Fernández-Córdoba, Cristina; Vela, Carlos; Villanueva, Mercè. «Equivalences among Z2s -linear Hadamard codes». Discrete Mathematics, Vol. 343, issue 3 (March 2020), art. 111721. DOI 10.1016/j.disc.2019.111721

Equivalences among $\mathbb{Z}_{2^s}$-linear Hadamard codes

Cristina Fernández-Córdoba, Carlos Vela, Mercè Villanueva

Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193 Cerdanyola del Vallès, Spain.

Abstract

The $\mathbb{Z}_{2^s}$-additive codes are subgroups of $\mathbb{Z}_{2^s}^n$, and can be seen as a generalization of linear codes over $\mathbb{Z}_2$ and $\mathbb{Z}_4$. A $\mathbb{Z}_{2^s}$-linear Hadamard code is a binary Hadamard code which is the Gray map image of a $\mathbb{Z}_{2^s}$-additive code. A partial classification of these codes by using the dimension of the kernel is known. In this paper, we establish that some $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t are equivalent, once t is fixed. This allows us to improve the known upper bounds for the number of such nonequivalent codes. Moreover, up to $t = 11$, this new upper bound coincides with a known lower bound (based on the rank and dimension of the kernel). Finally, when we focus on $s \in \{2, 3\}$, the full classification of the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t is established by giving the exact number of such codes.

Keywords: Rank, Kernel, Hadamard code, $\mathbb{Z}_{2^s}$-additive code, Gray map, classification
2000 MSC: 94B25, 94B60

1. Introduction

Let $\mathbb{Z}_{2^s}$ be the ring of integers modulo 2^s with $s \geq 1$. The set of n-tuples over $\mathbb{Z}_{2^s}$ is denoted by $\mathbb{Z}_{2^s}^n$. A binary code of length n is a nonempty subset of $\mathbb{Z}_2^n$, and it is linear if it is a subspace of $\mathbb{Z}_2^n$. A nonempty subset of $\mathbb{Z}_{2^s}^n$ is a $\mathbb{Z}_{2^s}$-additive code if it is a subgroup of $\mathbb{Z}_{2^s}^n$. Note that, when $s = 1$, a $\mathbb{Z}_{2^s}$-additive code is a binary linear code and, when $s = 2$, it is a quaternary linear code or a linear code over $\mathbb{Z}_4$.

The Hamming weight of a binary vector $\mathbf{u} \in \mathbb{Z}_2^n$, denoted by $\mathrm{wt}_H(\mathbf{u})$, is the number of nonzero coordinates of $\mathbf{u}$. The Hamming distance of two binary vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^n$, denoted by $d_H(\mathbf{u}, \mathbf{v})$, is the number of coordinates in which they differ. Note that $d_H(\mathbf{u}, \mathbf{v}) = \mathrm{wt}_H(\mathbf{v} - \mathbf{u})$. The minimum distance of a binary code C is $d(C)=\min\{d_H(\mathbf{u},\mathbf{v}) : \mathbf{u},\mathbf{v}\in C, \mathbf{u}\neq\mathbf{v}\}$. The Lee weight of an element $i\in\mathbb{Z}_{2^s}$ is $\mathrm{wt}_L(i)=\min\{i,2^s-i\}$ and the Lee weight of a vector $\mathbf{u}=(u_1,u_2,\dots,u_n)\in\mathbb{Z}_{2^s}^n$ is $\mathrm{wt}_L(\mathbf{u})=\sum_{j=1}^n \mathrm{wt}_L(u_j)\in\mathbb{Z}_{2^s}$. The Lee distance of two vectors $\mathbf{u},\mathbf{v}\in\mathbb{Z}_{2^s}^n$ is $d_L(\mathbf{u},\mathbf{v})=\mathrm{wt}_L(\mathbf{v}-\mathbf{u})$. The minimum distance of a $\mathbb{Z}_{2^s}$-additive code $\mathcal{C}$ is $d(\mathcal{C})=\min\{d_L(\mathbf{u},\mathbf{v}) : \mathbf{u},\mathbf{v}\in\mathcal{C}, \mathbf{u}\neq\mathbf{v}\}$.

In [12], a Gray map from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ is defined as $\phi(0)=(0,0)$, $\phi(1)=(0,1)$, $\phi(2)=(1,1)$ and $\phi(3)=(1,0)$. There exist different generalizations of this Gray map, which go from $\mathbb{Z}_{2^s}$ to $\mathbb{Z}_2^{2^{s-1}}$ [5, 6, 13]. The one given in [5], by Carlet, is the map $\phi_s:\mathbb{Z}_{2^s}\to\mathbb{Z}_2^{2^{s-1}}$ defined as follows:

$$\phi_s(u)=(u_{s-1},\dots,u_{s-1})+(u_0,\dots,u_{s-2})Y_{s-1}, \tag{1}$$

where $u\in\mathbb{Z}_{2^s}$, $[u_0,u_1,\dots,u_{s-1}]_2$ is the binary expansion of u, that is $u=\sum_{i=0}^{s-1}2^iu_i$ ($u_i\in\{0,1\}$), and Y_{s-1} is a matrix of size $(s-1)\times 2^{s-1}$ which columns are the elements of $\mathbb{Z}_2^{s-1}$. Note that the rows of Y_{s-1} form a basis of a first order Reed-Muller code after adding the all-one row. The generalized Gray map from $\mathbb{Z}_{2^s}$ to $\mathbb{Z}_2^{2^{s-1}}$ given in [13], by Krotov, is defined in a more general way in terms of the codewords of a Hadamard code. In this paper, we will focus on Carlet's Gray map ϕ_s, which is a particular case of the Krotov's one satisfying that $\sum\lambda_i\phi_s(2^i)=\phi_s(\sum\lambda_i 2^i)$. Then, we define $\Phi_s:\mathbb{Z}_{2^s}^n\to\mathbb{Z}_2^{n2^{s-1}}$ as the component-wise Gray map ϕ_s.

Let $\mathcal{C}$ be a $\mathbb{Z}_{2^s}$-additive code of length n. We say that its binary image $C=\Phi_s(\mathcal{C})$ is a $\mathbb{Z}_{2^s}$-linear code of length $2^{s-1}n$. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_{2^s}^n$, it is isomorphic to an abelian structure $\mathbb{Z}_{2^s}^{t_1}\times\mathbb{Z}_{2^{s-1}}^{t_2}\times\cdots\times\mathbb{Z}_4^{t_{s-1}}\times\mathbb{Z}_2^{t_s}$, and we say that $\mathcal{C}$, or equivalently $C=\Phi_s(\mathcal{C})$, is of type $(n;t_1,\dots,t_s)$. Note that $|\mathcal{C}|=2^{st_1}2^{(s-1)t_2}\cdots 2^{t_s}$. If $\mathcal{C}$ is a $\mathbb{Z}_{2^s}$-additive code of type $(n;t_1,\dots,t_s)$, then a generator matrix of $\mathcal{C}$ with minimum number of rows has exactly $t_1+\cdots+t_s$ rows. A 2-linear combination of the elements of $\mathcal{B}=\{\mathbf{b}_1,\dots,\mathbf{b}_r\}\subseteq\mathbb{Z}_{2^s}^n$ is $\sum_{i=1}^r\lambda_i\mathbf{b}_i$, for $\lambda_i\in\mathbb{Z}_2$. We say that $\mathcal{B}$ is a 2-basis of $\mathcal{C}$ if the elements in $\mathcal{B}$ are 2-linearly independent and any $\mathbf{c}\in\mathcal{C}$ is a 2-linear combination of the elements of $\mathcal{B}$.

Let $\mathcal{S}_n$ be the symmetric group of permutations on the set $\{1,\dots,n\}$. Two binary codes, C_1 and C_2, are said to be equivalent if there is a vector $\mathbf{a}\in\mathbb{Z}_2^n$ and a permutation of coordinates $\pi\in\mathcal{S}_n$ such that $C_2=\{\mathbf{a}+\pi(\mathbf{c}) : \mathbf{c}\in C_1\}$. Two $\mathbb{Z}_{2^s}$-additive codes, $\mathcal{C}_1$ and $\mathcal{C}_2$, are said to be permutation equivalent if they differ only by a permutation of coordinates, that is, if there is a permutation of coordinates $\pi\in\mathcal{S}_n$ such that $\mathcal{C}_2=\{\pi(\mathbf{c}) : \mathbf{c}\in\mathcal{C}_1\}$. A binary code C is transitive if for each $\mathbf{x}\in C$ there exists a permutation $\pi_{\mathbf{x}}\in\mathcal{S}_n$

such that $\mathbf{x} + \pi_{\mathbf{x}}(C) = C$. A binary code C is propelinear if it is transitive and it satisfies that if $\mathbf{x} + \pi_{\mathbf{x}}(\mathbf{y}) = \mathbf{z}$, then $\pi_{\mathbf{z}} = \pi_{\mathbf{x}}\pi_{\mathbf{y}}$. In [19], it is shown that $\mathbb{Z}_4$-linear codes are in fact propelinear codes.

Two structural properties of binary codes are the rank and the dimension of the kernel. The rank of a binary code C is simply the dimension of the linear span, $\langle C\rangle$, of C. The kernel of a binary code C is defined as $\mathrm{K}(C) = \{\mathbf{x} \in \mathbb{Z}_2^n : \mathbf{x} + C = C\}$ [2]. If the all-zero vector belongs to C, then $\mathrm{K}(C)$ is a linear subcode of C. Note also that if C is linear, then $K(C) = C = \langle C\rangle$. We denote the rank of a binary code C as $\mathrm{rank}(C)$ and the dimension of the kernel as $\ker(C)$. These invariants can be used to distinguish between nonequivalent binary codes, since equivalent ones have the same rank and dimension of the kernel.

A binary code of length n, $2n$ codewords and minimum distance $n/2$ is called a Hadamard code. Hadamard codes can be constructed from Hadamard matrices [1, 16]. Note that linear Hadamard codes are in fact first order Reed-Muller codes, or equivalently, the dual of extended Hamming codes [16, Ch.13 §3]. The $\mathbb{Z}_{2^s}$-additive codes that, under the Gray map Φ_s, give a Hadamard code are called $\mathbb{Z}_{2^s}$-additive Hadamard codes and the corresponding binary images are called $\mathbb{Z}_{2^s}$-linear Hadamard codes. Note that $\mathbb{Z}_{2^s}$-additive Hadamard codes are the only regular proper $\mathbb{Z}_{2^s}$-additive two-weight homogeneous codes with dual Krotov distance at least 4 [21]. The homogeneous weight of an element $i \in \mathbb{Z}_{2^s}$, denoted by $\mathrm{wt}(i)$, is such that $\mathrm{wt}(0) = 0$, $\mathrm{wt}(2^{s-1}) = 2^{s-1}$ and $\mathrm{wt}(i) = 2^{s-1}$ for all $i \in \mathbb{Z}_{2^s}\backslash\{0, 2^{s-1}\}$.

The $\mathbb{Z}_4$-linear Hadamard codes of length 2^t can be classified by using either the rank or the dimension of the kernel [14, 18]. For $s > 2$, the dimension of the kernel for $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t is established in [7], and it is proved that this invariant only provides a complete classification for certain values of t and s. Lower and upper bounds are also established for the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, when both t and s are fixed, and when just t is fixed; denoted by $\mathcal{A}_{t,s}$ and $\mathcal{A}_t$, respectively. The rank of these codes is computed in [8] only for $s = 3$, and it is proved that in this case the rank is not enough to obtain a complete classification. However, it is also shown that, for $s = 3$, by using both invariants, the rank and dimension of the kernel, it is possible to provide a full classification for any $t \geq 3$. Moreover, the exact value of $\mathcal{A}_{t,3}$ is given. From [7] and [8], we can check that there are nonlinear codes having the same rank and dimension of the kernel for different values of s, once the length 2^t is fixed, for all $5 \leq t \leq 11$.

In this paper, we show that there are Hadamard codes that can be seen as $\mathbb{Z}_{2^s}$-linear codes for different values of s, up to permutations. Moreover, for $t \leq 11$, we see that the codes that are permutation equivalent are, in fact, those having the same pair of invariants, rank and dimension of the kernel. These equivalence results allow us to obtain a more accurate classification of the $\mathbb{Z}_{2^s}$-linear Hadamard codes, than the one given in [7]. The paper is organised as follows. In Section 2, we recall the recursive construction of the $\mathbb{Z}_{2^s}$-linear Hadamard codes, the known partial classification, and some bounds on the number of nonequivalent such codes, presented in [7]. In Section 3, we prove some equivalence relations among the $\mathbb{Z}_{2^s}$-linear Hadamard codes of the same length 2^t. Moreover, we prove that some $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s > 2$ are also propelinear. Later, in Section 4, we improve the classification given in [7] by refining the known bounds. Then, in Section 5, we show that the rank, together with the dimension of the kernel, provide a full classification for the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t with $s \in \{2, 3\}$. In addition, in this case, we obtain the exact number of nonequivalent such codes. Finally, in Section 6, we give some conclusions and further research on this topic.

2. Partial classification

The description of a generator matrix having minimum number of rows for a $\mathbb{Z}_4$-additive Hadamard code, as long as a recursive construction of these matrices, are given in [14]. In [13], the $\mathbb{Z}_{2^s}$-additive Hadamard codes with $s > 2$ are introduced and generator matrices with minimum number of rows are given for these codes. In this section, we provide some results presented in [7] and related to their recursive construction, partial classification and bounds on the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t.

Let $T_i = \{j \cdot 2^{i-1} \, : \, j \in \{0, 1, \dots, 2^{s-i+1} - 1\}\}$ for all $i \in \{1, \dots, s\}$. Note that $T_1 = \{0, \dots, 2^s - 1\}$. Let t_1, t_2,…,t_s be nonnegative integers with $t_1 \geq 1$. Consider the matrix $A^{t_1,\dots,t_s}$ whose columns are of the form $\mathbf{z}^T$, $\mathbf{z} \in \{1\} \times T_1^{t_1-1} \times T_2^{t_2} \times \cdots \times T_s^{t_s}$. Let $\mathbf{0}, \mathbf{1}, \mathbf{2}, \dots, \mathbf{2^s - 1}$ be the vectors having the same element $0, 1, 2, \dots, 2^s - 1$ from $\mathbb{Z}_{2^s}$ in all its coordinates, respectively. The order of a vector $\mathbf{u}$ over $\mathbb{Z}_{2^s}$, denoted by $\mathrm{ord}(\mathbf{u})$, is the smallest positive integer m such that $m\mathbf{u} = \mathbf{0}$.

Any matrix $A^{t_1,\dots,t_s}$ can be obtained by applying the following recursive construction. We start with $A^{1,0,\dots,0} = (1)$. Then, if we have a matrix

$A = A^{t_1,\dots,t_s}$, for any $i \in \{1,\dots,s\}$, we may construct the matrix

$$A_i = \begin{pmatrix} A & A & \cdots & A \\ 0\cdot \mathbf{2^{i-1}} & 1\cdot \mathbf{2^{i-1}} & \cdots & (2^{s-i+1}-1)\cdot \mathbf{2^{i-1}} \end{pmatrix}. \qquad (2)$$

Finally, permuting the rows of A_i, we obtain a matrix $A^{t'_1,\dots,t'_s}$, where $t'_j = t_j$ for $j \neq i$ and $t'_i = t_i + 1$. Note that any permutation of columns of A_i gives also a matrix $A^{t'_1,\dots,t'_s}$. Along this paper, we consider that the matrices $A^{t_1,\dots,t_s}$ are constructed recursively starting from $A^{1,0,\dots,0}$ in the following way. First, we add $t_1 - 1$ rows of order 2^s, up to obtain $A^{t_1,0,\dots,0}$; then t_2 rows of order 2^{s-1} up to generate $A^{t_1,0,\dots,0}$; and so on, until we add t_s rows of order 2 to achieve $A^{t_1,\dots,t_s}$. See [7] for examples.

Let $\mathcal{H}^{t_1,\dots,t_s}$ be the $\mathbb{Z}_{2^s}$-additive code generated by the matrix $A^{t_1,\dots,t_s}$, where $t_1,\dots,t_s$ are nonnegative integers with $t_1 \geq 1$. Let $n = 2^{t-s+1}$, where $t = (\sum_{i=1}^{s}(s-i+1)\cdot t_i) - 1$. The code $\mathcal{H}^{t_1,\dots,t_s}$ has length n, and the corresponding $\mathbb{Z}_{2^s}$-linear code $H^{t_1,\dots,t_s} = \Phi(\mathcal{H}^{t_1,\dots,t_s})$ is a binary Hadamard code of length 2^t [7, 13]. In [7], it is shown that, in order to classify the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, we can focus on $t \geq 5$ and $2 \leq s \leq t-2$, since in the rest of the cases there is exactly one code, which is linear. Moreover, for any $t \geq 5$ and $2 \leq s \leq t-2$, there are exactly two $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, $H^{1,0,\dots,0,t+1-s}$ and $H^{1,0,\dots,0,1,t-1-s}$, which are linear.

Tables 1 and 3, for $5 \leq t \leq 11$ and $2 \leq s \leq t-2$, show all possible values $(t_1,\dots,t_s)$ for which there exists a nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard code $H^{t_1,\dots,t_s}$ of length 2^t. For each one of them, the values (r,k) are shown, where r is the rank (computed by using the computer algebra system Magma [4, 20]) and k is the dimension of the kernel ([7, 14]). The rank for $s = 2$ and $s = 3$ can also be computed by using the results given in [18] and [8], respectively. Note that if two codes have different values (r,k), then they are not equivalent. Therefore, from the values of the dimension of the kernel given in these tables, it is easy to see that this invariant does not classify. From [8], we have that, considering only the rank, it is not possible to fully classify these codes either.

Let $X_{t,s}$ be the number of nonnegative integer solutions $(t_1,\dots,t_s) \in \mathbb{N}^s$ of the equation $t = (\sum_{i=1}^{s}(s-i+1)\cdot t_i) - 1$ with $t_1 \geq 1$. Let $\mathcal{A}_{t,s}$ be the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t and a fixed $s \geq 2$. Then, for any $t \geq 5$ and $2 \leq s \leq t-2$, we have that $\mathcal{A}_{t,s} \leq X_{t,s} - 1$, since there are exactly two codes which are linear. Moreover, when $t \leq 11$, this bound is tight. It is still an open problem to know whether this bound is tight for $t \geq 12$.

	$t=5$		$t=6$		$t=7$		$t=8$	
	$(t_1,\dots,t_s)$	(r,k)	$(t_1,\dots,t_s)$	(r,k)	$(t_1,\dots,t_s)$	(r,k)	$(t_1,\dots,t_s)$	(r,k)
$\mathbb{Z}_4$	$(3,0)$	(7,4)	$(3,1)$	(8,5)	$(3,2)$	(9,6)	$(3,3)$	(10,7)
					$(4,0)$	(11,5)	$(4,1)$	(12,6)
$\mathbb{Z}_8$	$(2,0,0)$	(8,3)	$(1,2,0)$	(8,5)	$(1,2,1)$	(9,6)	$(1,2,2)$	(10,7)
			$(2,0,1)$	(9,4)	$(2,0,2)$	(10,5)	$(1,3,0)$	(12,6)
					$(2,1,0)$	(12,4)	$(2,0,3)$	(11,6)
							$(2,1,1)$	(13,5)
							$(3,0,0)$	(17,4)
$\mathbb{Z}_{16}$			$(1,1,0,0)$	(9,4)	$(1,0,2,0)$	(9,6)	$(1,0,2,1)$	(10,7)
					$(1,1,0,1)$	(10,5)	$(1,1,0,2)$	(11,6)
					$(2,0,0,0)$	(14,3)	$(1,1,1,0)$	(13,5)
							$(2,0,0,1)$	(15,4)
$\mathbb{Z}_{32}$					$(1,0,1,0,0)$	(10,5)	$(1,0,0,2,0)$	(10,7)
							$(1,0,1,0,1)$	(11,6)
							$(1,1,0,0,0)$	(15,4)
$\mathbb{Z}_{64}$							$(1,0,0,1,0,0)$	(11,6)

Table 1: Type, rank and dimension of the kernel for all nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t for $5 \le t \le 8$.

In [7], a partial classification for the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t is given. Specifically, lower and upper bounds on the number of nonequivalent such codes, once only t is fixed, are established. The exact number of nonequivalent codes of length 2^t, for $3 \le t \le 7$, which coincides with the lower bound, is also established in [7]. These values are highlighted in bold type in Table 2.

Theorem 2.1. *[7] Let $\mathcal{A}_t$ be the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t with $t \ge 3$. Then,*

$$\mathcal{A}_t \le 1 + \sum_{s=2}^{t-2} (X_{t,s} - 2) \tag{3}$$

and

$$\mathcal{A}_t \le 1 + \sum_{s=2}^{t-2} (\mathcal{A}_{t,s} - 1). \tag{4}$$

t	3	4	5	6	7	8	9	10	11
lower bound (r, k)	**1**	**1**	**3**	**3**	**6**	7	11	13	20
upper bound (3) and (4)	1	1	3	5	10	16	26	38	57

Table 2: Bounds for the number $\mathcal{A}_t$ of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t for $3 \leq t \leq 11$.

In this paper, in order to improve this partial classification, we analyse the equivalence relations among the $\mathbb{Z}_{2^s}$-linear Hadamard codes with the same length 2^t and different values of s. We prove that some of them are indeed permutation equivalent. For $5 \leq t \leq 11$, the ones that are permutation equivalent coincide with the ones that have the same invariants, rank and dimension of the kernel, that is, the same pair (r, k) in Tables 1 and 3. Finally, by using this equivalence relations, we improve the upper bounds on the number $\mathcal{A}_t$ of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t given by Theorem 2.1. This allow us to determine the exact value of $\mathcal{A}_t$ for $8 \leq t \leq 11$, since one of the new upper bounds coincides with the lower bound (r, k) for these cases.

	$t=9$		$t=10$		$t=11$	
	$(t_1,\dots,t_s)$	(r,k)	$(t_1,\dots,t_s)$	(r,k)	$(t_1,\dots,t_s)$	(r,k)
$\mathbb{Z}_4$	$(3,4)$	(11,8)	$(3,5)$	(12,9)	$(3,6)$	(13,10)
	$(4,2)$	(13,7)	$(4,3)$	(14,8)	$(4,4)$	(15,9)
	$(5,0)$	(16,6)	$(5,1)$	(17,7)	$(5,2)$	(18,8)
					$(6,0)$	(22,7)
$\mathbb{Z}_8$	$(1,2,3)$	(11,8)	$(1,2,4)$	(12,9)	$(1,2,5)$	(13,10)
	$(1,3,1)$	(13,7)	$(1,3,2)$	(14,8)	$(1,3,3)$	(15,9)
	$(2,0,4)$	(12,7)	$(1,4,0)$	(17,7)	$(1,4,1)$	(18,8)
	$(2,1,2)$	(14,6)	$(2,0,5)$	(13,8)	$(2,0,6)$	(14,9)
	$(2,2,0)$	(17,5)	$(2,1,3)$	(15,7)	$(2,1,4)$	(16,8)
	$(3,0,1)$	(18,5)	$(2,2,1)$	(18,6)	$(2,2,2)$	(19,7)
			$(3,0,2)$	(19,6)	$(2,3,0)$	(23,6)
			$(3,1,0)$	(24,5)	$(3,0,3)$	(20,7)
					$(3,1,1)$	(25,6)
					$(4,0,0)$	(32,5)
$\mathbb{Z}_{16}$	$(1,0,2,2)$	(11,8)	$(1,0,2,3)$	(12,9)	$(1,0,2,4)$	(13,10)
	$(1,0,3,0)$	(13,7)	$(1,0,3,1)$	(14,8)	$(1,0,3,2)$	(15,9)
	$(1,2,0,0)$	(18,5)	$(1,1,0,4)$	(13,8)	$(1,0,4,0)$	(18,8)
	$(1,1,0,3)$	(12,7)	$(1,1,1,2)$	(15,7)	$(1,1,0,5)$	(14,9)
	$(1,1,1,1)$	(14,6)	$(1,1,2,0)$	(18,6)	$(1,1,1,3)$	(16,8)
	$(2,0,0,2)$	(16,5)	$(1,2,0,1)$	(19,6)	$(1,1,2,1)$	(19,7)
	$(2,0,1,0)$	(20,4)	$(2,0,0,3)$	(17,6)	$(1,2,0,2)$	(20,7)
			$(2,0,1,1)$	(21,5)	$(1,2,1,0)$	(25,6)
			$(2,1,0,0)$	(28,4)	$(2,0,0,4)$	(18,7)
					$(2,0,1,2)$	(22,6)
					$(2,0,2,0)$	(27,5)
					$(2,1,0,1)$	(29,5)
					$(3,0,0,0)$	(44,4)
$\mathbb{Z}_{32}$	$(1,0,0,2,1)$	(11,8)	$(1,0,0,2,2)$	(12,9)	$(1,0,0,2,3)$	(13,10)
	$(1,0,1,0,2)$	(12,7)	$(1,0,0,3,0)$	(14,8)	$(1,0,0,3,1)$	(15,9)
	$(1,0,1,1,0)$	(14,6)	$(1,0,1,0,3)$	(13,8)	$(1,0,1,0,4)$	(14,9)
	$(1,1,0,0,1)$	(16,5)	$(1,0,1,1,1)$	(15,7)	$(1,0,1,1,2)$	(16,8)
	$(2,0,0,0,0)$	(26,3)	$(1,0,2,0,0)$	(19,6)	$(1,0,1,2,0)$	(19,7)
			$(1,1,0,0,2)$	(17,6)	$(1,0,2,0,1)$	(20,7)
			$(1,1,0,1,0)$	(21,5)	$(1,1,0,0,3)$	(18,7)
			$(2,0,0,0,1)$	(27,4)	$(1,1,0,1,1)$	(22,6)
					$(1,1,1,0,0)$	(29,5)
					$(2,0,0,0,2)$	(28,5)
					$(2,0,0,1,0)$	(36,4)
$\mathbb{Z}_{64}$	$(1,0,0,0,2,0)$	(11,8)	$(1,0,0,0,2,1)$	(12,9)	$(1,0,0,0,2,2)$	(13,10)
	$(1,0,0,1,0,1)$	(12,7)	$(1,0,0,1,0,2)$	(13,8)	$(1,0,0,0,3,0)$	(15,9)
	$(1,0,1,0,0,0)$	(16,5)	$(1,0,0,1,1,0)$	(15,7)	$(1,0,0,1,0,3)$	(14,9)
			$(1,0,1,0,0,1)$	(17,6)	$(1,0,0,1,1,1)$	(16,8)
			$(1,1,0,0,0,0)$	(27,4)	$(1,0,0,2,0,0)$	(20,7)
					$(1,0,1,0,0,2)$	(18,7)
					$(1,0,1,0,1,0)$	(22,6)
					$(1,1,0,0,0,1)$	(28,5)
					$(2,0,0,0,0,0)$	(48,3)
$\mathbb{Z}_{128}$	$(1,0,0,0,1,0,0)$	(12,7)	$(1,0,0,0,0,2,0)$	(12,9)	$(1,0,0,0,0,2,1)$	(13,10)
			$(1,0,0,0,1,0,1)$	(13,8)	$(1,0,0,0,1,0,2)$	(14,9)
			$(1,0,0,1,0,0,0)$	(17,6)	$(1,0,0,0,1,1,0)$	(16,8)
					$(1,0,0,1,0,0,1)$	(18,7)
					$(1,0,1,0,0,0,0)$	(28,5)
$\mathbb{Z}_{256}$			$(1,0,0,0,0,1,0,0)$	(13,8)	$(1,0,0,0,0,0,2,0)$	(13,10)
					$(1,0,0,0,0,1,0,1)$	(14,9)
					$(1,0,0,0,1,0,0,0)$	(18,7)
$\mathbb{Z}_{512}$					$(1,0,0,0,0,0,1,0,0)$	(14,9)

Table 3: Type, rank and dimension of the kernel for all nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t for $9 \le t \le 11$.

3. Equivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes

In this section, we give some properties of the generalized Gray map Φ_s. We also prove that some of the $\mathbb{Z}_{2^s}$-linear Hadamard codes of the same length 2^t, having different values of s are permutation equivalent. Moreover, we see that they coincide with the ones having the same rank and dimension of the kernel for $5 \leq t \leq 11$.

Lemma 3.1. *[7] Let $\lambda_i \in \{0,1\}$, $i \in \{0,\dots,s-2\}$. Then,*

$$\sum_{i=0}^{s-2} \lambda_i \phi_s(2^i) = \phi_s(\sum_{i=0}^{s-2} \lambda_i 2^i).$$

Let $\gamma_s \in \mathcal{S}_{2^{s-1}}$ be the permutation defined as

$$\begin{pmatrix} 1 & 2 & \dots & 2^{s-2} & 2^{s-2}+1 & 2^{s-2}+2 & \dots & 2^{s-1} \\ 1 & 3 & \dots & 2^{s-1}-1 & 2 & 4 & \dots & 2^{s-1} \end{pmatrix}.$$

For example, we have that $\gamma_3 = (2,3) \in \mathcal{S}_4$ and $\gamma_4 = (2,3,5)(4,7,6) \in \mathcal{S}_8$. Then, we can define the map $\tau_s : \mathbb{Z}_{2^s} \rightarrow \mathbb{Z}_{2^{s-1}}^2$ as

$$\tau_s(u) = \Phi_{s-1}^{-1}(\gamma_s^{-1}(\phi_s(u))), \tag{5}$$

where $u \in \mathbb{Z}_{2^s}$.

Example 3.1. *For $s = 3$, we have*

$$\begin{array}{rcccl} \Phi_3(0) & = & (0,0,0,0) & = & \gamma_3(0,0,0,0) = \gamma_3(\Phi_2(0,0)) \\ \Phi_3(1) & = & (0,1,0,1) & = & \gamma_3(0,0,1,1) = \gamma_3(\Phi_2(0,2)) \\ \Phi_3(2) & = & (0,0,1,1) & = & \gamma_3(0,1,0,1) = \gamma_3(\Phi_2(1,1)) \\ \Phi_3(3) & = & (0,1,1,0) & = & \gamma_3(0,1,1,0) = \gamma_3(\Phi_2(1,3)) \\ \Phi_3(4) & = & (1,1,1,1) & = & \gamma_3(1,1,1,1) = \gamma_3(\Phi_2(2,2)) \\ \Phi_3(5) & = & (1,0,1,0) & = & \gamma_3(1,1,0,0) = \gamma_3(\Phi_2(2,0)) \\ \Phi_3(6) & = & (1,1,0,0) & = & \gamma_3(1,0,1,0) = \gamma_3(\Phi_2(3,3)) \\ \Phi_3(7) & = & (1,0,0,1) & = & \gamma_3(1,0,0,1) = \gamma_3(\Phi_2(3,1)). \end{array} \tag{6}$$

These equalities define the map $\tau_3 : \mathbb{Z}_8 \rightarrow \mathbb{Z}_4^2$ as $\tau_3(0) = (0,0)$, $\tau_3(1) = (0,2)$, $\tau_3(2) = (1,1)$, $\tau_3(3) = (1,3)$, $\tau_3(4) = (2,2)$, $\tau_3(5) = (2,0)$, $\tau_3(6) = (3,3)$ and $\tau_3(7) = (3,1)$.

Lemma 3.2. *Let $s \geq 2$. Then,*

(i) $\tau_s(1) = (0, 2^{s-2})$,

(ii) $\tau_s(2^i u) = 2^{i-1}(u, u)$ *for all* $i \in \{1, \dots, s-1\}$ *and* $u \in \{0, 1, \dots, 2^{s-1}-1\}$.

Proof. First, $\tau_s(1) = \Phi_{s-1}^{-1}(\gamma_s^{-1}(\phi_s(1))) = \Phi_{s-1}^{-1}(\gamma_s^{-1}(0,1,0,1,\dots,0,1)) = \Phi_{s-1}^{-1}(\mathbf{0}, \mathbf{1}) = (0, 2^{s-2})$, and (i) holds.

In order to prove (ii), let $u \in \mathbb{Z}_{2^s}$ and $[u_0, \dots, u_{s-1}]_2$ be its binary expansion. The binary expansion of $2^i u$ is $[0, \dots, 0, u_0, \dots, u_{s-i-1}]_2$ and we have that $\phi_s(2^i u) = (u_{s-i-1}, \dots, u_{s-i-1}) + (0, \dots, 0, u_0, \dots, u_{s-i-2})Y_{s-1}$. Recall that the matrix Y_{s-1} given in (1), related to the definition of ϕ_s, is a matrix of size $(s-1) \times 2^{s-1}$ which columns are the elements of $\mathbb{Z}_2^{s-1}$. Without loss of generality, we consider that Y_s is the matrix obtained recursively from $Y_1 = (0\,1)$ and

$$Y_s = \begin{pmatrix} Y_{s-1} & Y_{s-1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}. \tag{7}$$

It is easy to see that

$$\gamma_s^{-1}(Y_{s-1}) = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ Y_{s-2} & Y_{s-2} \end{pmatrix}. \tag{8}$$

Then, we have that

$$\begin{aligned}
&\gamma_s^{-1}(\phi_s(2^i u)) = \\
&\quad = (u_{s-i-1}, \overset{(2^{s-1})}{\dots}, u_{s-i-1}) + (0, \overset{(i)}{\dots}, 0, u_0, \dots, u_{s-i-2}) \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ Y_{s-2} & Y_{s-2} \end{pmatrix} = \\
&\quad = (u_{s-i-1}, \overset{(2^{s-1})}{\dots}, u_{s-i-1}) + (0, \overset{(i-1)}{\dots}, 0, u_0, \dots, u_{s-i-2}) \begin{pmatrix} Y_{s-2} & Y_{s-2} \end{pmatrix} = \\
&\qquad\qquad = (\phi_{s-1}(2^{i-1}u), \phi_{s-1}(2^{i-1}u)) = \Phi_{s-1}(2^{i-1}(u,u)).
\end{aligned}$$

Therefore, $\tau_s(2^i u) = \Phi_{s-1}^{-1}(\gamma_s^{-1}(\phi_s(2^i u))) = 2^{i-1}(u,u)$, and (ii) holds. $\square$

Proposition 3.1. *Let $s \geq 2$ and $\lambda_i \in \{0,1\}$, $i \in \{0, \dots, s-1\}$. Then,*

$$\phi_s(\sum_{i=0}^{s-1} \lambda_i 2^i) = \gamma_s(\Phi_{s-1}(\sum_{i=0}^{s-1} \tau_s(\lambda_i 2^i))). \tag{9}$$

Proof. By Lemma 3.2, we know that for all $i \in \{1,\dots,s-1\}$, $\tau_s(2^i) = (2^{i-1}, 2^{i-1})$ and $\tau_s(1) = (0, 2^{s-2})$. Then, by Lemma 3.1, we have that

$$\gamma_s(\Phi_{s-1}(\sum_{i=0}^{s-1} \tau_s(\lambda_i 2^i))) = \gamma_s(\sum_{i=0}^{s-1} \Phi_{s-1}(\tau_s(\lambda_i 2^i))).$$

Moreover, γ_s commutes with the addition. Therefore, by applying the definition of the map τ_s given in (5), we obtain that

$$\gamma_s(\Phi_{s-1}(\sum_{i=0}^{s-1} \tau_s(\lambda_i 2^i))) = \sum_{i=0}^{s-1} \gamma_s(\Phi_{s-1}(\tau_s(\lambda_i 2^i))) = \sum_{i=0}^{s-1} \phi_s(\lambda_i 2^i),$$

181 which is equal to $\phi_s(\sum_{i=0}^{s-1} \lambda_i 2^i)$ by Lemma 3.1. □

Corollary 3.1. *Let $s \geq 2$ and $\lambda_i \in \{0,1\}$, $i \in \{0,\dots,s-1\}$. Then,*

$$\tau_s(\sum_{i=0}^{s-1} \lambda_i 2^i) = \sum_{i=0}^{s-1} \tau_s(\lambda_i 2^i). \tag{10}$$

Proof. By Proposition 3.1, we have that

$$\phi_s(\sum_{i=0}^{s-1} \lambda_i 2^i) = \gamma_s(\Phi_{s-1}(\sum_{i=0}^{s-1} \tau_s(\lambda_i 2^i))),$$

and, therefore,

$$\Phi_{s-1}^{-1}(\gamma_s^{-1}(\phi_s(\sum_{i=0}^{s-1} \lambda_i 2^i))) = \sum_{i=0}^{s-1} \tau_s(\lambda_i 2^i),$$

182 that is, $\tau_s(\sum_{i=0}^{s-1} \lambda_i 2^i) = \sum_{i=0}^{s-1} \tau_s(\lambda_i 2^i)$. □

Now, we extend the permutation $\gamma_s \in \mathcal{S}_{2^{s-1}}$ to a permutation $\gamma_s \in \mathcal{S}_{2^{s-1}n}$ such that restricted to each set of 2^{s-1} coordinates $\{2^{s-1}i+1, 2^{s-1}i+2, \dots, 2^{s-1}(i+1)\}$, $i \in \{0,\dots,n-1\}$, acts as $\gamma_s \in \mathcal{S}_{2^{s-1}}$. Then, we component-wise extend function τ_s defined in (5) to $\tau_s : \mathbb{Z}_{2^s}^n \rightarrow \mathbb{Z}_{2^{s-1}}^{2n}$ and define $\tilde{\tau}_s = \rho^{-1} \circ \tau_s$, where $\rho \in \mathcal{S}_{2n}$ is defined as

$$\begin{pmatrix} 1 & 2 & \dots & i & \dots & n & n+1 & \dots & n+i & \dots & 2n \\ 1 & 3 & \dots & 2i-1 & \dots & 2n-1 & 2 & \dots & 2i & \dots & 2n \end{pmatrix}.$$

If $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{Z}_{2^s}^n$ and $\tau_s(u_i) = (u_i^1, u_i^2)$ for all $i \in \{1, \ldots, n\}$, then $\tau_s(\mathbf{u}) = (u_1^1, u_1^2, u_2^1, u_2^2, \ldots, u_n^1, u_n^2)$ and $\tilde{\tau}_s(\mathbf{u}) = (u_1^1, \ldots, u_n^1, u_1^2, \ldots, u_n^2)$. Note also that

$$\Phi_s(\mathbf{u}) = \gamma_s(\Phi_{s-1}(\rho(\tilde{\tau}_s(\mathbf{u}))))$$

for all $\mathbf{u} \in \mathbb{Z}_{2^s}^n$, since $\tilde{\tau}_s(\mathbf{u}) = \rho^{-1}(\tau_s(\mathbf{u})) = \rho^{-1}(\Phi_{s-1}^{-1}(\gamma_s^{-1}(\Phi_s(\mathbf{u}))))$.

Let $\mathbf{w}_i^{(s)}$ be the ith row of $A^{t_1,\ldots,t_s}$, $1 \leq i \leq t_1 + \cdots + t_s$. By construction, $\mathbf{w}_1^{(s)} = \mathbf{1}$ and $\mathrm{ord}(\mathbf{w}_i^{(s)}) \leq \mathrm{ord}(\mathbf{w}_j^{(s)})$ if $i > j$. Let σ_i be the integer such that $\mathrm{ord}(\mathbf{w}_i^{(s)}) = 2^{\sigma_i}$. Then, $\mathcal{B}^{t_1,\ldots,t_s} = \{2^{p_i}\mathbf{w}_i^{(s)} : 1 \leq i \leq t_1 + \cdots + t_s,\ 0 \leq p_i \leq \sigma_i - 1\}$ is a 2-basis of $\mathcal{H}^{t_1,\ldots,t_s}$.

Example 3.2. *Let $\mathcal{H}^{2,1}$ and $\mathcal{H}^{1,1,0}$ be the $\mathbb{Z}_4$-additive and $\mathbb{Z}_8$-additive Hadamard codes, which are generated by*

$$A^{2,1} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 \end{pmatrix}, \quad \textit{and} \quad A^{1,1,0} = \begin{pmatrix} 1\,1\,1\,1 \\ 0\,2\,4\,6 \end{pmatrix},$$

respectively. The corresponding 2-bases are

$$\begin{aligned} \mathcal{B}^{2,1} &= \{\mathbf{w}_1^{(2)}, 2\mathbf{w}_1^{(2)}, \mathbf{w}_2^{(2)}, 2\mathbf{w}_2^{(2)}, \mathbf{w}_3^{(2)}\} \\ &= \{(1,1,1,1,1,1,1,1), (2,2,2,2,2,2,2,2), (0,1,2,3,0,1,2,3), \\ &\quad\ (0,2,0,2,0,2,0,2), (0,0,0,0,2,2,2,2)\}, \quad \textit{and} \\ \mathcal{B}^{1,1,0} &= \{\mathbf{w}_1^{(3)}, 2\mathbf{w}_1^{(3)}, 4\mathbf{w}_1^{(3)}, \mathbf{w}_2^{(3)}, 2\mathbf{w}_2^{(3)}\} \\ &= \{(1,1,1,1), (2,2,2,2), (4,4,4,4), (0,2,4,6), (0,4,0,4)\}. \end{aligned}$$

Proposition 3.2. *Let $t_s \geq 1$, and $\mathcal{H}^{t_1,\ldots,t_s}$ and $\mathcal{H}^{1,t_1-1,t_2,\ldots,t_{s-1},t_s-1}$ be the $\mathbb{Z}_{2^s}$-additive and $\mathbb{Z}_{2^{s+1}}$-additive Hadamard codes with generator matrices $A^{t_1,\ldots,t_s}$ and $A^{1,t_1-1,t_2,\ldots,t_{s-1},t_s-1}$, respectively. Let $\mathbf{w}_i^{(s)}$ and $\mathbf{w}_i^{(s+1)}$ be the ith row of $A^{t_1,\ldots,t_s}$ and $A^{1,t_1-1,t_2,\ldots,t_{s-1},t_s-1}$, respectively. Then, we have that*

(i) $\tilde{\tau}_{s+1}(2^{p_i}\mathbf{w}_i^{(s+1)}) = 2^{p_i}\mathbf{w}_i^{(s)}$, *for all* $i \in \{2, \ldots, t_1 + \cdots + t_s - 1\}$ *and* $p_i \in \{0, \ldots, \sigma_i - 1\}$, *where* $\mathrm{ord}(\mathbf{w}_i^{(s)}) = 2^{\sigma_i}$;

(ii) $\tilde{\tau}_{s+1}(2^{j+1}\mathbf{w}_1^{(s+1)}) = 2^j\mathbf{w}_1^{(s)}$, *for all* $j \in \{0, \ldots, s-1\}$;

(iii) $\tilde{\tau}_{s+1}(\mathbf{w}_1^{(s+1)}) = \mathbf{w}_{t_1+\cdots+t_s}^{(s)}$.

Proof. Consider $A^{t_1,\dots,t_s}$ with $t_s \geq 1$, and $\mathbf{w}_i^{(s)}$ its ith row for $i \in \{1,\dots,t_1+\cdots+t_s\}$. Then, the matrix over $\mathbb{Z}_{2^{s+1}}$

$$\begin{pmatrix} \mathbf{w}_1^{(s)} \\ 2\mathbf{w}_2^{(s)} \\ \vdots \\ 2\mathbf{w}_{t_1+\cdots+t_s}^{(s)} \end{pmatrix}$$

is, by definition, $A^{1,t_1-1,t_2,\dots,t_{s-1},t_s}$. Moreover, by construction we have that

$$A^{1,t_1-1,t_2,\dots,t_{s-1},t_s} = \begin{pmatrix} A^{1,t_1-1,t_2,\dots,t_{s-1},t_s-1} & A^{1,t_1-1,t_2,\dots,t_{s-1},t_s-1} \\ \mathbf{0} & \mathbf{2^s} \end{pmatrix}.$$

Therefore, if $\mathbf{w}_i^{(s+1)}$ is the ith row of $A^{1,t_1-1,t_2,\dots,t_{s-1},t_s-1}$ for $i \in \{2,\dots,t_1+t_2+\cdots+t_s-1\}$, we have that $(\mathbf{w}_i^{(s+1)},\mathbf{w}_i^{(s+1)}) = 2\mathbf{w}_i^{(s)}$ and $\mathrm{ord}(\mathbf{w}_i^{(s)}) = \mathrm{ord}(\mathbf{w}_i^{(s+1)}) = \sigma_i$. Let $\mathbf{v}_i^{(s+1)}$ be the vector over $\mathbb{Z}_{2^{s+1}}$ such that $\mathbf{w}_i^{(s+1)} = 2\mathbf{v}_i^{(s+1)}$ and $\mathbf{w}_i^{(s)} = (\mathbf{v}_i^{(s+1)},\mathbf{v}_i^{(s+1)})$. Let $(\mathbf{v}_i^{(s+1)})_j$ be the jth coordinate of $\mathbf{v}_i^{(s+1)}$. By the definition of $\tilde{\tau}_{s+1}$ and Lemma 3.2, for $p_i \in \{0,\dots,\sigma_i-1\}$, we have that

$$\begin{aligned} \tilde{\tau}_{s+1}(2^{p_i}\mathbf{w}_i^{(s+1)}) = \rho^{-1}(\tau_{s+1}(2^{p_i}\mathbf{w}_i^{(s+1)})) = \rho^{-1}(\tau_{s+1}(2^{p_i+1}\mathbf{v}_i^{(s+1)})) = \\ = \rho^{-1}(2^{p_i}((\mathbf{v}_i^{(s+1)})_1,(\mathbf{v}_i^{(s+1)})_1,\dots,(\mathbf{v}_i^{(s+1)})_n,(\mathbf{v}_i^{(s+1)})_n)) = \\ = 2^{p_i}(\mathbf{v}_i^{(s+1)},\mathbf{v}_i^{(s+1)}) = 2^{p_i}\mathbf{w}_i^{(s)}, \end{aligned}$$

and (i) holds.

Since $\mathbf{w}_1^{(s)} = (\mathbf{w}_1^{(s+1)},\mathbf{w}_1^{(s+1)}) = \mathbf{1}$ and $\mathbf{w}_{t_1+\cdots+t_s}^{(s)} = (\mathbf{0},\mathbf{2^{s-1}})$, then the equalities in items (ii) and (iii) hold by the definition of $\tilde{\tau}_{s+1}$ and Lemma 3.2. □

Note that, from the previous proposition, we have that $\tilde{\tau}_s$ is a bijection between the 2-bases, $\mathcal{B}^{t_1,\dots,t_s}$ and $\mathcal{B}^{1,t_1-1,\dots,t_{s-1},t_s-1}$.

Example 3.3. *Let $\mathcal{H}^{2,1}$ and $\mathcal{H}^{1,1,0}$ be the same codes considered in Example 3.2. The length of $\mathcal{H}^{1,1,0}$ is $n=4$. Then, the extension of $\gamma_3 = (2,3) \in \mathcal{S}_4$ is $\gamma_3 = (2,3)(6,7)(10,11)(14,15) \in \mathcal{S}_{16}$, and*

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 5 & 7 & 2 & 4 & 6 & 8 \end{pmatrix} \in \mathcal{S}_8. \quad (11)$$

In this case, we have that

$$\begin{aligned}
\Phi_3(1,1,1,1) &= \gamma_3(\Phi_2(0,2,0,2,0,2,0,2)) = \gamma_3(\Phi_2(\rho(0,0,0,0,2,2,2,2)))\\
\Phi_3(2,2,2,2) &= \gamma_3(\Phi_2(1,1,1,1,1,1,1,1)) = \gamma_3(\Phi_2(\rho(1,1,1,1,1,1,1,1)))\\
\Phi_3(4,4,4,4) &= \gamma_3(\Phi_2(2,2,2,2,2,2,2,2)) = \gamma_3(\Phi_2(\rho(2,2,2,2,2,2,2,2)))\\
\Phi_3(0,2,4,6) &= \gamma_3(\Phi_2(0,0,1,1,2,2,3,3)) = \gamma_3(\Phi_2(\rho(0,1,2,3,0,1,2,3)))\\
\Phi_3(0,4,0,4) &= \gamma_3(\Phi_2(0,0,2,2,0,0,2,2)) = \gamma_3(\Phi_2(\rho(0,2,0,2,0,2,0,2))).
\end{aligned}$$

Since $\Phi_3(\mathbf{u}) = \gamma_3(\Phi_2(\rho(\tilde{\tau}_3(\mathbf{u}))))$ *for all* $\mathbf{u} \in \mathbb{Z}_8^4$*, the map* $\tilde{\tau}_3$ *sends the elements of the* 2*-basis* $\mathcal{B}^{1,1,0}$ *into the elements of the* 2*-basis* $\mathcal{B}^{2,1}$*. That is, as it is shown in Proposition 3.2,*

$$\begin{aligned}
\tilde{\tau}_3(\mathbf{w}_1^{(3)}) &= \tilde{\tau}_3(1,1,1,1) = (0,0,0,0,2,2,2,2) = \mathbf{w}_3^{(2)}\\
\tilde{\tau}_3(2\mathbf{w}_1^{(3)}) &= \tilde{\tau}_3(2,2,2,2) = (1,1,1,1,1,1,1,1) = \mathbf{w}_1^{(2)}\\
\tilde{\tau}_3(4\mathbf{w}_1^{(3)}) &= \tilde{\tau}_3(4,4,4,4) = (2,2,2,2,2,2,2,2) = 2\mathbf{w}_1^{(2)}\\
\tilde{\tau}_3(\mathbf{w}_2^{(3)}) &= \tilde{\tau}_3(0,2,4,6) = (0,1,2,3,0,1,2,3) = \mathbf{w}_2^{(2)}\\
\tilde{\tau}_3(2\mathbf{w}_2^{(3)}) &= \tilde{\tau}_3(0,4,0,4) = (0,2,0,2,0,2,0,2) = 2\mathbf{w}_2^{(2)},
\end{aligned} \tag{12}$$

so $\tilde{\tau}_3$ *is a bijection between both* 2*-bases.*

Lemma 3.3. *Let* $\mathcal{H}_s = \mathcal{H}^{t_1,\dots,t_s}$ *be a* $\mathbb{Z}_{2^s}$*-additive code with* $t_s \geq 1$*, and* $\mathcal{H}_{s+1} = \mathcal{H}^{1,t_1-1,t_2,\dots,t_{s-1},t_s-1}$ *be a* $\mathbb{Z}_{2^{s+1}}$*-additive Hadamard code. Then,* $H_s = \Phi_s(\mathcal{H}_s)$ *is permutation equivalent to* $H_{s+1} = \Phi_{s+1}(\mathcal{H}_{s+1})$*.*

Proof. Let t be the integer such that H_s and H_{s+1} are of length 2^t. Let $\mathcal{B}_s = \{\mathbf{v}_1^{(s)}, \dots, \mathbf{v}_{t+1}^{(s)}\}$ and $\mathcal{B}_{s+1} = \{\mathbf{v}_1^{(s+1)}, \dots, \mathbf{v}_{t+1}^{(s+1)}\}$ be the 2-basis of $\mathcal{H}_s$ and $\mathcal{H}_{s+1}$, respectively. By Proposition 3.2, $\tilde{\tau}_{s+1}$ is a bijection between $\mathcal{B}_s$ and $\mathcal{B}_{s+1}$. By the definition of $\tilde{\tau}_{s+1}$ and Corollary 3.1, we have that $\tilde{\tau}_{s+1}$ commutes with the addition, so $\tilde{\tau}_{s+1}(\mathcal{H}_{s+1}) = \mathcal{H}_s$.

Let $\rho_* \in \mathcal{S}_{2^t}$ be a permutation such that $\Phi_s(\rho(\mathbf{u})) = \rho_*(\Phi_s(\mathbf{u}))$ for all $\mathbf{u} \in \mathcal{H}_s$. Since $\mathcal{H}_s = \tilde{\tau}_{s+1}(\mathcal{H}_{s+1}) = \rho^{-1}(\Phi_s^{-1}(\gamma_{s+1}^{-1}(\Phi_{s+1}(\mathcal{H}_{s+1}))))$, we have that $\Phi_s(\mathcal{H}_s) = \rho_*^{-1}(\gamma_{s+1}^{-1}(\Phi_{s+1}(\mathcal{H}_{s+1})))$. Therefore, we obtain $H_s = (\gamma_{s+1} \circ \rho_*)^{-1}(H_{s+1})$, where $\gamma_{s+1} \circ \rho_* \in \mathcal{S}_{2^t}$. □

The following theorem determines which $\mathbb{Z}_{2^{s'}}$-linear Hadamard codes are equivalent to a given $\mathbb{Z}_{2^s}$-linear Hadamard code $H^{t_1,\dots,t_s}$. We denote by $\mathbf{0}^j$ the all-zero vector of length j. Let σ be the integer such that $\mathrm{ord}(\mathbf{w}_2^{(s)}) = 2^{s+1-\sigma}$. Note that $\sigma = 1$ if and only if $t_1 \geq 2$. Moreover, since σ_2 is the integer such that $\mathrm{ord}(\mathbf{w}_2^{(s)}) = 2^{\sigma_2}$, we have that $\sigma = s + 1 - \sigma_2$.

Theorem 3.1. *Let $H^{t_1,\dots,t_s}$ be a $\mathbb{Z}_{2^s}$-linear Hadamard code with $t_s \geq 1$. Then, $H^{t_1,\dots,t_s}$ is equivalent to the $\mathbb{Z}_{2^{s+\ell}}$-linear Hadamard code $H^{1,\mathbf{0}^{\ell-1},t_1-1,t_2,\dots,t_{s-1},t_s-\ell}$, for all $\ell \in \{1,\dots,t_s\}$.*

Proof. Consider $\mathcal{H}_0 = \mathcal{H}^{t_1,\dots,t_s}$ and $\mathcal{H}_\ell = \mathcal{H}^{1,\mathbf{0}^{\ell-1},t_1-1,t_2,\dots,t_{s-1},t_s-\ell}$ for $\ell \in \{1,\dots,t_s\}$. By Lemma 3.3, we have that $H_i = \Phi(\mathcal{H}_i)$ is permutation equivalent to $H_{i+1} = \Phi(\mathcal{H}_{i+1})$ for all $i \in \{0,\dots,\ell-1\}$ and $\ell \in \{1,\dots,t_s\}$. Therefore, we have that H_0 and H_ℓ are permutation equivalent for all $\ell \in \{1,\dots,t_s\}$. $\square$

Let $t_1, t_2, \dots, t_s$ be nonnegative integers with $t_1 \geq 2$. Let $C_H(t_1,\dots,t_s) = [H_1 = H^{t_1,\dots,t_s}, H_2, \dots, H_{t_s+1}]$ be the sequence of all $\mathbb{Z}_{2^{s'}}$-linear Hadamard codes of length 2^t, where $t = \left(\sum_{i=1}^{s'}(s'-i+1)\cdot t_i\right) - 1$, that are permutation equivalent to $H^{t_1,\dots,t_s}$ by Theorem 3.1. We denote by $C_H(t_1,\dots,t_s)[i]$ the ith code H_i in the sequence, for $1 \leq i \leq t_s+1$. We consider that the order of the codes in $C_H(t_1,\dots,t_s)$ is the following:

$$C_H(t_1,\dots,t_s)[i] = \begin{cases} H^{t_1,\dots,t_s}, & \text{if } i = 1, \\ H^{1,\mathbf{0}^{i-2},t_1-1,t_2,\dots,t_{s-1},t_s-i+1}, & \text{otherwise.} \end{cases} \tag{13}$$

We refer to $C_H(t_1,\dots,t_s)$ as the *chain of equivalences* of $H^{t_1,\dots,t_s}$. Note that if $t_s = 0$, then $C_H(t_1,\dots,t_s) = [H^{t_1,\dots,t_s}]$.

Corollary 3.2. *Let $t_1, t_2, \dots, t_s$ be nonnegative integers with $t_1 \geq 2$. Then,*

$$|C_H(t_1,\dots,t_s)| = t_s + 1.$$

Example 3.4. *The chain of equivalences of $H^{3,3}$ is the sequence $C_H(3,3) = [H^{3,3}, H^{1,2,2}, H^{1,0,2,1}, H^{1,0,0,2,0}]$ and contains exactly $t_2+1 = 4$ codes. Note that this sequence contains all the codes of length 2^8 having the pair $(r,k) = (10,7)$ in Table 1. In the same table, we can see that there is only one code of length 2^7 having the pair $(r,k) = (12,4)$, named $H^{2,1,0}$. The chain of equivalences of this code is $C_H(2,1,0) = [H^{2,1,0}]$, which contains just this code, since $t_3 + 1 = 1$.*

Proposition 3.3. *Let $t_1, t_2, \dots, t_s$ be nonnegative integers with $t_1 \geq 2$. Then, the $\mathbb{Z}_{2^{s'}}$-linear Hadamard code $H^{t'_1,\dots,t'_{s'}} = C_H(t_1,\dots,t_s)[i]$, $1 \leq i \leq t_s+1$, satisfies* *(i)* $s' = s + i - 1$,

(ii) $\sigma' = i$,

(iii) $t'_{s'} = t_s - i + 1$,

(iv) $(t'_1, \ldots, t'_{s'}) = \begin{cases} (t_1, \ldots, t_s), & \textit{if } i = 1, \\ (1, \mathbf{0}^{i-2}, t_1 - 1, t_2, \ldots, t_{s-1}, t_s - i + 1), & \textit{otherwise.} \end{cases}$

Proof. Straightforward from Theorem 3.1 and the definition of the chain of equivalences $C_H(t_1, \ldots, t_s)$. □

Note that the value of s' is different for every code $H^{t'_1,\ldots,t'_{s'}}$ belonging to the same chain of equivalences $C_H(t_1, \ldots, t_s)$.

Corollary 3.3. *Let $t_1, t_2, \ldots, t_s$ be nonnegative integers with $t_1 \geq 2$.*

(i) The $\mathbb{Z}_{2^{s'}}$-linear Hadamard code $H^{t'_1,\ldots,t'_{s'}} = C_H(t_1, \ldots, t_s)[1]$ is the only one in $C_H(t_1, \ldots, t_s)$ with $\sigma' = 1$, that is, the only one with $t'_1 \geq 2$.

(ii) The $\mathbb{Z}_{2^{s'}}$-linear Hadamard code $H^{t'_1,\ldots,t'_{s'}} = C_H(t_1, \ldots, t_s)[t_s + 1]$ is the only one in $C_H(t_1, \ldots, t_s)$ with $t'_{s'} = 0$.

Now, given any $\mathbb{Z}_{2^s}$-linear Hadamard code $H^{t_1,\ldots,t_s}$, we determine the chain of equivalences containing this code, as well as its position in the sequence. Therefore, note that indeed we prove that any code $H^{t_1,\ldots,t_s}$ (with $t_1 \geq 1$) belongs to an unique chain of equivalences $C_H(t'_1, \ldots, t'_{s'})$ with $t'_1 \geq 2$.

Proposition 3.4. *Let $t_1, t_2, \ldots, t_s$ be nonnegative integers with $t_1 \geq 1$. The $\mathbb{Z}_{2^s}$-linear Hadamard code $H^{t_1,\ldots,t_s}$ belongs to an unique chain of equivalences. If $t_1 \geq 2$, then $\sigma = 1$ and $H^{t_1,\ldots,t_s} = C_H(t_1, \ldots, t_s)[1]$. Otherwise, if $t_1 = 1$, then $\sigma > 1$ and $H^{t_1,\ldots,t_s} = C_H(t'_1, \ldots, t'_{s'})[\sigma]$, where $(t'_1, \ldots, t'_{s'}) = (t_\sigma + 1, t_{\sigma+1}, \ldots, t_{s-1}, t_s + \sigma - 1)$ and $s' = s - \sigma + 1$.*

Proof. If $t_1 \geq 2$, it is clear by the definition of chain of equivalences and Corollary 3.3. If $t_1 = 1$, then $\sigma > 1$. By Proposition 3.3, since $H^{t_1,\ldots,t_s} = C_H(t'_1, \ldots, t'_{s'})[\sigma]$, we have that $(t_1, \ldots, t_s) = (1, \mathbf{0}^{\sigma-2}, t'_1 - 1, t'_2, \ldots, t'_{s'-1}, t'_{s'} - \sigma + 1)$. Therefore, $t_\sigma = t'_1 - 1$, $t_{\sigma+1} = t'_2$, …, $t_{s-1} = t'_{s'-1}$, $t_s = t'_{s'} - \sigma + 1$, and the result follows. □

Corollary 3.4. *Let $H^{t_1,\dots,t_s}$ be a $\mathbb{Z}_{2^s}$-linear Hadamard code and $C_H(t'_1,\dots,t'_{s'})$ the chain of equivalences such that $H^{t_1,\dots,t_s} = C_H(t'_1,\dots,t'_{s'})[\sigma]$. Then,*

$$|C_H(t'_1,\dots,t'_{s'})| = t_s + \sigma.$$

Proof. If $t_1 \geq 2$, then $H^{t_1,\dots,t_s} = C_H(t_1,\dots,t_s)[1]$ by Proposition 3.4. By Corollary 3.2, $|C_H(t_1,\dots,t_s)| = t_s + 1 = t_s + \sigma$. Otherwise, if $t_1 = 1$, then $H^{t_1,\dots,t_s} = C_H(t_\sigma + 1, t_{\sigma+1},\dots, t_{s-1}, t_s + \sigma - 1)[\sigma]$ by Proposition 3.4. Finally, $|C_H(t_\sigma + 1, t_{\sigma+1},\dots, t_{s-1}, t_s + \sigma - 1)| = t_s + \sigma - 1 + 1 = t_s + \sigma$ by Corollary 3.2. □

Example 3.5. *The $\mathbb{Z}_{2^4}$-linear Hadamard code $H^{1,0,2,1}$ has $t_1 = 1$, $\sigma = 3$ and $s = 4$. By Proposition 3.4, since $\sigma = 3$ and $s' = s - \sigma + 1 = 2$, this code is placed in the third position of the chain of equivalences $C_H(t'_1, t'_2)$, where $t'_1 = t_3 + 1 = 2 + 1 = 3$ and $t'_2 = t_4 + \sigma - 1 = 1 + 3 - 1 = 3$. Therefore, $H^{1,0,2,1} = C_H(3,3)[3]$. By Corollary 3.4, $C_H(3,3)$ contains exactly $t_4 + \sigma = 1 + 3 = 4$ codes, which are the ones described in Example 3.4.*

If $H^{t_1,\dots,t_s}$ is a $\mathbb{Z}_{2^s}$-linear Hadamard code of length 2^t with $t_1 \geq 2$ and $t_s = 0$, then $|C_H(t_1,\dots,t_s)| = 1$ by Corollary 3.4. In this case, from Tables 1 and 3, we can see that $H^{t_1,\dots,t_s}$ is not equivalent to any other code $H^{t'_1,\dots,t'_{s'}}$ of the same length 2^t, for $t \leq 11$. We conjecture that this is true for any $t \geq 12$. The values of $(t_1,\dots,t_s)$ for which the codes $H^{t_1,\dots,t_s}$ are not equivalent to any other such code of the same length 2^t, for $t \leq 11$, can be found in Table 4.

$t = 5$	(3,0), (2,0,0)
$t = 7$	(4,0), (2,1,0), (2,0,0,0)
$t = 8$	(3,0,0)
$t = 9$	(5,0), (2,2,0), (2,0,1,0), (2,0,0,0,0)
$t = 10$	(3,1,0), (2,1,0,0)
$t = 11$	(6,0), (2,3,0), (4,0,0), (2,0,2,0), (3,0,0,0), (2,0,0,1,0), (2,0,0,0,0,0)

Table 4: Type of all $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t with $\sigma = 1$ and $t_s = 0$ for $t \leq 11$.

From Tables 1 and 3, we can also see that the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t with $t \leq 11$ having the same values (r,k) are the ones which are equivalent by Theorem 3.1. We conjecture that this is true for any $t \geq 12$.

Recall that all $\mathbb{Z}_4$-linear codes are propelinear, so also transitive [19]. Now, as a corollary of Proposition 3.4, we show under which conditions a $\mathbb{Z}_{2^s}$-linear Hadamard code with $s > 2$ is propelinear because it is permutation equivalent to a $\mathbb{Z}_4$-linear code. First, we give the following lemma that is easily proven.

Lemma 3.4. *Let C_1 and C_2 be permutation equivalent binary codes. If C_1 is propelinear, then so it is C_2.*

Corollary 3.5. *Let $t_1, t_2, \ldots, t_s$ be nonnegative integers with $t_1 \geq 1$ and $s \geq 2$. Then, $H^{t_1,\ldots,t_s}$ is propelinear if either $s = 2$ or $s > 2$, $t_1 = 1$ and $\sigma = s - 1$.*

Proof. By [19], we have that all $\mathbb{Z}_4$-linear codes are propelinear. Therefore, $H^{t_1,\ldots,t_s}$ is propelinear if $s = 2$.

Assume $s > 2$, $\sigma = s - 1$ and $t_1 = 1$. By Proposition 3.4, the code $H^{t_1,\ldots,t_s} = H^{1,0,\ldots,0,t_{s-1},t_s}$ is permutation equivalent to $H^{t_{s-1}+1,t_s+s-2}$, which is $\mathbb{Z}_4$-linear and so propelinear. Then the statement follows by Lemma 3.4. □

4. Improvement of the partial classification

In this section, we improve some results given in [7], on the classification of the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, once t is fixed. More precisely, we improve the upper bounds of $\mathcal{A}_t$ given by Theorem 2.1 and determine the exact value of $\mathcal{A}_t$ for $t \leq 11$ by using the equivalence results established in Section 3.

Next, we prove two corollaries of Theorem 3.1, which allow us to improve the known upper bounds for $\mathcal{A}_t$.

Corollary 4.1. *Let $H^{t_1,\ldots,t_s}$ be a $\mathbb{Z}_{2^s}$-linear Hadamard code. Then, $H^{t_1,\ldots,t_s}$ is equivalent to $t_s+\sigma$ $\mathbb{Z}_{2^{s'}}$-linear Hadamard codes for $s' \in \{s+1-\sigma, \ldots, s+t_s\}$. Among them, there is exactly one $H^{t'_1,\ldots,t'_{s'}}$ with $t'_1 \geq 2$, and there is exactly one $H^{t'_1,\ldots,t'_{s'}}$ with $t'_{s'} = 0$.*

Proof. The code $H^{t_1,\ldots,t_s}$ belongs to a chain of equivalences C, which can be determined by Proposition 3.4. We have that $H^{t_1,\ldots,t_s}$ is equivalent to any code in C by Theorem 3.1, and the number of codes in C is $t_s+\sigma$ by Corollary

3.4. By Proposition 3.4, the first code in C has $s' = s-\sigma+1$. By Proposition 3.3, the ith code $H^{t'_1,\dots,t'_{s'}} = C[i]$ has $s' = s-\sigma+i$ for $i \in \{1,\dots,t_s+\sigma\}$. Therefore, $s' \in \{s-\sigma+1,\dots,s+t_s\}$. Finally, by Corollary 3.3, $C[1]$ is the only code in C with $t'_1 \geq 2$ and $C[t_s+\sigma]$ is the only code in C with $t'_{s'} = 0$. $\square$

From Corollary 4.1, in order to determine the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, $\mathcal{A}_t$, we just have to consider one code out of the $t_s+\sigma$ codes that are equivalent. For example, we can consider the one with $t_1 \geq 2$.

Corollary 4.2. *Let H be a nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard code of length 2^t. If $s \in \{\lfloor (t+1)/2\rfloor + 1,\dots,t+1\}$, then there is an equivalent $\mathbb{Z}_{2^{s'}}$-linear Hadamard code of length 2^t with $s' \in \{2,\dots,\lfloor (t+1)/2\rfloor\}$.*

Proof. Let $H^{t_1,\dots,t_s}$ be a $\mathbb{Z}_{2^s}$-linear Hadamard code with $s \in \{\lfloor (t+1)/2\rfloor+1,\dots,t+1\}$. Since $\sum_{i=1}^{s}(s+1-i)t_i = t+1$, then $t_1 = 1$ and we have that $\sigma > 1$. Therefore, by Proposition 3.4, $H^{t_1,\dots,t_s}$ is permutation equivalent to the $\mathbb{Z}_{2^{s-\sigma+1}}$-linear Hadamard code $H = H^{t_\sigma+1,t_{\sigma+1},\dots,t_{s-1},t_s+\sigma-1}$.

Now, we just need to see that $s-\sigma+1 < \lfloor (t+1)/2\rfloor$. Since the length of H is 2^t, we have that $t+1 = (s-\sigma+1)(t_\sigma+1)+\sum_{i=2}^{s-\sigma+1}(s-\sigma+2-i)t_{\sigma-1+i}+\sigma-1$. Therefore, $(s-\sigma+1)(t_\sigma+1) \leq t+1$ and $s-\sigma+1 \leq (t+1)/(t_\sigma+1)$. By the definition of t_σ, we know that $t_\sigma \geq 1$, so $s-\sigma+1 \leq \lfloor (t+1)/2\rfloor$. $\square$

Note that we can focus on the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t with $s \in \{2,\dots,\lfloor (t+1)/2\rfloor\}$ by Corollary 4.2, and we can restrict ourselves to the codes having $t_1 \geq 2$ by Corollary 4.1. With this on mind, in order to classify all such codes for a given $t \geq 3$, we define $\tilde{X}_{t,s} = |\{(t_1,\dots,t_s) \in \mathbb{N}^s : t+1 = \sum_{i=1}^{s}(s-i+1)t_i,\ t_1 \geq 2\}|$ for $s \in \{3,\dots,\lfloor (t+1)/2\rfloor\}$ and $\tilde{X}_{t,2} = |\{(t_1,t_2) \in \mathbb{N}^2 : t+1 = 2t_1+t_2,\ t_1 \geq 3\}|$. Note that, in the definition of $\tilde{X}_{t,2}$, we consider $t_1 \geq 3$ because the code is linear if $t_1 = 2$ [14].

Theorem 4.1. *Let $\mathcal{A}_t$ be the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t with $t \geq 3$. Then,*

$$\mathcal{A}_t \leq 1 + \sum_{s=2}^{\lfloor \frac{t+1}{2} \rfloor} \tilde{X}_{t,s} \tag{14}$$

and

$$\mathcal{A}_t \leq 1 + \sum_{s=2}^{\lfloor \frac{t+1}{2} \rfloor} (\mathcal{A}_{t,s} - 1). \quad (15)$$

Moreover, for $3 \leq t \leq 11$, the upper bound (14) is tight.

Proof. In [7], it is proven that the codes $H^{1,0,\dots,0,t_s}$ and $H^{1,0,\dots,0,1,t_s}$, with $s > 2$ and $t_s \geq 0$, are the only $\mathbb{Z}_{2^s}$-linear Hadamard codes which are linear. Note that they are not included in the definition of $\tilde{X}_{t,s}$ for $s \in \{3, \dots, \lfloor (t+1)/2 \rfloor\}$. When $s = 2$, recall that the codes with $t_1 = 1$ and $t_1 = 2$ are the ones which are linear [14]. Note that they are not included in the definition of $\tilde{X}_{t,2}$ either. Therefore, the new upper bounds (14) and (15) follow by Corollaries 4.1 and 4.2, after adding 1 to take into account the linear code.

In Table 5, for $3 \leq t \leq 11$, these new upper bounds together with previous bounds are shown. Note that the lower bound (r, k) coincides with the upper bound (14) for $t \leq 11$, so this upper bound is tight for $t \leq 11$. □

t	3	4	5	6	7	8	9	10	11
lower bound (r, k)	**1**	**1**	**3**	**3**	**6**	**7**	**11**	**13**	**20**
upper bound (14)	**1**	**1**	**3**	**3**	**6**	**7**	**11**	**13**	**20**
upper bound (15)	1	1	3	4	9	12	22	28	47
upper bound (3) and (4)	1	1	3	5	10	16	26	38	57

Table 5: Bounds for the number $\mathcal{A}_t$ of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t for $3 \leq t \leq 11$.

This last result improves the partial classification given in [7]. Actually, by definition, we have that $\tilde{X}_{t,s} \leq X_{t,s} - 2$, so the upper bound (14) is clearly better than (3). It is also clear that the upper bound (15) is better than (4) since there are fewer addends. Therefore, both new upper bounds improve the previous known upper bounds obtained in [7]. Recall that $\mathcal{A}_{t,s} = X_{t,s} - 1$ for any $3 \leq t \leq 11$ and $2 \leq s \leq t - 2$. If this equation is also true for any $t \geq 12$, then upper bounds (3) and (4) coincide. Moreover, upper bound (14) would always be better than (15) since $\tilde{X}_{t,s} \leq X_{t,s} - 2 = \mathcal{A}_{t,s} - 1$.

5. Full classification of $\mathbb{Z}_4$-linear and $\mathbb{Z}_8$-linear Hadamard codes

A complete classification of $\mathbb{Z}_4$-linear and $\mathbb{Z}_8$-linear Hadamard codes is given in [14] and [8], respectively. By the results in Section 3, we know that there are nonlinear Hadamard codes which are equivalent to both, a $\mathbb{Z}_4$-linear and a $\mathbb{Z}_8$-linear code. In this section, we establish the complete classification for the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t with $s \in \{2,3\}$. We also determine the number of nonequivalent such codes.

Theorem 5.1. *Every $\mathbb{Z}_4$-linear Hadamard code of length 2^t is equivalent to a $\mathbb{Z}_8$-linear Hadamard code, except for the $\mathbb{Z}_4$-linear Hadamard code $H^{(t+1)/2,0}$ with $t \geq 5$ odd.*

Proof. First of all, for $t \leq 4$, we know that all $\mathbb{Z}_{2^s}$-linear Hadamard codes are linear, so they are permutation equivalent to the binary linear Hadamard code of length 2^t. Recall that, for $s = 2$, we have that $t = 2t_1 + t_2 - 1$. Then, if t is even, all the solutions for $t = 2t_1 + t_2 - 1$ satisfy that $t_2 \geq 1$. Then, by using Theorem 3.1, we have that every $\mathbb{Z}_4$-linear Hadamard code H^{t_1,t_2} of length 2^t is permutation equivalent to the $\mathbb{Z}_8$-linear Hadamard code H^{1,t_1-1,t_2-1}.

If t is odd, then there exists one solution for $t = 2t_1 + t_2 - 1$ with $t_2 = 0$, that is, when $t_1 = (t+1)/2$. For the rest of solutions with $t_2 \geq 1$, again by using Theorem 3.1, we know that each $\mathbb{Z}_4$-linear Hadamard code is permutation equivalent to a $\mathbb{Z}_8$-linear Hadamard code. Finally, we have to show that the code $H^{(t+1)/2,0}$ is not permutation equivalent to a $\mathbb{Z}_8$-linear Hadamard code.

Suppose that there exists a $\mathbb{Z}_8$-linear Hadamard code H^{t_1,t_2,t_3} that is permutation equivalent to $H^{(t+1)/2,0}$. We know that both codes should have the same length and dimension of the kernel. Recall that $\ker(H^{(t+1)/2,0}) = (t+1)/2+1$ since $t \geq 5$ [14]. We also have that $\ker(H^{t_1,t_2,t_3}) = t_1+t_2+t_3+\sigma_{t_1}$, where $\sigma_{t_1} = 1$ if $t_1 \geq 2$ and $\sigma_{t_1} = 2$ if $t_1 = 1$ [7]. On the one hand, if $t_1 = 1$, then $\sigma_{t_1} = 2$ and, from the equations $t+1 = 3 + 2t_2 + t_3$ and $(t+1)/2+1 = 1+t_2+t_3+2$, we obtain that $t_3 = -1$ which is not possible. On the other hand, if $t_1 \geq 2$, then $\sigma_{t_1} = 1$ and we have the following equations:

$$\left.\begin{array}{rcl} t+1 & = & 3t_1 + 2t_2 + t_3 \\ \dfrac{t+1}{2} + 1 & = & t_1 + t_2 + t_3 + 1 \end{array}\right\} \Rightarrow \left\{\begin{array}{rcl} t_3 & = & t_1 \\ t_2 & = & \dfrac{t+1-4t_1}{2} \end{array}\right. .$$

These two codes should also have the same rank, so $\mathrm{rank}(H^{t_1,(t+1-4t_1)/2,t_1}) = \mathrm{rank}(H^{(t+1)/2,0})$. As proven in [18], we have that if $t_1 \geq 1$ and $t_2 \geq 0$, then

$$\mathrm{rank}(\Phi(\mathcal{H}^{t_1,t_2})) = 2t_1 + t_2 + \binom{t_1 - 1}{2}.$$

From [8], we also have that

$$\mathrm{rank}(\Phi(\mathcal{H}^{t_1,t_2,t_3})) = \frac{t_1^4}{24} - \frac{t_1^3}{12} + \frac{35t_1^2}{24} + \frac{7t_1}{12} + \frac{t_2}{2}(t_1^2 + t_1 + t_2 + 1) + t_3 + 1.$$

Then, after simplifying, we obtain that

$$t_1^3 - 26t_1^2 + (6t + 65)t_1 - 18t - 4 = 0. \tag{16}$$

Note that the left-hand side of equation (16) is strictly positive for $t_1 \geq 26$, since we can rewrite it as $t_1^3 + (6t + 65)t_1 > 26t_1^2 + 18t + 4$. For $t_1 \in \{3, 6, 8, 9, 10, 12, \ldots, 25\}$, equation (16) has no integer solution for t. For $t_1 = 1$, it has solution $t = 3$, but recall that $t \geq 4$. For $t_1 = 4$, it has solution $t = 16$, but in this case $t_2 = 1/2 \notin \mathbb{Z}$. Finally, for $t_1 \in \{2, 5, 7, 11\}$, it has solutions $t = 5, 17, 20, 23$, respectively, but in all these cases, $t_2 < 0$. Therefore, the result holds. □

We have shown that the classification of the $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s \in \{2, 3\}$ is complete. Specifically, there exists only one binary nonlinear Hadamard code of length 2^t that is $\mathbb{Z}_4$-linear, but not $\mathbb{Z}_8$-linear, when t odd. When t is even, all the $\mathbb{Z}_4$-linear Hadamard codes of length 2^t are also $\mathbb{Z}_8$-linear. This means that to generate all the $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s \in \{2, 3\}$ of a fixed length 2^t, it is enough to generate all the $\mathbb{Z}_8$-linear Hadamard codes, and add the code $H^{(t+1)/2,0}$ if t is odd. Finally, in Theorem 5.2, we establish the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s \in \{2, 3\}$, once the length 2^t if fixed.

Theorem 5.2. *Let $\mathcal{A}_{t,\{2,3\}}$ be the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t with $s \in \{2, 3\}$. Then,*

$$\mathcal{A}_{t,\{2,3\}} = \begin{cases} 1 & \text{if } t < 5 \\ \mathcal{A}_{t,3} + (t \mod 2) & \text{if } t \geq 5, \end{cases}$$

where the number of nonequivalent $\mathbb{Z}_8$-linear Hadamard codes of length 2^t is

$$\mathcal{A}_{t,3} = \left\lfloor \frac{t+1}{3} \right\rfloor + \sum_{i=1}^{\lfloor (t+1)/3 \rfloor} \left\lfloor \frac{t+1-3i}{2} \right\rfloor - 1.$$

Proof. The explicit expression for $\mathcal{A}_{t,3}$ is proven in [8]. Then, the expression for $\mathcal{A}_{t,\{2,3\}}$ follows from Theorem 5.1 □

In Table 6, we can see the complete classification of the $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s \in \{2,3\}$ for $7 \leq t \leq 9$. In the second row, there are the codes that are both $\mathbb{Z}_4$-linear and $\mathbb{Z}_8$-linear together with its pair (r,k). In the first and third rows, there are the codes that are just $\mathbb{Z}_4$-linear or $\mathbb{Z}_8$-linear, respectively.

	$t=7$		$t=8$		$t=9$	
	type	(r,k)	type	(r,k)	type	(r,k)
$\mathbb{Z}_4$	$(4,0)$	(11,5)			$(5,0)$	(16,6)
$\mathbb{Z}_4$ $\mathbb{Z}_8$	$(3,2)$ $(1,2,1)$	(9,6)	$(3,3)$ $(1,2,2)$ $(4,1)$ $(1,3,0)$	(10,7) (12,6)	$(3,4)$ $(1,2,3)$ $(4,2)$ $(1,3,1)$	(11,8) (13,7)
$\mathbb{Z}_8$	$(2,0,2)$ $(2,1,0)$	(10,5) (12,4)	$(2,0,3)$ $(2,1,1)$ $(3,0,0)$	(11,6) (13,5) (17,4)	$(2,0,4)$ $(2,1,2)$ $(2,2,0)$ $(3,0,1)$	(12,7) (14,6) (17,5) (18,5)

Table 6: Type, rank and dimension of the kernel for all nonlinear $\mathbb{Z}_4$-linear and $\mathbb{Z}_8$-linear Hadamard codes of length 2^t for $7 \leq t \leq 9$.

6. Conclusions

The results presented in this paper allow us to improve the partial classification on the number $\mathcal{A}_t$ of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes having the same length 2^t, given in [7]. Specifically, we establish that there are some families of such codes which are equivalent. This result allows us to give new upper bounds on $\mathcal{A}_t$. Moreover, we show that one of them, (14), is tight for any $3 \leq t \leq 11$. Actually, for these cases, we notice that the full classification is also given by considering the pairs of invariants, rank and dimension of the kernel. A future research would be to establish whether this is also true in general, that is for any $t \geq 12$.

Recall that $\mathcal{A}_{t,s}$ is the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes having the same value of s and the same length 2^t. In general, by definition, we have that $\mathcal{A}_{t,s} \leq X_{t,s} - 1$. From Tables 1 and 3, for $5 \leq t \leq 11$ and $2 \leq s \leq t-2$, we know that $\mathcal{A}_{t,s} = X_{t,s} - 1$, that is, the classification of these codes is given by the number of solutions $(t_1, \ldots, t_s) \in \mathbb{N}^s$ of the equation $t = (\sum_{i=1}^{s}(s-i+1)\cdot t_i) - 1$ with $t_1 \geq 1$. Moreover, $\mathcal{A}_{t,s}$ also coincides with the exact number of different pairs of invariants, rank and dimension of the kernel. It is an open problem to determine whether $\mathcal{A}_{t,s} = X_{t,s} - 1$ for all $t \geq 12$. Note that when this equation holds, the upper bound (14) is better than (15).

As we can see in Table 4, there are some $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t which are not equivalent to any other such code with the same length. For example, the codes $H^{4,0}$, $H^{2,1,0}$, and $H^{2,0,0,0}$ of length 2^7 are just $\mathbb{Z}_4$-linear, $\mathbb{Z}_8$-linear, and $\mathbb{Z}_{16}$-linear codes, respectively. In general, we conjecture that the $\mathbb{Z}_{2^s}$-linear Hadamard codes $H^{t_1,\ldots,t_s}$ with $t_1 \geq 2$ (i.e. $\sigma = 1$) and $t_s = 0$ are not equivalent to any other $\mathbb{Z}_{2^{s'}}$-linear Hadamard code of the same length.

When we focus on the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t with $s \in \{2,3\}$, we are able to give a complete classification for any $t \geq 3$, by using the equivalence results given in Section 3 and the explicit formula for the rank of the $\mathbb{Z}_4$-linear and $\mathbb{Z}_8$-linear Hadamard codes, computed in [14] and [8], respectively.

There are Hadamard codes, called $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes, which came from the image of a generalized Gray map of subgroups of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. If $\alpha = 0$, they correspond to $\mathbb{Z}_4$-linear Hadamard codes. In [18], the classification of all $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes of length 2^t with $\alpha \neq 0$ is given. Moreover, in [15], it is proven that each one of these codes is equivalent to a $\mathbb{Z}_4$-linear Hadamard code, except for one, namely $\bar{H}_t$, when t is even. It is known that $\bar{H}_t$ has rank $r = 1 + t + \binom{t/2}{2}$ and dimension of the kernel $k = 1 + t/2$ [18]. From this result and Tables 1 and 3, it is easy to check that $\bar{H}_t$ is not equivalent to any $\mathbb{Z}_{2^s}$-linear Hadamard code of the same length 2^t for $4 \leq t \leq 11$ even. Another further research could be to show that this is also true for any $t \geq 12$ even.

In [22], a more general family of Hadamard codes, constructed from the image of the generalized Gray map of subgroups of $\mathbb{Z}_p^{\alpha_1} \times \mathbb{Z}_{p^2}^{\alpha_2} \times \cdots \times \mathbb{Z}_{p^s}^{\alpha_s}$ with p prime, are described. The techniques developed in [7, 8, 9] and in this paper could also be applied to these codes in order to classify them. In [10], the results on the kernel and its dimension of $\mathbb{Z}_{2^s}$-linear Hadamard codes given in [7] have been used to establish equivalent results for the family of $\mathbb{Z}_{2^s}$-linear simplex and MacDonald codes defined in [11].

Finally, it is also worth to mention that we have found that some $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s > 2$ are propelinear (so also transitive). It is an open problem to determine whether there are other $\mathbb{Z}_{2^s}$-linear Hadamard codes that are propelinear (or transitive) and not equivalent to a $\mathbb{Z}_4$-linear Hadamard code.

7. Acknowledgements

The authors would like to thank the anonymous referees for their comments, which enabled them to improve the paper.

This work has been partially supported by the Spanish MINECO under Grant TIN2016-77918-P (AEI/FEDER, UE), and by the Catalan AGAUR under Grant 2017SGR-00463. The material in this paper was presented in part at the 16th International Workshop on Algebraic and Combinatorial Coding Theory in Svetlogorsk (Kaliningrad region), Russia, 2018 [9].

References

[1] Assmus, E. F., Key, J. D.: Designs and Their Codes. Cambridge University Press, Great Britain (1992).

[2] Bauer, H., Ganter, B., Hergert, F.: Algebraic techniques for nonlinear codes. Combinatorica, 3, no. 1, pp. 21–33 (1983).

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

[4] Bosma, W., Cannon, J. J., Fieker, C., Steel, A.: Handbook of Magma functions, Edition 2.22, 5669 pages (2016). `http://magma.maths.usyd.edu.au/magma/`.

[5] Carlet, C.: $\mathbb{Z}_{2^k}$-linear codes. IEEE Trans. Inf. Theory, 44, no. 4, pp. 1543–1547 (1998).

[6] Dougherty, S. T., Fernández-Córdoba, C.: Codes over $\mathbb{Z}_{2^k}$, Gray map and self-dual codes. Advances in Mathematics of Communications, 5, no. 4, pp. 571–588 (2011).

[7] C. Fernández-Córdoba, C. Vela, and M. Villanueva, On $\mathbb{Z}_{2^s}$-linear Hadamard codes: kernel and partial classification. Designs, Codes and Cryptography, 87, no. 2-3, pp. 417–435 (2019).

[8] C. Fernández-Córdoba, C. Vela, and M. Villanueva, "On $\mathbb{Z}_8$-linear Hadamard codes: rank and classification," submitted to *IEEE Trans. Inf. Theory*, (2018).

[9] Fernández-Córdoba, C., Vela, C., Villanueva, M.: On some equivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes. Proc. of 16th International Workshop on Algebraic and Combinatorial Coding Theory, Svetlogorsk (Kaliningrad region), Russia, pp. 80–84 (2018).

[10] Fernández-Córdoba, C., Vela, C., Villanueva, M.: On the kernel of $\mathbb{Z}_{2^s}$-linear simplex and MacDonald codes, arXiv:1910.07911, (2019).

[11] Gupta, M. K., On some linear codes over $\mathbb{Z}_{2^s}$. PhD. Thesis (1998).

[12] Hammons, A. R., Kumar, P. V., Calderbank, A. R., Sloane, N. J. A., Solé, P.: The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes. IEEE Trans. Inf. Theory, 40, no. 2, pp. 301–319 (1994).

[13] Krotov, D. S.: On $\mathbb{Z}_{2^k}$-dual binary codes. IEEE Trans. Inf. Theory, 53, no. 4, pp. 1532–1537 (2007).

[14] Krotov, D. S.: $\mathbb{Z}_4$-linear Hadamard and extended perfect codes. Proc. of International Workshop on Coding and Cryptography, ser. Electron. Notes Discrete Math. 6, pp. 107–112 (2001).

[15] Krotov, D. S., Villanueva, M.: Classification of the $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes and their automorphism groups. IEEE Trans. Inf. Theory, 61, no. 2, pp. 887–894 (2015).

[16] MacWilliams, F. J., Sloane, N. J. A.: The Theory of Error-Correcting Codes. Elsevier, Amsterdam (1977).

[17] Shi, M., Sepasdar, Z., Alahmadi, A., Solé, P.: On two-weight $\mathbb{Z}_{2^k}$-codes. Designs, Codes and Cryptography, 86, no. 6, pp. 1201–1209 (2018).

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

[19] Pujol, J., Rifà, J.: Translation invariant propelinear codes. IEEE Trans. Inf. Theory, 43, pp. 590–598 (1997).

[20] Pujol, J., Villanueva, M.: Q-ary codes. A Magma package, version 1.0. Universitat Autònoma de Barcelona, Barcelona (2017). http://ccsg/uab.cat.

[21] Shi, M., Sepasdar, Z., Alahmadi, A., Solé, P.: On two-weight $\mathbb{Z}_{2^k}$-codes. Designs, Codes and Cryptography, 86, no. 6, pp. 1201–1209 (2018).

[22] Shi, M., Wu, R., Krotov, D. S.: On $\mathbb{Z}_p\mathbb{Z}_{p^k}$-additive codes and their duality. IEEE Trans. Inf. Theory, 65, no. 6, pp. 3841–3847 (2019).