\delta}{2} + 1 + \rho' = \sigma' + \rho' + \binom{\rho'-1}{2} + \rho' = \sigma' + \rho' + \binom{\rho'}{2}$.

From Corollary 4.12, if m is odd then the upper bound $r \leq m + 1 + \binom{\frac{m+1}{2}}{2}$ can only be reached for Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes of shape 3 or shape 5 , with $m = 5$. For m even the upper bound $r \leq m + 2 + \binom{\frac{m}{2}}{2}$ only can be obtained with Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes of shape 2. For instance, for $m = 4$ this maximum is 7 and it is reached by the code of Proposition 4.5 which is of shape 2. For $m = 5$, the upper bound for the rank of a $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code is 9. In the next example we will show a $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code with $m = 5$ and rank 9, by using the latest construction.

Example 5.3. Take the Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-linear code $C = \Phi(\mathcal{C})$, with $m = 4$ and parameter $\delta = 2$. This code $\mathcal{C}$ is generated by $(1,1,1,1\,2,2,2,2,2,2)$, $(0,1,0,1,0,2,1,1,1,1)$, $(0,0,1,1,1,1,0,1,2,3) \in \mathbb{Z}_2^4 \times \mathbb{Z}_4^6$.

Now, construct $\xi(\mathcal{C}) \subset \mathbb{Z}_4^4 \times Q_8^6$ generated by

$$\begin{aligned} x_1 &= (2,2,2,2,\mathbf{a}^2,\mathbf{a}^2,\mathbf{a}^2,\mathbf{a}^2,\mathbf{a}^2,\mathbf{a}^2) \\ z_2 &= (0,2,0,2,\mathbf{1},\mathbf{a}^2,\mathbf{a},\mathbf{a},\mathbf{a},\mathbf{a}) \\ z_3 &= (0,0,2,2,\mathbf{a},\mathbf{a},\mathbf{1},\mathbf{a},\mathbf{a}^2,\mathbf{a}^3) \end{aligned}$$

If we choose $z_1 = (1,1,1,1,\mathbf{b},\mathbf{ab},\mathbf{b},\mathbf{ab},\mathbf{ab},\mathbf{a}^3\mathbf{b})$ then $C^{(z_1)}$ is a Hadamard code of length 32, type $(3,0,3)$, shape 3, rank $r = 9$ and dimension of the kernel $k = 3$.

5.2 The generalized Kronecker construction

We give a generalization of the Kronecker construction of Hadamard matrices in the context of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes.

If H is a Hadamard matrix then the Kronecker matrix of H is $\mathcal{K}(H) = \begin{pmatrix} H & H \\ H & -H \end{pmatrix}$, which is another Hadamard matrix. If C is the Hadamard code associated to H and $\mathcal{K}(C)$ is the Hadamard code associated to $\mathcal{K}(H)$ then $\mathcal{K}(C)$ is formed by concatenation of vectors so, the vectors in $\mathcal{K}(C)$ are of the form $(c|c)$ and $(c|(c)^c)$, with $c \in C$.

Let $\Delta : \mathcal{G} \to \mathcal{G} \times \mathcal{G}$ be the diagonal map, i.e., $\Delta(x) = (x|x)$ for each $x \in \mathcal{G}$.

Assume that $C = \Phi(\mathcal{C})$, for $\mathcal{C}$ a subgroup of $\mathcal{G}$. Then $\mathcal{K}(C) = \Phi(\mathcal{K}(\mathcal{C}))$ where $\mathcal{K}(\mathcal{C}) = \langle \Delta(\mathcal{C}), (1|\mathbf{u}) \rangle$. Moreover $k(\mathcal{K}(C)) = k(C) + 1$, $r(\mathcal{K}(C)) = r(C) + 1$ and if $\mathcal{C}$ is of type (σ, δ, ρ) then $\mathcal{K}(\mathcal{C})$ is of type $(\sigma + 1, \delta, \rho)$.

More generally, let g be an element of $\mathcal{G}$ of order 2 modulo $\mathcal{C}$ which normalizes $\mathcal{C}$, i.e.,

$$\mathcal{C}^g = \mathcal{C} \quad \text{and} \quad g^2 \in \mathcal{C}.$$

Consider the subgroup $\mathcal{K}_g(\mathcal{C}) = \langle \Delta(\mathcal{C}), (g|g\mathbf{u}) \rangle$ of $\mathcal{G} \times \mathcal{G}$. For instance, $\mathcal{K}_g(\mathcal{C}) = \mathcal{K}(\mathcal{C})$ if and only if $g \in \mathcal{C}$. We claim that $\Phi(\mathcal{K}_g(\mathcal{C}))$ is a Hadamard code.

First we have that $\Delta(\mathcal{C})$ is a subgroup of $\mathcal{G} \times \mathcal{G}$ of cardinality $2n$. Moreover, $(g|g\mathbf{u})^2 = (g^2|g^2) \in \Delta(\mathcal{C})$; $\mathcal{C}^g = \mathcal{C}$ and $c \in \mathcal{C}$ then $(g|g\mathbf{u})^{-1}(c|c)(g|g\mathbf{u}) = (gcg^{-1}|gcg^{-1})$. Therefore $\mathcal{K}_g(\mathcal{C}) = \Delta(\mathcal{C}) \cup \{(gc|g\mathbf{u}c) : c \in \mathcal{C}\}$ is a subgroup of $\mathcal{G} \times \mathcal{G}$ of cardinality $4n$. Furthermore, for every $c \in \mathcal{C}$ we have $\mathrm{wt}(\Phi(c|c)) = 2\mathrm{wt}(\Phi(c)) \in \{0, n, 2n\}$ and $\mathrm{wt}(\Phi(cg|c\mathbf{u}g)) = \mathrm{wt}(\Phi(cg)|(\Phi(cg))^c) = \mathrm{wt}(\Phi(cg)) + 2n - \mathrm{wt}(\Phi(cg)) = 2n$.

Moreover, $r(\mathcal{K}_g(C)) = r(C) + 1$ and $k(\mathcal{K}_g(C)) \leq k(C) + 1$. Assume that $\mathcal{C}$ is of type (σ, δ, ρ). If g has order 2 then $\mathcal{K}_g(\mathcal{C})$ is of type $(\sigma + 1, \delta, \rho)$. If g has order 4 and commutes with all the elements of $Z(\mathcal{C})$ then $\mathcal{K}_g(\mathcal{C})$ is of type $(\sigma, \delta + 1, \rho)$. Finally, if $C_{Z(\mathcal{C})}(g) = \{x \in Z(\mathcal{C}) : xg = gx\}$ is of order $\sigma + \delta_1$ with $\delta_1 < \delta$ then $\mathcal{K}_g(\mathcal{C})$ is of type $(\sigma, \delta_1, \rho + \delta - \delta_1 + 1)$.

Example 5.4. As an example of the above construction, from the code C constructed in Proposition 4.5 and taking $g = (\mathbf{b}, \mathbf{ab}, \mathbf{1}, \mathbf{1}) \in Q_8^4$ we obtain a new code $\mathcal{K}_g(C)$ of binary length 32, which is a quaternionic Hadamard, non $\mathbb{Z}_2\mathbb{Z}_4$-linear code, with dimension of the kernel 2 and rank 8. It is equivalent to the code of Example 4.13.

Example 5.5. Note that in some cases, when the size of the kernel of C is strictly greater than the size of the center of $\mathcal{C}$ it could happen that using the above generalized Kronecker construction the dimension of the kernel of the new code $\mathcal{K}_g(C)$ is lower than the original. As an example, take $\mathcal{C}$ the subgroup of Q_8^8 generated by

$$\begin{aligned} z_1 &= (\mathbf{a}, \mathbf{a}, \mathbf{a}, \mathbf{a}, \mathbf{a}, \mathbf{a}, \mathbf{a}, \mathbf{a},) \\ z_2 &= (\mathbf{b}, \mathbf{ab}, \mathbf{b}, \mathbf{ab}, \mathbf{b}, \mathbf{ab}, \mathbf{b}, \mathbf{ab}) \\ z_3 &= (\mathbf{a}^2, \mathbf{1}, \mathbf{a}^2, \mathbf{1}, \mathbf{a}^2, \mathbf{1}, \mathbf{a}^2, \mathbf{1}) \\ z_4 &= (\mathbf{a}^2, \mathbf{a}^2, \mathbf{1}, \mathbf{1}, \mathbf{a}, \mathbf{a}, \mathbf{a}^3, \mathbf{a}^3) \end{aligned}$$

The corresponding binary code $C = \Phi(\mathcal{C})$ is a Hadamard, non $\mathbb{Z}_2\mathbb{Z}_4$-linear code of length 32, type $(3, 0, 3)$, shape 3, rank 7 and dimension of the kernel 4.

Take $g = (\mathbf{a}^2, \mathbf{a}^2, \mathbf{1}, \mathbf{1}, \mathbf{b}, \mathbf{ab}, \mathbf{b}, \mathbf{ab}) \in Q_8^8$ and construct $\mathcal{K}_g(C)$, which turn out to be a Hadamard, non $\mathbb{Z}_2\mathbb{Z}_4$-linear, code of length 64, type $(3, 0, 4)$, shape 2, rank 8 and dimension of the kernel 3.

5.3 Some final remarks

Using the above constructions from an initial well known code (linear or $\mathbb{Z}_2\mathbb{Z}_4$-linear) we can construct several infinite families of $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes, which are not $\mathbb{Z}_2\mathbb{Z}_4$-linear .

We already mentioned that the Hadamard codes of length 16 can be completely classified using the invariants given by the rank and the dimension of the kernel. However, in general, for larger lengths, we can find nonisomorphic Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes with the same invariants.

Example 5.6. As an example, consider the code C in Example 5.5. It is a binary Hadamard, non $\mathbb{Z}_2\mathbb{Z}_4$-linear code of length 32, rank 7 and dimension of the kernel 4. We also know a $\mathbb{Z}_2\mathbb{Z}_4$-linear code of length 32, rank 7 and dimension of the kernel 4 (item 1 of Theorem 4.11). It is the code C', where $C' = \Phi(\mathcal{C}')$ and $\mathcal{C}'$ is a subgroup of $\mathbb{Z}_2^8 \times \mathbb{Z}_4^{12}$ generated by:

$$\begin{aligned} x_1 =&(1,1,1,1,1,1,1,1,2,2,2,2,2,2,2,2,2,2,2,2)\\ x_2 =&(0,0,0,0,1,1,1,1,0,0,0,0,0,0,2,2,2,2,2,2)\\ y_1 =&(0,1,0,1,0,1,0,1,0,2,1,1,1,1,0,2,1,1,1,1)\\ y_2 =&(0,0,1,1,0,0,1,1,1,1,0,1,2,3,1,1,0,1,2,3) \end{aligned}$$

Note that the examples we wrote into the paper achieve almost all the shapes according Theorem 4.11. For instance, shape 1 is satisfied for all well known $\mathbb{Z}_2\mathbb{Z}_4$-linear and $\mathbb{Z}_4$-linear Hadamard codes; the code in Proposition 4.5 is of shape 2; the code in Example 5.3 is of shape 3 and the code in Example 4.13 is of shape 5. However, we have not yet found any examples of shape 4. We supply such an example below.

Example 5.7. Let $\mathcal{C}$ be the code $\langle (1,1,0,0,\mathbf{a}), (1,0,1,0,\mathbf{b}),$ $(1,1,1,1,\mathbf{a}^2)\rangle$. The code $\mathcal{C}$ is of shape 4 and the binary $\mathbb{Z}_2^4 \times Q_8$-code $C = \Phi(\mathcal{C})$ is a linear Hadamard code.

We can use a slight variation of the Kronecker construction to obtain a shape 4 non linear code with the maximum rank allowed for this shape.

First of all, we use the Kronecker construction to obtain the code $\mathcal{D} = \mathcal{K}(\mathcal{C})$, which is generated by

$$\begin{aligned} x_1 =&(1,1,1,1,1,1,1,1,\mathbf{a}^2,\mathbf{a}^2)\\ x_2 =&(0,0,0,0,1,1,1,1,\mathbf{1},\mathbf{a}^2)\\ z_1 =&(1,1,0,0,1,1,0,0,\mathbf{a},\mathbf{a})\\ z_2 =&(1,0,1,0,1,0,1,0,\mathbf{b},\mathbf{b}) \end{aligned}$$

The code $D = \Phi(\mathcal{D})$ is a (linear) binary code of length 16, shape 4 and dimension of the kernel and rank equal to the dimension of D, which is 5.

Finally, take the code $\bar{\mathcal{D}}$ with generators x_1, x_2, z_1 and

$$\bar{z}_2 = (1,0,1,0,1,0,1,0,\mathbf{ab},\mathbf{b}).$$

It is straightforward to check that $\bar{\mathcal{D}}$ is of shape 4 and the binary code $\bar{D} = \Phi(\bar{\mathcal{D}})$ is of rank 6. Indeed, the code $\bar{\mathcal{D}}$ has a new swapper $(z_1 : \bar{z}_2) = (0,\ldots,0,\mathbf{a}^2,\mathbf{1})$ which did not exist in $\mathcal{D}$.

Acknowledgment

The authors wish to thank J. Borges and M. Villanueva for useful discussions and valuable comments. Also, the authors would like to thank the anonymous referees for their very useful comments and suggestions.

References

[1] E. F. Assmus Jr. and J. D. Key, *D*esigns and their codes, Cambridge University Press, Great Britain, 1992.

[2] J. Borges, C. Fernández and J. Rifà, "Every $\mathbb{Z}_{2k}$-code is a binary propelinear code", *In COMB'01. Electronic Notes in Discrete Mathematics*, vol. 10, Elsevier Science, November 2001.

[3] 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.

[4] J. Borges and J. Rifà, "A characterization of 1-perfect additive codes", *IEEE Trans. on Information Theory*, vol. 45(5), pp. 1688-1697, 1999.

[5] J. Borges, K. Phelps, J. Rifà and V. Zinoviev, "On $\mathbb{Z}_4$-Linear Preparata-Like and Kerdock-Like Codes". *IEEE Trans. on Information Theory*, vol. 49(11), pp. 2834-2843, 2003.

[6] . J. Doyen, X. Hubaut and M. Vandensavel, "Ranks of incidence matrices of Steiner triple systems", Math. Z., Vol. 163 (1978) pp. 251-259.

[7] C. Fernández-Córdoba, J. Pujol, 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.

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

[9] D.S. Krotov, "$\mathbb{Z}_4$-linear Hadamard and extended perfect codes". Electron. Notes Discrete Math. 6, pp. 107-112 (2001).

[10] F. I. MacWilliams and N. J. Sloane, *The theory of Error-Correcting codes*, North-Holland, New York (1977).

[11] K. T. Phelps, J. Rifà and M. Villanueva, "Rank and Kernel of binary Hadamard codes", *IEEE Trans. on Information Theory*, vol. 51, no. 11, pp: 3931-3937, 2005.

[12] 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. on Information Theory*, vol. 52, no. 1, pp. 316-319, 2006.

[13] J. Rifà, J.M. Basart and L. Huguet, "On completely regular propelinear codes", in *Proc. 6th International Conference, AAECC-6.* 1989, number 357 in LNCS, pp. 341-355, Springer-Verlag.

[14] J. Rifà and J. Pujol, "Translation invariant propelinear codes", *IEEE Trans. on Information Theory*, vol. 43, pp. 590-598, 1997.

[15] L. Teirlinck, "On projective and affine hyperplanes", J. Combinatorial Theory, Ser. A, Vol. 28 (1980), pp. 290-306.