On the additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes. Rank and Kernel

Kevin T. Phelps, Josep Rifà, *Senior Member, IEEE,* and Mercè Villanueva

***Abstract*— All the possible non-isomorphic additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes are characterized and, for each one, the rank and the dimension of the kernel is computed.**

***Index Terms*— additive codes, extended perfect codes, Hadamard matrices, Hadamard codes, kernel, rank, $\mathbb{Z}_4$-linear codes.**

I. Introduction

Let $\mathbb{Z}_4$ and $\mathbb{F} = \mathbb{Z}_2$ be the additive groups of integers modulo 4 and 2 respectively. Let $\mathbb{F}^n$ denote the set of all binary vectors of length n. The Hamming distance between two vectors $x, y \in \mathbb{F}^n$ is denoted by $d(x, y)$. The support of a vector $x \in \mathbb{F}^n$ is the set of nonzero coordinate positions of x and is denoted by $supp(x)$.

A *(binary)* (n, M, d)*-code* is a subset, C, of $\mathbb{F}^n$ such that $|C| = M$ and $d(c_1, c_2) \geq d$ for every different $c_1, c_2 \in C$. The elements of a code are called *codewords*. A *1-perfect code* C of length n is a subset of $\mathbb{F}^n$ such that all the vectors in $\mathbb{F}^n$ are within distance one from a unique codeword. For any $t > 1$ there exists exactly one linear 1-perfect code of length $2^t - 1$, up to isomorphism, which is the well-known *Hamming code*. An *extended code* of the code C is a code resulting from adding an overall parity check digit to each codeword of C.

Two codes $C_1, C_2 \in \mathbb{F}^n$ are *equivalent* if there exists a vector $a \in \mathbb{F}^n$ and a permutation π such that $C_2 = \{a + \pi(c) \mid c \in C_1\}$.

Two structural properties of non-linear codes are the rank and kernel. The *rank* of a binary code C, $r = rank(C)$, is simply the dimension of the linear span of the words of C. By the binary orthogonal code of the non-linear code C, denoted by $C^{\perp}$, we mean the dual of the subspace spanned by C having dimension $n - r$. The *kernel* of a binary code C is defined as $K(C) = \{x \in \mathbb{F}^n \mid x + C = C\}$. If the zero word is in C, then $K(C)$ is a linear subspace of C. In general, C can be written as the union of cosets of $K(C)$ and $K(C)$ is the largest such linear code for which this is true [1]. We will denote the dimension of the kernel of C by $k = ker(C)$.

The celebrated article [12] about $\mathbb{Z}_4$-linear codes has spawned significant research relating such codes to classical well-known codes which were not linear, such as the Preparata codes or the Kerdock codes as well as linear codes such as Reed-Muller codes. The tool used to view a $\mathbb{Z}_4$ code as a binary code is the Gray map φ, which takes a $\mathbb{Z}_4$ symbol and maps it into a pair of bits as

Research partially supported by CICYT Grants TIC2003-08604-C04-01, TIC2003-02041 and by Catalan DURSI Grant 2001SGR 00219.

K. T. Phelps is with the Dept. of Mathematics & Statistics, Auburn University, Auburn, Al 36849-5307 (email: phelpkt@auburn.edu).

Josep Rifà and Mercè Villanueva are with the Dept. of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (email: {josep.rifa, merce.villanueva}@autonoma.edu).

follows: $\varphi(0) = 00$, $\varphi(1) = 01$, $\varphi(2) = 11$, $\varphi(3) = 10$. The Gray map is an isometry which transforms Lee distances defined in the quaternary ones to Hamming distances defined in the binary codes.

More general than the $\mathbb{Z}_4$-linear codes are the additive codes, which, roughly speaking, can be seen as codes with some coordinates in $\mathbb{Z}_2$ and other coordinates in $\mathbb{Z}_4$ in such a way that the code is an Abelian subgroup of $(\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta, +)$, where $+$ means the usual additive operation on $\mathbb{Z}_2$ and $\mathbb{Z}_4$.

The paper is arranged as follows. In section 2, we introduce the definitions, constructions and general properties for additive codes and Hadamard additive codes. In section 3 and 4 we compute, respectively, the rank and the dimension of the kernel for additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes, using the fact that they are the additive dual of extended 1-perfect additive codes. We will see that either of these two parameters, the rank or the dimension of the kernel, completely characterize these codes.

II. Additive Codes and Additive Hadamard Codes

Let $\star$ be a binary operation defined in $\mathbb{F}^n$, such that $u \star v \in \mathbb{F}^n$ for $v, u \in \mathbb{F}^n$. We consider the algebraic structure of $\mathbb{F}^n$ with such an operation. Let $\mathbf{0}$ be the zero vector and, for $i = 1, \ldots, n$, let e_i be the vector of weight 1 with the nonzero coordinate in the ith position.

The operation $\star : \mathbb{F}^n \times \mathbb{F}^n \longrightarrow \mathbb{F}^n$ is said to be *distance-compatible* (see [10]) if for every $v \in \mathbb{F}^n$ there exists a coordinate permutation π_v, such that:

(i) $v \star e_i = v + e_{\pi_v(i)}$, for $i = 1, \ldots, n$

(ii) $v \star \mathbf{0} = \mathbf{0} \star v = v$

(iii) $v \star e_i = w \star e_i$ if and only if $w = v$.

If $(\mathbb{F}^n, \star)$ is a group and $\star$ is distance-compatible, then we say that $(\mathbb{F}^n, \star)$ is a *distance-compatible group*.

Definition 2.1: An additive code of length n is a subgroup of $(\mathbb{F}^n, \star)$, where $(\mathbb{F}^n, \star)$ is a distance-compatible Abelian group.

Additive codes were first defined in [4, p.71] in terms of association schemes. In [2] it is proved that, when the association scheme is the Hamming scheme $\mathbb{F}^n$, then Definition 2.1 is equivalent to that of [4]. Also in [2] it is proved that a (binary) additive code $(C, \star)$ of length n is isomorphic to a subgroup of $(\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta, +)$, where $+$ means the usual additive operation on $\mathbb{Z}_2$ and $\mathbb{Z}_4$. Code C has length $n = \alpha + 2\beta$ as a binary code and we will say that C is an additive code of type (α, β). Note that the case $\beta = 0$ corresponds to a binary linear code and the case $\alpha = 0$ corresponds to a $\mathbb{Z}_4$-linear code.

The isomorphism $(\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta, +) \cong (\mathbb{F}^n, \star)$, where $\alpha + 2\beta = n$ is given by:

$$\Phi(x, y) = (x, \phi(y)) \quad \forall x \in \mathbb{Z}_2^\alpha,\ \forall y \in \mathbb{Z}_4^\beta;$$

where $\phi : \mathbb{Z}_4^\beta \longrightarrow \mathbb{Z}_2^{2\beta}$ is the usual Gray map, that is, $\phi(y_1, \ldots, y_\beta) = (\varphi(y_1), \ldots, \varphi(y_\beta))$, and $\varphi(0) = (0,0), \varphi(1) = (0,1), \varphi(2) = (1,1), \varphi(3) = (1,0)$. Hence, $u \star v = \Phi(\Phi^{-1}(u) + \Phi^{-1}(v)), \quad \forall u, v \in \mathbb{F}^n$.

We will use C to mean the additive code in $\mathbb{F}^n$ and $\mathcal{C} = \Phi^{-1}(C)$ for the subgroup in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$.

In $\mathcal{C}$ we define an inner product (see [9]) such that for any $u, v \in \mathcal{C}$ we have

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

and we also define the dual code $\mathcal{C}^\perp$ in the standard way

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

We will use $C_\perp = \Phi(\mathcal{C}^\perp)$ to mean the binary code, additive dual of C.

A *Hadamard matrix* H of order n is an $n \times n$ matrix of $+1$'s and -1's such that $HH^T = nI$, where I is the $n \times n$ identity matrix. In other words, the real

inner product of any row with itself is n and distinct rows are orthogonal. Since $nH^{-1} = H^T$, we also have $H^T H = nI$, thus the columns have the same properties and the transpose of any Hadamard matrix, H, is also a Hadamard matrix, which is not necessary equivalent to H. We know that if a Hadamard matrix H of order n exists, then n is 1, 2 or a multiple of 4 (see [6]).

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. We can change the first row and column of H into $+1$'s and we obtain an equivalent Hadamard matrix which is called *normalized*.

From now on, we will use H' to denote a normalized Hadamard matrix of order n. If $+1$'s are replaced by 0's and -1's by 1's, H' is changed into a *(binary) Hadamard matrix* $c(H')$. Since the rows of H' are orthogonal, any two rows of $c(H')$ agree in $n/2$ places and differ in $n/2$ places, and so have Hamming distance $n/2$. The binary $(n, 2n, n/2)$-code consisting of the rows of $c(H')$ and their complements is called a *(binary) Hadamard code* (see [6]) and we will use H to denote it.

A first and easy example of a Hadamard matrix is given by the binary dual code of an extended (binary) Hamming code. When we consider non-linear extended (binary) 1-perfect codes, we can find Hadamard matrices in [5] constructed by using the codewords of the quaternary dual code corresponding to an extended 1-perfect $\mathbb{Z}_4$-linear code. A more general construction can be found in [3] where additive codes are used and not just $\mathbb{Z}_4$-linear ones. In all these cases, the Hadamard matrices will have order a power of 2.

Let $(C, \star)$ be an additive code of type (α, β). For each $x \in C$ we can define a coordinate permutation π_x, such that for every $y \in C$, $x \star y = x + \pi_x(y)$. Again let e_i be the vector with all the coordinates zeroes except for the i-th coordinate which is 1. If i is in the first α coordinates, then $\pi_x(e_i) = e_i$, otherwise let i' the companion coordinate of i after the Gray map, then permutation π_x is such that

$$\begin{aligned}
&\pi_x(e_i) = e_i \quad \text{if } i, i' \notin supp(x)\\
&\pi_x(e_i) = e_i \quad \text{if } i, i' \in supp(x)\\
&\pi_x(e_i) = e_{i'} \quad \text{if } i \in supp(x) \text{ and } i' \notin supp(x)\\
&\pi_x(e_i) = e_{i'} \quad \text{if } i' \in supp(x) \text{ and } i \notin supp(x)
\end{aligned}$$

Code $(C, \star)$ is also a propelinear code and for our purposes we only need to emphasize that for all $x, y \in C$ we have $\pi_{x\star y} = \pi_x \pi_y$ (see [11]).

Lemma 2.1: Let $(C, \star)$ be an additive code (Definition 2.1) and let D be the binary linear span of C, so D is the minimum linear binary code which contains C. Then D is generated by all the vectors $\pi_x(y)$, where $x, y \in C$ and $(D, \star)$ is an additive code too.

Proof: For $x, y \in C$ we have that $x \star y = x + \pi_x(y) \in C$ and so, $x + x \star y \in D$. This means that for all $x, y \in C$, $\pi_x(y) \in D$. Let S be the binary linear span of $\{\pi_x(y)\}$. Note that $C \subset S$, since $0 \in C$ and $x = \pi_0(x)$, so $D = S$.

To prove that D is an additive code we need to show that

$$\big(\sum_j \pi_{x_j}(y_j)\big) \star \big(\sum_k \pi_{x_k}(y_k)\big) \in D \qquad (1)$$

where all the vectors x_j, y_j, x_k, y_k are in C. Since operation $\star$ is commutative and, in general, $a \star (b + c) = a + (a \star b) + (a \star c)$, to prove (1) we just need to see that for all $x, y, z, w \in C$

$$\pi_x(y) \star \pi_z(w) \in D.$$

We know that $\pi_x(y) \star \pi_z(w) = \pi_x(y) + \pi_{\pi_x(y)}(\pi_z(w))$ so, we need to prove that $\pi_{\pi_x(y)}(\pi_z(w)) \in D$. Now observe that for all $a, b, c \in C$ we can compute $\pi_{\pi_a(b)}(c) = c + \pi_a(b) + \pi_{a\star c}(b)$, since $\pi_a(b) \star c = c \star \pi_a(b)$ and

thus $\pi_{\pi_x(y)}(\pi_z(w)) = \pi_z\big(w + \pi_x(y) + \pi_x\pi_w(y)\big) = \pi_z(w) + \pi_{z\star x}(y) + \pi_{z\star x\star w}(y) \in D$. ■

III. Additive $\mathbb{Z}_4$-linear Hadamard codes. Rank and kernel

We will begin considering $\mathbb{Z}_4$-linear Hadamard codes. These codes are the quaternary dual of the extended 1-perfect $\mathbb{Z}_4$-linear codes.

The characterization of the extended 1-perfect $\mathbb{Z}_4$-linear codes, up to equivalence, is given in [3], so we know that for each possible length, $n = 2^t$, there are exactly $\lfloor \frac{t+1}{2} \rfloor$ non-equivalent extended 1-perfect $\mathbb{Z}_4$-linear codes. Each one of these codes can be given by a parity check matrix consisting of all column vectors of the form $\bar{\mathbb{Z}}_2^{\gamma} \times \{1 \in \mathbb{Z}_4\} \times \mathbb{Z}_4^{\delta-1}$, where $t+1 = \gamma + 2\delta$ and $\bar{\mathbb{Z}}_2$ means the subgroup $\{0, 2\} \subset \mathbb{Z}_4$. This parity check matrix can be seen as the generator matrix for the corresponding $\mathbb{Z}_4$-linear Hadamard code which is a code of type $4^{\delta}2^{\gamma}$ using the same notation as in [12]. Note that in all these codes the quaternary all ones vector (which we will denote by $\mathbf{1}$) is always into the code.

For instance, in the case $n = 32$ ($t = 5$) there are three possible generator matrices given by ($\gamma = 0, \delta = 3$), ($\gamma = 2, \delta = 2$) and ($\gamma = 4, \delta = 1$). The figure 1 shows the generator matrix for the corresponding $\mathbb{Z}_4$-linear Hadamard code with parameters ($\gamma = 2, \delta = 2$).

Cases $\delta = 1$ and $\delta = 2$ give us isomorphic $\mathbb{Z}_4$-linear Hadamard codes, so there are $\lfloor \frac{t-1}{2} \rfloor$, and not $\lfloor \frac{t+1}{2} \rfloor$, non-equivalent $\mathbb{Z}_4$-linear Hadamard codes (see [5] or Corollary 3.4).

Now, we will compute the rank and the dimension of the kernel for all these $\mathbb{Z}_4$-linear Hadamard codes.

Proposition 3.1: For all $\delta \in \{3, \ldots, \lfloor \frac{t+1}{2} \rfloor\}$, the corresponding quaternary dual code of the extended 1-perfect $\mathbb{Z}_4$-linear code, that is, the $\mathbb{Z}_4$-linear Hadamard code H has $rank(H) = t + 1 + \binom{\delta-1}{2}$. For $\delta = 1, 2$, the $\mathbb{Z}_4$-linear Hadamard code is a binary linear code and has $rank(H) = t + 1$.

Proof: By Lemma 2.1, we know that for all x, y in the $\mathbb{Z}_4$-linear Hadamard code H, vectors $\pi_x(y)$ generate the binary linear span of this code, and so the rank will be the number of independent vectors in $\{\pi_x(y) \,|\, x, y \in H\}$.

In the generator matrix G of H there are γ vectors of order two (e.g. see figure 1) and δ vectors of order four. Take the Gray map of the vectors of order two and, for the vectors u of order four consider $x = \Phi(u)$ and $\pi_x(x) = \Phi(3u)$. All these $\gamma + 2\delta$ binary vectors are independent since for the vectors of order four $x = \Phi(u)$ and $\pi_x(x) = \Phi(3u)$ are independent over $\mathbb{Z}_2$. Now, we have established that the rank will be $\gamma + 2\delta + d$, where d is the number of additional independent vectors taken from $\{\pi_x(y)\}$, where x, y correspond to different rows in the quaternary part of G. Since $x\star y = y\star x$, $\pi_y(x) = y + x + \pi_x(y)$, there are a maximum of $\binom{\delta}{2}$ additional independent vectors. We know that $\pi_{\Phi(\mathbf{1})}(y) = \pi_y(y)$, so we can rule out these vectors in the previous count. Moreover, the rest of vectors $\pi_x(y)$, where $x \neq y$ and $x, y \neq \Phi(\mathbf{1})$ are independent, since there exists some quaternary coordinate where vectors x and y have value (01) and all the other vectors have value (00) but for the vector $\pi_x(y)$ which has the value (10). Then, the rank is $\gamma + 2\delta + \binom{\delta-1}{2} = t + 1 + \binom{\delta-1}{2}$.

Note that for $\delta = 1, 2$ the above argument can not be considered so, in these cases, the rank is only $\gamma + 2\delta = t + 1$. ■

We know that two equivalent codes have the same rank, so this previous result (Proposition 3.1) leads us to Corollary 3.4.

The kernel for $\mathbb{Z}_4$-linear Hadamard codes was previ-

$$\left(\begin{array}{cccccccccccccccc} 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 \end{array}\right)$$

Fig. 1. Generator matrix for the $\mathbb{Z}_4$-linear Hadamard code with parameters ($\gamma = 2, \delta = 2$)

ously computed in [5] (see also [3]), but we will prove the statement again in order to keep our arguments self contained.

Lemma 3.2: Let C be a $\mathbb{Z}_4$-linear Hadamard code, then the only independent vectors in the kernel of C are those of order two and vector $\Phi(\mathbf{1})$.

Proof: A vector $v \in C$ is in the kernel if and only if $v+x \in C$, for all $x \in C$. We know that $v+x = v \star \pi_v(x)$, so $v \in C$ is in the kernel if and only if $\pi_v(x) \in C$, for all $x \in C$. Vectors v of order two have $\pi_v = Id$ and are in the kernel. The vector $\Phi(\mathbf{1})$, for which $\pi_{\Phi(\mathbf{1})}(x) = \pi_x(x) = x \star x \star x \in C$, is also in the kernel of C.

Apart from these vectors, we will see that there are no more independent vectors in the kernel of C. By the proof of Proposition 3.1, all the vectors $x \neq y$ which are not of order two and $x, y \neq \Phi(\mathbf{1})$, the $\pi_x(y)$ form a set of independent vectors and also independent from vectors of order two in C. By Lemma 2.1 these vectors are in the linear span of C, but out of C. ■

Proposition 3.3: [5] (see also [3]) For all the values $\delta \in \{3, \ldots, \lfloor \frac{t+1}{2} \rfloor\}$, the corresponding $\mathbb{Z}_4$-linear Hadamard code of length 2^t has $ker(H) = t + 2 - \delta$. For $\delta = 1, 2$, the $\mathbb{Z}_4$-linear Hadamard code is a binary linear code and has $ker(H) = t + 1$.

Proof: By Lemma 3.2 in the $\mathbb{Z}_4$-linear Hadamard code, H, all the vectors of order two and the vector $\Phi(\mathbf{1})$ are in the kernel, so all the γ vectors of order two and the δ vectors $x \star x$, for all x in the last δ rows of the generator matrix G, are in the kernel. This means that in the kernel there are at least $\gamma + \delta + 1 = t + 2 - \delta$ independent binary vectors. Again, by Lemma 3.2, for $\delta \geq 3$ there are no more vectors in the kernel. ■

Finally, after doing the exact computation for the rank and the dimension of the kernel, we can give the following characterization that was previously stated in [3] and [5].

Corollary 3.4: [3], [5] For each possible value δ, there exists a unique quaternary dual code H of the extended 1-perfect $\mathbb{Z}_4$-linear code and all these codes H are pairwise non-equivalent, except for $\delta = 1$ and $\delta = 2$, where the codes H coincides with the binary dual of the extended Hamming code.

IV. Additive non-$\mathbb{Z}_4$-linear Hadamard codes. Rank and kernel

Next question leads us to consider additive non-$\mathbb{Z}_4$-linear Hadamard codes. The additive dual of these codes are the extended 1-perfect additive non-$\mathbb{Z}_4$-linear codes.

The characterization of the extended 1-perfect additive non-$\mathbb{Z}_4$-linear codes, up to equivalence, is given in [3], so we know that for each $t \geq 3$ and length, $n = 2^t$, there are exactly $\lfloor \frac{t}{2} \rfloor$ non-equivalent extended 1-perfect additive non-$\mathbb{Z}_4$-linear codes. Each one of these codes is the kernel of a group homomorphism

$$\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta} \longrightarrow \mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta},$$

$$\left(\begin{array}{cccccccc|cccccccccc} 1&1&1&1&1&1&1&1&2&2&2&2&2&2&2&2&2&2&2&2\\ 0&0&0&0&1&1&1&1&0&0&0&0&0&0&2&2&2&2&2&2\\ \hline 0&0&1&1&0&0&1&1&1&1&1&1&0&2&1&1&1&1&0&2\\ 0&1&0&1&0&1&0&1&0&1&2&3&1&1&0&1&2&3&1&1 \end{array}\right)$$

Fig. 2. Generator matrix for the additive non-$\mathbb{Z}_4$-linear Hadamard code with parameters ($\alpha = 8, \beta = 12, \gamma = 2, \delta = 2$)

where $\alpha = 2^{\gamma+\delta-1}$, $\beta = 2^{\gamma+2\delta-2} - 2^{\gamma+\delta-2}$ and they can be given by a parity check matrix $\left(\begin{array}{c|c} A & B \\ \hline D & Q \end{array}\right)$. The submatrix A is a binary $(\gamma \times \alpha)$ matrix; B is a $(\gamma \times \beta)$ matrix whose elements are in $\bar{Z}_2 = \{0, 2\} \subset \mathbb{Z}_4$; D is a binary $(\delta \times \alpha)$ matrix and Q is a quaternary $(\delta \times \beta)$ matrix. The column vectors of this parity check matrix are all possible (up to sign) vectors of the form $\{1 \in \mathbb{Z}_2\} \times \mathbb{Z}_2^{\gamma-1} \times \mathbb{Z}_4^{\delta}$, where $\delta \in \{0, 1, 2, \cdots, \lfloor \frac{t}{2} \rfloor\}$ and $\gamma + 2\delta = t + 1$. There are exactly α nonzero column vectors of order two which we will write as the first α columns using binary notation and β independent column vectors of order four which we will write as the last β columns. This parity check matrix can be seen as the generator matrix for the corresponding additive non-$\mathbb{Z}_4$-linear Hadamard code.

For instance, in the case $n = 32$ ($t = 5$) there are three possible generator matrices given by ($\gamma = 2, \delta = 2$), ($\gamma = 4, \delta = 1$) and ($\gamma = 6, \delta = 0$). The figure 2 shows the generator matrix for the corresponding additive non-$\mathbb{Z}_4$-linear Hadamard code with parameters ($\gamma = 2, \delta = 2$) and so ($\alpha = 8, \beta = 12$).

Cases $\delta = 0$ and $\delta = 1$ give us isomorphic additive non-$\mathbb{Z}_4$-linear Hadamard codes, so there are $\lfloor \frac{t}{2} \rfloor$ non-equivalent additive non-$\mathbb{Z}_4$-linear Hadamard codes (see Corollary 4.3).

Now, like in the $\mathbb{Z}_4$-linear case, we are interested in computing the rank and the dimension of the kernel for all non-equivalent additive non-$\mathbb{Z}_4$-linear Hadamard codes.

Lemma 4.1: Let C be an additive non-$\mathbb{Z}_4$-linear Hadamard code, then the only vectors in the kernel of C are those of order two.

Proof: The proof follows that of Lemma 3.2, but avoids the vector $\Phi(\mathbf{1})$ which is not in the code. ■

Proposition 4.2: For all $\delta \in \{2, \cdots, \lfloor \frac{t}{2} \rfloor\}$, the corresponding additive dual code of the extended 1-perfect additive non-$\mathbb{Z}_4$-linear code of length 2^t, that is, the additive non-$\mathbb{Z}_4$-linear Hadamard code H has $rank(H) = t + 1 + \binom{\delta}{2}$ and $ker(H) = t + 1 - \delta$. For $\delta = 0, 1$, the Hadamard code is a binary linear code and has $ker(H) = rank(H) = t + 1$.

Proof: For the rank, the argument is similar to Proposition 3.1, except for the considerations about vector $\Phi(\mathbf{1})$ which is not in the code. So, finally the rank is $\gamma + 2\delta + \binom{\delta}{2} = t + 1 + \binom{\delta}{2}$. Note that for $\delta = 0, 1$ the general computation, like in Proposition 3.1, can not be considered and the rank is only $\gamma + 2\delta = t + 1$.

For the kernel, the argument is similar to Proposition 3.3, but using Lemma 4.1 instead of Lemma 3.2. ■

Using the fact that different rank (or different dimension for the kernel) means the codes are non-equivalent, we can conclude that there are $\lfloor \frac{t}{2} \rfloor$ non-equivalent Hadamard codes as can be summarized in the following proposition.

Corollary 4.3: For each possible value δ, there exists

a unique additive dual code H of the extended 1-perfect additive non-$\mathbb{Z}_4$-linear code and all these codes H are pairwise non-equivalent, except for $\delta = 0$ and $\delta = 1$, where the codes H coincides with the binary dual of the extended Hamming code.

ACKNOWLEDGMENT

The authors want to thank the anonymous referees for their work in reviewing this manuscript. Their comments have enabled us to improve the presentation of this paper.

REFERENCES

[1] H. Bauer, B. Ganter, F. Hergert, *Algebraic techniques for nonlinear codes*, Combinatorica, Vol. 3 (1983) pp. 21-33.

[2] J. Borges and J. Rifà, *A Characterization of* 1*-Perfect Additive Codes*, IEEE Transactions on Information Theory, Vol. 45, No. 5 (1999) pp. 1688-1697.

[3] J. Borges, K. T. Phelps and J. Rifà, *The rank and kernel of extended 1-perfect $\mathbb{Z}_4$-linear codes and additive non-$\mathbb{Z}_4$-linear codes*, IEEE Transactions on Information Theory, Vol. 49, No. 8 (2003) pp. 2028-2034.

[4] A.E. Brouwer, A.M. Cohen and A. Neumaier, *Distance Regular Graphs*. Springer-Verlag, 1989.

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

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

[7] K. T. Phelps, J. Rifà and M. Villanueva, *Rank and Kernel of additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes*, Proceedings of ACCT'04 conference. Kranevo, Bulgary, June 2004.

[8] K.T. Phelps, J.Rifà, "On binary 1-perfect additive codes: some structural properties," *IEEE Trans. Information Theory*, vol. 48, pp. 2587-2592, 2002.

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

[10] J. Rifà, "Well-ordered Steiner triple systems and 1-perfect partitions of the n-cube," *SIAM Discrete Mathematics*, Vol. 12 no 1 (1999), pp35-47.

[11] J. Rifà, J. M. Basart and L. Huguet, *On completely regular propelinear codes*, in Proc. 6th International Conference, AAECC-6, in LNCS, Springer-Verlag, no. 357 (1989) pp. 341-355.

[12] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The Z4-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Transactions on Information Theory, Vol. 40, No. 2, pp. 301-319, 1994.

Kevin T. Phelps was born in New York, New York (U.S.A.) in May 1948. He received his Bachelor's degree in Mathematics from Brown University in 1970 and his PhD degree in Mathematics from Auburn University in 1976. In 1976, he joined the faculty of Georgia Institute of Technology, School of Mathematics as an Assistant Professor, and was promoted to Associate Professor in 1983. In 1987, he joined the faculty at Auburn University, Division of Mathematics as a Professor. He became Head of the Department of Discrete and Statistical Sciences at Auburn University in 1992 and remains in that position. He has been a Visiting Professor at University of Waterloo, Canada, at the University of Bielefeld, Germany and at the Centre de Recerca Matemàtica, Universitat Autònoma de Barcelona, Spain. His research interests include Coding Theory, Combinatorial Designs and Set Systems, and cryptography as well as associated algorithmic and computational problems.

Josep Rifà was born in Manlleu, Catalonia (Spain) in July 1951. He received the graduate degree in Science (Mathematical Section) in 1973, from the University of Barcelona and the Ph.D. degree in Science (Computer Sciences Section) in 1987, from the Autonomous University of Barcelona. Since 1974 he was an Assistant Professor in the Mathematics Department, Barcelona University. In 1987 he joined the Autonomous University of Barcelona and since 1992 he is a full professor and, at present, the Head of Information and Communications Engineering Department. He currently serves as a Vice-chairman of the Spanish Chapter of Information Theory of IEEE. He has worked in several projects of Spanish CICYT and other organizations on subjects related to digital communications, error correcting codes and encryption of digital information. His research interests include information theory, coding theory and cryptography.

Mercè Villanueva was born in Roses, Catalonia (Spain) in January 1972. She received her Bachelor's degree in Mathematics in 1994 from the Autonomous University of Barcelona and her Ph.D. degree in Science (Computer Science Section) in 2001 from the same university. In 1994, she joined the Department of Information and Communications Engineering, at the Autonomous University of Barcelona, as an Assistant Professor, and was promoted to Associate Professor in 2002. Her research interests include subjects related to combinatorics, algebra, coding theory and graph theory.