PD-sets for (nonlinear) Hadamard Z_4-linear codes

R. D. Barrolleta[1], M. Villanueva[1]

[1] *Universitat Autònoma de Barcelona, Spain, {rolanddavid.barrolleta, merce.villanueva}@uab.cat*
This work was partially supported by the Spanish MEC under Grant TIN2013-40524-P, and by the Catalan AGAUR under Grant 2014SGR-691.

Any nonempty subset C of $\mathbb{Z}_2^n$ is a binary code and a subgroup of $\mathbb{Z}_2^n$ is called a *binary linear code*. Equivalently, any nonempty subset $\mathscr{C}$ of $\mathbb{Z}_4^n$ is a quaternary code and a subgroup of $\mathbb{Z}_4^n$ is called a *quaternary linear code*. Quaternary codes can be seen as binary codes under the usual Gray map $\Phi : \mathbb{Z}_4^n \rightarrow \mathbb{Z}_2^{2n}$ defined as $\Phi((y_1,\ldots,y_n)) = (\phi(y_1),\ldots,\phi(y_n))$, where $\phi(0) = (0,0)$, $\phi(1) = (0,1)$, $\phi(2) = (1,1)$, $\phi(3) = (1,0)$, for all $y = (y_1,\ldots,y_n) \in \mathbb{Z}_4^n$. If $\mathscr{C}$ is a quaternary linear code, the binary code $C = \Phi(\mathscr{C})$ is said to be a $\mathbb{Z}_4$-*linear code*.

A $\mathbb{Z}_2\mathbb{Z}_4$-*additive code* $\mathscr{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. We consider the extension of the Gray map $\Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \rightarrow \mathbb{Z}_2^{\alpha+2\beta}$ defined as $\Phi(x,y) = (x,\phi(y_1),\ldots,\phi(y_\beta))$, for all $x \in \mathbb{Z}_2^\alpha$ and $y = (y_1,\ldots,y_\beta) \in \mathbb{Z}_4^\beta$. This generalization allows us to consider $\mathbb{Z}_2\mathbb{Z}_4$-additive codes also as binary codes. If $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, the binary code $C = \Phi(\mathscr{C})$ is said to be a $\mathbb{Z}_2\mathbb{Z}_4$-*linear code*. Moreover, since the code $\mathscr{C}$ is isomorphic to an abelian group $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$, we say that $\mathscr{C}$ (or equivalently the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-linear code $C = \Phi(\mathscr{C})$) is of type $(\alpha,\beta;\gamma,\delta)$ [3]. Note that $\mathbb{Z}_2\mathbb{Z}_4$-additive codes can be seen as a generalization of binary (when $\beta = 0$) and quaternary (when $\alpha = 0$) linear codes. The *permutation automorphism group* of $\mathscr{C}$ and $C = \Phi(\mathscr{C})$, denoted by PAut($\mathscr{C}$) and PAut(C), respectively, is the group generated by all permutations that let the set of codewords invariant.

A binary Hadamard code of length n has $2n$ codewords and minimum distance $n/2$. The $\mathbb{Z}_2\mathbb{Z}_4$-additive codes such that, under the Gray map, give a binary Hadamard code are called $\mathbb{Z}_2\mathbb{Z}_4$-*additive Hadamard codes* and the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-linear codes are called *Hadamard* $\mathbb{Z}_2\mathbb{Z}_4$-*linear codes*, or just *Hadamard* $\mathbb{Z}_4$-*linear codes* when $\alpha = 0$. The permutation automorphism group of $\mathbb{Z}_2\mathbb{Z}_4$-additive Hadamard codes with $\alpha = 0$ was characterized in [9] and the permutation automorphism group of $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes was studied in [6].

Let C be a binary code of length n. For a vector $v \in \mathbb{Z}_2^n$ and a set $I \subseteq \{1,\ldots,n\}$, we denote by v_I the restriction of v to the coordinates in I and by C_I the set $\{v_I : v \in C\}$. Suppose that $|C| = 2^k$. A set $I \subseteq \{1,\ldots,n\}$ of k coordinate positions is an *information set* for C if $|C_I| = 2^k$. If such I exists, C is said to be a *systematic code*.

Permutation decoding is a technique, introduced by MacWilliams [8], which involves finding a subset S of the permutation automorphism group PAut(C) of a code C in order to assist in decoding. Let C be a systematic t-error-correcting code with information set I. A subset $S \subseteq \mathrm{PAut}(C)$ is an *s-PD-set* for the code C if every s-set of coordinate positions is moved out of the information set I by at least one element of the set S, where $1 \leq s \leq t$. If $s = t$, S is said to be a *PD-set*.

In [4], it is shown how to find s-PD-sets of size $s+1$ that satisfy the Gordon-Schönheim bound for partial permutation decoding for the binary simplex code S_m of length $2^m - 1$, for all $m \geq 4$ and $1 < s \leq \left\lfloor \frac{2^m-m-1}{m} \right\rfloor$. In [1], similar results are establish for the binary linear Hadamard code H_m (extended code of S_m) of length 2^m , for all $m \geq 4$ and $1 < s \leq \left\lfloor \frac{2^m-m-1}{1+m} \right\rfloor$, following the techniques described in [4].

The paper is organized as follows. In Section 1, we show that the Gordon-Schönheim bound can be adapted to systematic codes, not necessarily linear. Moreover, we apply the bound of the minimum size of s-PD-sets for binary Hadamard codes obtained in [1] to Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, which are systematic [2] but not linear in general. In Section 2, we provide a criterion to obtain s-PD-sets of size $s+1$ for $\mathbb{Z}_4$-linear codes. Finally, in Section 3, we recall a recursive construction to obtain all $\mathbb{Z}_2\mathbb{Z}_4$-additive codes with $\alpha = 0$ [7] and we give a recursive method to obtain s-PD-sets for the corresponding Hadamard $\mathbb{Z}_4$-linear codes.

1 Minimum size of s-PD-sets

There is a well-known bound on the minimum size of PD-sets for linear codes based on the length, dimension and minimum distance of such codes that can be adapted for systematic codes (not necessarily linear) easily:

Proposition 1. *Let C be a systematic t-error correcting code of length n, size $|C| = 2^k$ and minimum distance d. Let $r = n-k$ be the redundancy of C. If S is a PD-set for C, then*

$$|S| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \dots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \dots \right\rceil \right\rceil \right\rceil. \tag{1}$$

The above inequality (1) is often called the *Gordon-Schönheim bound*. This result is quoted and proved for linear codes in [5]. We can follow the same proof since the linearity of the code C is only used to guarantee that C is systematic. In [2], it is shown that $\mathbb{Z}_2\mathbb{Z}_4$-linear codes are systematic. Moreover, a systematic encoding is given for these codes.

The Gordon-Schönheim bound can be adapted to s-PD-sets for all s up to the error correcting capability of the code. Note that the error-correcting capability of any Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-linear code of length $n = 2^m$ is $t_m = \lfloor (d-1)/2 \rfloor = 2^{m-2} - 1$. Therefore, the right side of the bound given by (1), for Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-linear codes of length 2^m and for all $1 \leq s \leq t_m$, becomes

$$g_m(s) = \left\lceil \frac{2^m}{2^m-m-1} \left\lceil \frac{2^m-1}{2^m-m-2} \left\lceil \dots \left\lceil \frac{2^m-s+1}{2^m-m-s} \right\rceil \right\rceil \dots \right\rceil \right\rceil. \tag{2}$$

For any $m \geq 4$ and $1 \leq s \leq t_m$, we have that $g_m(s) \geq s+1$. The smaller the size of the PD-set is, the more efficient permutation decoding becomes. Because of this, we will focus on the case when $g_m(s) = s+1$.

2 s-PD-sets of size $s+1$ for $\mathbb{Z}_4$-linear codes

Let $\mathscr{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(0,\beta;\gamma,\delta)$ and let $C = \Phi(\mathscr{C})$ be the corresponding $\mathbb{Z}_4$-linear code. Let $\Phi : \mathrm{PAut}(\mathscr{C}) \to \mathrm{PAut}(C)$ be the map defined as

$$\Phi(\tau)(i) = \begin{cases} 2\tau(i/2), & \text{if } i \text{ is even,} \\ 2\tau(\frac{i+1}{2}) - 1 & \text{if } i \text{ is odd,} \end{cases}$$

for all $\tau \in \mathrm{Sym}(\beta)$ and $i \in \{1,\ldots,2\beta\}$. The map Φ is a group monomorphism. Given a subset $\mathscr{S}$ of $\mathrm{PAut}(\mathscr{C}) \subseteq \mathrm{Sym}(\beta)$, we define the set $S = \Phi(\mathscr{S}) = \{\Phi(\tau) : \tau \in \mathscr{S}\}$, which is a subset of $\mathrm{PAut}(C) \subseteq \mathrm{Sym}(2\beta)$.

A set $\mathscr{I} = \{i_1,\ldots,i_{\gamma+\delta}\} \subseteq \{1,\ldots,\beta\}$ of $\gamma+\delta$ coordinate positions is said to be a *quaternary information set* for the code $\mathscr{C}$ if the set $\Phi(\mathscr{I})$, defined as $\Phi(\mathscr{I}) = \{2i_1-1, 2i_1, \ldots, 2i_\delta - 1, 2i_\delta, 2i_{\delta+1}-1, \ldots, 2i_{\delta+\gamma}-1\}$, is an information set for $C = \Phi(\mathscr{C})$ for some ordering of elements of $\mathscr{I}$.

Let S be an s-PD-set of size $s+1$. The set S is a *nested* s-PD-set if there is an ordering of the elements of S, $S = \{\sigma_1,\ldots,\sigma_{s+1}\}$, such that $S_i = \{\sigma_1,\ldots,\sigma_{i+1}\} \subseteq S$ is an i-PD-set of size $i+1$, for all $i \in \{1,\ldots,s\}$.

Proposition 2. *Let $\mathscr{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(0,\beta;\gamma,\delta)$ with quaternary information set $\mathscr{I}$ and let s be a positive integer. If $\tau \in \mathrm{PAut}(\mathscr{C})$ has at least $\gamma+\delta$ disjoint cycles of length $s+1$ such that there is exactly one quaternary information position per cycle of length $s+1$, then $S = \{\Phi(\tau^i)\}_{i=1}^{s+1}$ is an s-PD-set of size $s+1$ for the $\mathbb{Z}_4$-linear code $C = \Phi(\mathscr{C})$ with information set $\Phi(\mathscr{I})$. Moreover, any ordering of the elements of S gives a nested r-PD-set for any $r \in \{1,\ldots,s\}$.*

Example 3. *Let $\mathscr{C}_{0,3}$ be the $\mathbb{Z}_2\mathbb{Z}_4$-additive Hadamard code of type $(0,16;0,3)$ with generator matrix*

$$\mathscr{G}_{0,3} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 \end{pmatrix}.$$

Let $\tau = (1,16,11,6)(2,7,12,13)(3,14,9,8)(4,5,10,15) \in \mathrm{PAut}(\mathscr{C}_{0,3}) \subseteq \mathrm{Sym}(16)$ [9]. It is straightforward to check that $\mathscr{I} = \{1,2,5\}$ is a quaternary information set for $\mathscr{C}_{0,3}$. Note that each information position in $\mathscr{I}$ is in a different cycle of τ. Let $\sigma = \Phi(\tau) \in \mathrm{PAut}(C_{0,3}) \subseteq \mathrm{Sym}(32)$, where $C_{0,3} = \Phi(\mathscr{C}_{0,3})$. Thus, by Proposition

2, $S = \{\sigma, \sigma^2, \sigma^3, \sigma^4\}$ is a 3-PD-set of size 4 for $C_{0,3}$ with information set $I = \{1,2,3,4,9,10\}$. Note that $C_{0,3}$ is the smallest Hadamard $\mathbb{Z}_4$-linear code that is a binary nonlinear code.

3 s-PD-sets for Hadamard $\mathbb{Z}_4$-linear codes

Let $\mathbf{0}, \mathbf{1}, \mathbf{2}$ and $\mathbf{3}$ be the repetition of symbol 0, 1, 2 and 3, respectively. Let $\mathscr{G}_{\gamma,\delta}$ be a generator matrix of the $\mathbb{Z}_2\mathbb{Z}_4$-additive Hadamard code $\mathscr{C}_{\gamma,\delta}$ of length $\beta = 2^{m-1}$ and type $(0,\beta;\gamma,\delta)$, where $m = \gamma + 2\delta - 1$. A generator matrix for the $\mathbb{Z}_2\mathbb{Z}_4$-additive Hadamard code $\mathscr{C}_{\gamma+1,\delta}$ of length $\beta' = 2\beta = 2^m$ and type $(0,\beta';\gamma+1,\delta)$ can be constructed as follows [7]:

$$\mathscr{G}_{\gamma+1,\delta} = \begin{pmatrix} \mathbf{0} & \mathbf{2} \\ \mathscr{G}_{\gamma,\delta} & \mathscr{G}_{\gamma,\delta} \end{pmatrix}. \tag{3}$$

Equivalently, a generator matrix for the $\mathbb{Z}_2\mathbb{Z}_4$-additive Hadamard code $\mathscr{C}_{\gamma,\delta+1}$ of length $\beta'' = 4\beta = 2^{m+1}$ and type $(0,\beta'';\gamma,\delta+1)$ can be constructed as [7]:

$$\mathscr{G}_{\gamma,\delta+1} = \begin{pmatrix} \mathscr{G}_{\gamma,\delta} & \mathscr{G}_{\gamma,\delta} & \mathscr{G}_{\gamma,\delta} & \mathscr{G}_{\gamma,\delta} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \end{pmatrix}. \tag{4}$$

Note that a generator matrix for every code $\mathscr{C}_{\gamma,\delta}$ can be obtained by applying (3) and (4) recursively over the generator matrix $\mathscr{G}_{0,1} = (1)$ of the code $\mathscr{C}_{0,1}$. From now on, we assume that $\mathscr{C}_{\gamma,\delta}$ is obtained by using these constructions.

Proposition 4. *Let $\mathscr{C}_{\gamma,\delta}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive Hadamard code of type $(0,\beta;\gamma,\delta)$ with quaternary information set $\mathscr{I}$. The set $\mathscr{I} \cup \{\beta+1\}$ is a suitable quaternary information set for both codes $\mathscr{C}_{\gamma+1,\delta}$ and $\mathscr{C}_{\gamma,\delta+1}$ obtained from $\mathscr{C}_{\gamma,\delta}$ by applying constructions (3) and (4), respectively.*

Despite the fact that the quaternary information set is the same for $\mathscr{C}_{\gamma+1,\delta}$ and $\mathscr{C}_{\gamma,\delta+1}$, the information set for the corresponding binary codes $C_{\gamma+1,\delta}$ and $C_{\gamma,\delta+1}$ are $I' = \Phi(\mathscr{I}) \cup \{2\beta+1\}$ and $I'' = \Phi(\mathscr{I}) \cup \{2\beta+1, 2\beta+2\}$, respectively.

Given two permutations $\sigma_1 \in \mathrm{Sym}(n_1)$ and $\sigma_2 \in \mathrm{Sym}(n_2)$, we define the permutation $(\sigma_1|\sigma_2) \in \mathrm{Sym}(n_1+n_2)$, where σ_1 acts on the coordinates $\{1,\ldots,n_1\}$ and σ_2 acts on the coordinates $\{n_1+1,\ldots,n_1+n_2\}$. Given $\sigma_i \in \mathrm{Sym}(n_i)$, $i \in \{1,\ldots,4\}$, we define the permutation $(\sigma_1|\sigma_2|\sigma_3|\sigma_4)$ in the same way.

Proposition 5. *Let S be an s-PD-set of size l for the Hadamard $\mathbb{Z}_4$-linear code $C_{\gamma,\delta}$ of binary length $n = 2\beta$ and type $(0,\beta;\gamma,\delta)$ with respect to an information set I. Then the set $(S|S) = \{(\sigma|\sigma) : \sigma \in S\}$ is an s-PD-set of size l with respect to the information set $I' = I \cup \{n+1\}$ for the Hadamard $\mathbb{Z}_4$-linear code $C_{\gamma+1,\delta}$ of binary length $2n$ and type $(0,2\beta;\gamma+1,\delta)$ constructed from (3) and the Gray map.*

Example 6. *Let S be the 3-PD-set of size 4 for $C_{0,3}$ of binary length 32 with respect to the information set $I = \{1,2,3,4,9,10\}$, given in Example* 3*. By Propositions* 4 *and* 5*, the set $(S|S)$ is a 3-PD-set of size 4 for the Hadamard $\mathbb{Z}_4$-linear code $C_{1,3}$ of binary length 64 with respect to the information set $I' = \{1,2,3,4,9,10,33\}$.*

Proposition 5 can not be generalized directly for Hadamard $\mathbb{Z}_4$-linear codes $C_{\gamma,\delta+1}$ constructed from (4). Note that if S is an s-PD-set for the Hadamard $\mathbb{Z}_4$-linear code $C_{\gamma,\delta}$, then the set $(S|S|S|S) = \{(\sigma|\sigma|\sigma|\sigma) : \sigma \in S\}$ is not in general an s-PD-set for the Hadamard $\mathbb{Z}_4$-linear code $C_{\gamma,\delta+1}$.

Proposition 7. *Let $\mathscr{S} \subseteq \mathrm{PAut}(\mathscr{C}_{\gamma,\delta})$ such that $\Phi(\mathscr{S})$ is an s-PD-set of size l for the Hadamard $\mathbb{Z}_4$-linear code $C_{\gamma,\delta}$ of binary length $n = 2\beta$ and type $(0,\beta;\gamma,\delta)$ with respect to an information set I. Then the set $\Phi((\mathscr{S}|\mathscr{S}|\mathscr{S}|\mathscr{S})) = \{\Phi((\tau|\tau|\tau|\tau)) : \tau \in \mathscr{S}\}$ is an s-PD-set of size l with respect to the information set $I'' = I \cup \{n+1, n+2\}$ for the Hadamard $\mathbb{Z}_4$-linear code $C_{\gamma,\delta+1}$ of binary length $4n$ and type $(0,4\beta;\gamma,\delta+1)$ constructed from (4) and the Gray map.*

Example 8. *Let $\mathscr{S} = \{\tau,\tau^2,\tau^3,\tau^4\}$, where τ is defined as in Example 3. By Proposition 7, the set $\Phi((\mathscr{S}|\mathscr{S}|\mathscr{S}|\mathscr{S}))$ is a 3-PD-set of size 4 for the Hadamard $\mathbb{Z}_4$-linear code $C_{0,4}$ of binary length 128 with respect to the information set $I' = \{1,2,3,4,9,10,33,34\}$.*

Propositions 5 and 7 can be applied recursively to acquire s-PD-sets for the infinite family of Hadamard $\mathbb{Z}_4$-linear codes obtained (by using constructions (3) and (4)) from a given Hadamard $\mathbb{Z}_4$-linear code where we already have such set.

References

[1] R. Barrolleta and M. Villanueva, "Partial permutation decoding for binary linear Hadamard codes," *Electronic Notes in Discrete Mathematics*, 46 (2014) 35-42.

[2] J. J. Bernal, J. Borges, C. Fernández-Córboda, and M. Villanueva, "Permutation decoding of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes," *Des. Codes and Cryptogr.*, DOI 10.1007/s10623-014-9946-4, 2014.

[3] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. Villanueva, "$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality," *Des. Codes and Cryptogr.*, vol. 54: 167–179, 2010.

[4] W. Fish, J. D. Key, and E. Mwambene, "Partial permutation decoding for simplex codes," *Advances in Mathematics of Comunications*, vol. 6(4): 505–516, 2012.

[5] W. C. Huffman, *Codes and groups, Handbook of coding theory*, 1998.

[6] D. S. Krotov and M. Villanueva "Classification of the $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes and their automorphism groups," *IEEE Trans. Inf. Theory*, vol. 61(2): 887–894, 2015.

[7] D. S. Krotov, "$\mathbb{Z}_4$-linear Hadamard and extended perfect codes," *Electronic Notes in Discrete Mathematics*, vol. 6 (2001), 107-112.

[8] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 1977.

[9] J. Pernas, J. Pujol and M. Villanueva. "Characterization of the automorphism group of quaternary linear Hadamard Codes," *Des. Codes Cryptogr.*, 70(1-2), 105–115, 2014.