Construction and classification of $\mathbb{Z}_{2^s}$-linear Hadamard codes [⋆]

C. Fernández-Córdoba, [1] C. Vela, [2] and M. Villanueva [3]

Departament d'Enginyeria de la Informació i de les Comunicacions
Universitat Autònoma de Barcelona
Cerdanyola del Vallès, Spain

Abstract

The $\mathbb{Z}_{2^s}$-additive and $\mathbb{Z}_2\mathbb{Z}_4$-additive codes are subgroups of $\mathbb{Z}_{2^s}^n$ and $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, respectively. Both families can be seen as generalizations of linear codes over $\mathbb{Z}_2$ and $\mathbb{Z}_4$. A $\mathbb{Z}_{2^s}$-linear ($\mathbb{Z}_2\mathbb{Z}_4$-linear) Hadamard code is a binary Hadamard code which is the Gray map image of a $\mathbb{Z}_{2^s}$-additive ($\mathbb{Z}_2\mathbb{Z}_4$-additive) code. It is known that there are exactly $\lfloor \frac{t-1}{2} \rfloor$ and $\lfloor \frac{t}{2} \rfloor$ nonequivalent $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes of length 2^t, with $\alpha = 0$ and $\alpha \neq 0$, respectively, for all $t \geq 3$. In this paper, new $\mathbb{Z}_{2^s}$-linear Hadamard codes are constructed for $s > 2$, which are not equivalent to any $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard code. Moreover, it is claimed that the new constructed nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard codes are pairwise nonequivalent.

Keywords: Hadamard codes, $\mathbb{Z}_{2^s}$-linear codes, generalized Gray map.

⋆ Research partially supported by the Spanish MINECO under Grant TIN2013-40524-P, and by the Catalan AGAUR under Grant 2014SGR-691.

[1] Email: `cristina.fernandez@uab.cat`
[2] Email: `carlos.vela@uab.cat`
[3] Email: `merce.villanueva@uab.cat`

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 the ring $\mathbb{Z}_{2^s}$ is denoted by $\mathbb{Z}_{2^s}^n$. In this paper, the elements of $\mathbb{Z}_{2^s}^n$ will also be called vectors over $\mathbb{Z}_{2^s}$ of length n. A binary code of length n is a nonempty subset of $\mathbb{Z}_2^n$. A nonempty subset $\mathcal{C}$ of $\mathbb{Z}_{2^s}^n$ ($\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$) is a $\mathbb{Z}_{2^s}$-additive ($\mathbb{Z}_2\mathbb{Z}_4$-additive) code if $\mathcal{C}$ is a subgroup of $\mathbb{Z}_{2^s}^n$ ($\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$). Note that, when $s = 1$ ($\beta = 0$), $\mathbb{Z}_{2^s}$-additive ($\mathbb{Z}_2\mathbb{Z}_4$-additive) is a binary linear code, and when $s = 2$ ($\alpha = 0$), it is a quaternary linear code or a linear code over $\mathbb{Z}_4$ [8]. For more details about $\mathbb{Z}_2\mathbb{Z}_4$-additive codes see [6].

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

In [8], 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 $\mathbb{Z}_2^{2^{s-1}}$ [5,7]. The one given in [7] is the map $\phi : \mathbb{Z}_{2^s} \to \mathbb{Z}_2^{2^{s-1}}$ defined as follows:

$$\phi(u) = (u_s, \ldots, u_s) + (u_1, \ldots, u_{s-1})Y,$$

where $u \in \mathbb{Z}_{2^s}$, $[u_1, u_2, \ldots, u_s]_2$ is the binary expansion of u, that is $u = \sum_{i=1}^s 2^{i-1} u_i$ ($u_i \in \mathbb{Z}_2$), and Y is a matrix of size $(s-1) \times 2^{s-1}$ which columns are the elements of $\mathbb{Z}_2^{s-1}$. Note that $(u_s, \ldots, u_s)$ and $(u_1, \ldots, u_{s-1})Y$ are binary vectors of length 2^{s-1}. Then, define $\Phi : \mathbb{Z}_{2^s}^n \to \mathbb{Z}_2^{n2^{s-1}}$ as the component-wise Gray map ϕ.

Let $\mathcal{C}$ be a $\mathbb{Z}_{2^s}$-additive code of length n. We say that its binary image $C = \Phi(\mathcal{C})$ 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 $C = \Phi(\mathcal{C})$, is of type $(n; t_1, \ldots, t_s)$. Note that $|C| = 2^{st_1} 2^{(s-1)t_2} \cdots 2^{t_s}$. For linear codes over finite fields, there exists a basis, since they are vector subspaces. For linear codes over a ring, we cannot give a basis, but there exists a generator matrix with minimum number of rows. If $\mathcal{C}$ is a $\mathbb{Z}_2^s$-additive code of type $(n; t_1, \ldots, t_s)$, then the minimum number of rows in a generator matrix of $\mathcal{C}$ is $t_1 + \cdots + t_s$.

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of length n. The Gray map $\Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \rightarrow \mathbb{Z}_2^{\alpha+2\beta}$ is defined as the identity in the first α coordinates and the componentwise Gray map ϕ in the last β coordinates. We say that $C = \Phi(\mathcal{C})$ is a $\mathbb{Z}_2\mathbb{Z}_4$-linear code of length $\alpha + 2\beta$. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, it is isomorphic to an abelian structure $\mathbb{Z}_4^{t_1} \times \mathbb{Z}_2^{t_2}$, and we say that $\mathcal{C}$, or equivalently C, is of type $(\alpha, \beta; t_1, t_2)$.

A binary code of length n, $2n$ codewords and minimum distance $n/2$ is called a Hadamard code. Hadamard codes can be constructed from normalized Hadamard matrices [1,11]. The $\mathbb{Z}_{2^s}$-additive codes that, under the Gray map Φ, give a Hadamard code are called $\mathbb{Z}_{2^s}$-additive Hadamard codes and the corresponding $\mathbb{Z}_{2^s}$-linear codes are called $\mathbb{Z}_{2^s}$-linear Hadamard codes.

The classification of $\mathbb{Z}_4$-linear Hadamard codes is given by the following result. For any integer $t \geq 3$ and each $t_1 \in \{1, \dots, \lfloor (t+1)/2 \rfloor\}$, there is a unique (up to equivalence) $\mathbb{Z}_4$-linear Hadamard code of type $(2^{t-1}; t_1, t+1-2t_1)$, and all these codes are pairwise nonequivalent, except for $t_1 = 1$ and $t_1 = 2$, where the codes are equivalent to the linear Hadamard code, that is, the dual of the extended Hamming code [9]. Therefore, the number of nonequivalent $\mathbb{Z}_4$-linear Hadamard codes of length 2^t is $\lfloor \frac{t-1}{2} \rfloor$ for all $t \geq 3$, and it is 1 for $t = 1$ and for $t = 2$.

In the case of $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes, it is known that for any integer $t \geq 3$ and each $t_1 \in \{0, \dots, \lfloor t/2 \rfloor\}$, there is a unique (up to equivalence) $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard code of type $(2^{t-t_1}, 2^{t-1} - 2^{t-t_1-1}; t_1, t+1-2t_1)$. Again, all these codes are pairwise nonequivalent, except for $t_1 = 0$ and $t_1 = 1$, where the codes are equivalent to the linear Hadamard code [4]. Therefore, the number of nonequivalent $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes of length 2^t with $\alpha \neq 0$ is $\lfloor \frac{t}{2} \rfloor$ for all $t \geq 3$. Actually, in [10], it is shown that each $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard code with $\alpha = 0$ is equivalent to a $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard code with $\alpha \neq 0$, so there are only $\lfloor \frac{t}{2} \rfloor$ nonequivalent $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes of length 2^t.

In this paper, we construct $\mathbb{Z}_{2^s}$-additive Hadamard codes, we show that there are $\mathbb{Z}_{2^s}$-linear Hadamard codes which are not equivalent to any $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard code, and we claim that the new constructed nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard codes are pairwise nonequivalent.

2 Construction of Hadamard codes

Let $T_i = \{j \cdot 2^{s-i} \ : \ j \in \{0, 1, \dots, 2^i - 1\}\}$, for all $i \in \{1, \dots, s\}$. Note that $T_s = \{0, \dots, 2^s - 1\}$. 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 z^T, $z \in \{1\} \times T_s^{t_1-1} \times T_{s-1}^{t_2} \times \cdots \times T_1^{t_s}$.

Example 2.1 For $s = 3$, for example, we have the following matrices:

$$A^{1,0,1} = \begin{pmatrix} 1\,1 \\ 0\,4 \end{pmatrix}, \quad A^{1,1,0} = \begin{pmatrix} 11\ 11 \\ 02\ 46 \end{pmatrix}, \quad A^{2,0,0} = \begin{pmatrix} 11\ 11\ 11\ 11 \\ 01\ 23\ 45\ 67 \end{pmatrix},$$

$$A^{1,1,1} = \begin{pmatrix} 11\ 11\ 11\ 11 \\ 02\ 46\ 02\ 46 \\ 00\ 00\ 44\ 44 \end{pmatrix}, \quad A^{2,0,1} = \begin{pmatrix} 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11 \\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67 \\ 00\ 00\ 00\ 00\ 44\ 44\ 44\ 44 \end{pmatrix},$$

$$A^{2,1,0} = \begin{pmatrix} 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11 \\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67 \\ 00\ 00\ 00\ 00\ 22\ 22\ 22\ 22\ 44\ 44\ 44\ 44\ 66\ 66\ 66\ 66 \end{pmatrix}.$$

Let $\mathcal{H}^{t_1,\ldots,t_s}$ be the $\mathbb{Z}_{2^s}$-additive code generated by the matrix $A^{t_1,\ldots,t_s}$, where $t_1, \ldots, t_s \geq 0$ with $t_1 \geq 1$. Let $n = 2^{t-s+1}$, where $t = (\sum_{i=1}^{s}(s-i+1)\cdot t_i) - 1$. It is easy to see that the $\mathbb{Z}_{2^s}$-additive code $\mathcal{H}^{t_1,\ldots,t_s}$ is of length n, have $|\mathcal{H}^{t_1,\ldots,t_s}| = 2^s n = 2^{t+1}$ codewords and minimum (Lee) distance n. Note that this code is of type $(n; t_1, t_2, \ldots, t_s)$. Let $H^{t_1,\ldots,t_s} = \Phi(\mathcal{H}^{t_1,\ldots,t_s})$ be the corresponding $\mathbb{Z}_{2^s}$-linear code.

Theorem 2.2 *Let $t_1, \ldots, t_s$ be nonnegative integers with $t_1 \geq 1$. The $\mathbb{Z}_{2^s}$-linear code $H^{t_1,\ldots,t_s}$ of type $(n; t_1, t_2, \ldots, t_s)$ is a binary Hadamard code of length 2^t, with $t = (\sum_{i=1}^{s}(s-i+1)\cdot t_i) - 1$.*

Example 2.3 Let $\mathcal{H}^{2,0,0}$ be the $\mathbb{Z}_8$-additive code generated by $A^{2,0,0}$ given in Example 2.1. The $\mathbb{Z}_8$-linear code $H^{2,0,0} = \Phi(\mathcal{H}^{2,0,0})$ has length 32, 64 codewords and minimum (Hamming) distance 16. Therefore, it is a binary Hadamard code.

3 Classification of Hadamard 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 $\mathrm{K}(C) = \{x \in \mathbb{Z}_2^n : x + C = C\}$ [3]. If the all-zero vector belongs to C, then $\mathrm{K}(C)$ is a linear subcode of C. In general, C can be written as the union of cosets of $\mathrm{K}(C)$, and $\mathrm{K}(C)$ is the largest linear code for which this is true [3]. We will denote the rank of a binary code C as $\mathrm{rank}(C)$ and the dimension of the kernel as $\ker(C)$. The $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes can be classified using either the rank or the dimension of the kernel, as it is proven in [9,12], where these parameters are computed.

Theorem 3.1 *For a fixed $t \geq 3$, the $\mathbb{Z}_{2^s}$-linear Hadamard codes $H^{t_1,\dots,t_s}$, with $t_1,\dots,t_s \geq 0$, $t_1 \geq 1$, and $t = (\sum_{i=1}^{s}(s-i+1)\cdot t_i) - 1$, are pairwise nonequivalent binary codes of length 2^t.*

Example 3.2 Consider the $\mathbb{Z}_8$-linear Hadamard code $H^{2,0,0}$ given in Example 2.3. Using MAGMA software, we have that $\ker(H^{2,0,0}) = 3$ and $\mathrm{rank}(H^{2,0,0}) = 8$. Therefore, the code $H^{2,0,0}$ is a binary nonlinear Hadamard code. The code $H^{2,0,0}$ has binary length 32. There are three nonequivalent $\mathbb{Z}_4$-linear Hadamard codes of length 32, $\mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{C}_3$, of type $(16; 5, 1)$, $(16; 4, 2)$ and $(16; 3, 3)$, respectively. The codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are linear, and $\mathcal{C}_3$ has rank 7 and the dimension of the kernel is 3. Hence, there is no $\mathbb{Z}_4$-linear Hadamard code equivalent to the $\mathbb{Z}_8$-linear Hadamard code $H^{2,0,0}$.

Table 1 shows the number of $\mathbb{Z}_8$-linear Hadamard codes vs. $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes of length 2^t. Moreover, for example, for $t = 6$ as we have seen in Example 2.3, both binary Hadamard codes are nonequivalent. Therefore, we can construct binary nonlinear Hadamard codes that are $\mathbb{Z}_{2^s}$-linear codes and are not equivalent to any $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes.

t	3	4	5	6	7	8	9	10	11
$\mathbb{Z}_8$	0	0	1	2	3	5	6	8	10
$\mathbb{Z}_2\mathbb{Z}_4$	0	0	1	1	2	2	3	3	4

Table 1

Number of nonlinear $\mathbb{Z}_8$-linear and $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes of length 2^t.

References

[1] Assmus, E. F., and J. D. Key, "Designs and their codes," Cambridge University Press, Great Britain, (1992).

[2] Bannai, E., S. T. Dougherty, M. Harada and M. Oura, *Type II codes, even unimodular lattices, and invariant rings,* IEEE Trans. Inform. Theory, **45** (1999), 1194–1205.

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

[4] Borges, J., K. T. Phelps, and J. Rifà, *The rank and kernel of extended* 1*-perfect* Z_4*-linear and additive non-*Z_4*-linear codes*, IEEE Trans. Inf. Theory, **49** (2003), no. 8, 2028–2034.

[5] Dougherty,S. T., and C. Fernández-Córdoba, *Codes Over* $\mathbb{Z}_{2^k}$*, Gray Map and Self-Dual Codes*, Advances in Mathematics of Communications 5, **4** (2011), 571–588.

[6] Borges, J., C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. villanueva, $\mathbb{Z}_2\mathbb{Z}_4$-*linear codes: generator matrices and duality*, Designs, Codes and Cryptography, **54** (2010), Issue 2, 167-179.

[7] Carlet, C. $\mathbb{Z}_{2^k}$*-linear codes*, IEEE Trans. Inform. Theory, **44** (1998), 1543–1547.

[8] Hammons, A. R., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory, **40** (1994), 301–319.

[9] Krotov, D. S., $\mathbb{Z}_4$*-linear Hadamard and extended perfect codes,* WCC2001, International Workshop on Coding and Cryptography, ser. Electron. Notes Discrete Math., **6** (2001), 107–112.

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

[11] MacWilliams, F. J., and N. J. A. Sloane, “The theory of error-correcting codes”, *16* (1977), Elsevier.

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