Post-print of:Barrolleta, RD and Villanueva, M. "PD-sets for Z4-linear codes: Hadamard and Kerdock codes" in 2016 IEEE International Symposium on Information Theory (Aug. 2016), p. 1317-1321. DOI 10.1109/ISIT.2016.7541512

PD-sets for Z_4-linear codes: Hadamard and Kerdock codes

Roland D. Barrolleta and Mercè Villanueva
Department of Information and Communications Engineering
Universitat Autònoma de Barcelona
08193-Cerdanyola del Vallès, Spain
Email: {rolanddavid.barrolleta, merce.villanueva}@uab.cat

***Abstract*—Permutation decoding is a technique that strongly depends on the existence of a special subset, called PD-set, of the permutation automorphism group of a code. In this paper, a general criterion to obtain s-PD-sets of size $s+1$, which enable correction up to s errors, for Z_4-linear codes is provided. Furthermore, some explicit constructions of s-PD-sets of size $s+1$ for important families of (nonlinear) Z_4-linear codes such as Hadamard and Kerdock codes are given.**

I. Introduction

Let $\mathbb{Z}_2$ and $\mathbb{Z}_4$ be the rings of integers modulo 2 and modulo 4, respectively. Let $\mathbb{Z}_2^n$ denote the set of all binary vectors of length n and let $\mathbb{Z}_4^n$ be the set of all n-tuples over the ring $\mathbb{Z}_4$. 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 $\mathcal{C}$ 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 $y = (y_1,\ldots,y_n) \in \mathbb{Z}_4^n$. Let $\mathcal{C}$ be a quaternary linear code. Then, the binary code $C = \Phi(\mathcal{C})$ is said to be a $\mathbb{Z}_4$*-linear code*. Moreover, since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$, it is isomorphic to an abelian group $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ and we say that $\mathcal{C}$ (or equivalently, the corresponding $\mathbb{Z}_4$-linear code $C = \Phi(\mathcal{C})$) is of type $2^\gamma 4^\delta$ [6].

Let C be a binary code of length n. For a vector $v \in \mathbb{Z}_2^n$ and a set $I \subseteq \{1,\ldots,n\}$, $|I| = k$, we denote the restriction of v to the coordinates in I by $v_I \in \mathbb{Z}_2^k$ and the set $\{v_I : v \in C\}$ by C_I. If $|C| = 2^k$, a set $I \subseteq \{1,\ldots,n\}$ of k coordinate positions such that $|C_I| = 2^k$ is called an *information set* for C. If such a set I exists, then C is said to be a *systematic code*. In [3], it is shown that $\mathbb{Z}_4$-linear codes are systematic, and a systematic encoding is given for these codes.

Let $\mathrm{Sym}(n)$ be the symmetric group of permutations on the set $\{1,\ldots,n\}$ and let $\mathrm{id} \in \mathrm{Sym}(n)$ be the identity permutation. The group operation in $\mathrm{Sym}(n)$ is the function composition, $\sigma_1\sigma_2$, which maps any element x to $\sigma_1(\sigma_2(x))$, $\sigma_1,\sigma_2 \in \mathrm{Sym}(n)$. A $\sigma \in \mathrm{Sym}(n)$ acts linearly on words of $\mathbb{Z}_2^n$ or $\mathbb{Z}_4^n$ by permuting their coordinates as follows: $\sigma((v_1,\ldots,v_n)) = (v_{\sigma^{-1}(1)},\ldots,v_{\sigma^{-1}(n)})$. The *permutation automorphism group* of $\mathcal{C}$ or $C = \Phi(\mathcal{C})$, denoted by $\mathrm{PAut}(\mathcal{C})$ or $\mathrm{PAut}(C)$, respectively, is the group generated by all permutations that preserve the set of codewords.

Permutation decoding is a technique introduced in [9] by MacWilliams for linear codes that involves finding a subset of the permutation automorphism group of a code in order to assist in decoding. A new permutation decoding method for $\mathbb{Z}_4$-linear codes (not necessarily linear) was introduced in [3]. In general, the method works as follows. Given a systematic t-error-correcting code C with information set I, we denote the received vector by $y = x + e$, where $x \in C$ and e is the error vector. Suppose that at most t errors occur. Permutation decoding consists of moving all errors in y out of I, by using an automorphism of C. This technique is strongly based on the existence of a special subset of $\mathrm{PAut}(C)$. Specifically, a subset $S \subseteq \mathrm{PAut}(C)$ is said to be an s-PD-*set* for the code C if every s-set of coordinate positions is moved out of I by at least one element of S, where $1 \leq s \leq t$. When $s = t$, S is said to be a PD-*set*.

A *binary Hadamard code* of length n is a binary code with $2n$ codewords and minimum distance $n/2$. It is well-known that there is a unique binary linear Hadamard code H_m of length $n = 2^m$, $m \geq 2$, which is the dual of the extended Hamming code of length $2^m - 1$ [10]. The quaternary linear codes that, under the Gray map, give a binary Hadamard code are called *quaternary linear Hadamard codes* and the corresponding $\mathbb{Z}_4$-linear codes are called $\mathbb{Z}_4$*-linear Hadamard codes*. For any $m \geq 3$ and each $\delta \in \{1,\ldots,\lfloor \frac{m+1}{2} \rfloor\}$, there is a unique (up to equivalence) $\mathbb{Z}_4$-linear Hadamard code of length 2^m, which is the Gray map image of a quaternary linear code of length $\beta = 2^{m-1}$ and type $2^\gamma 4^\delta$, where $m = \gamma+2\delta-1$. It is known that the $\mathbb{Z}_4$-linear Hadamard codes are nonlinear if and only if $\delta \geq 3$ [8]. These codes have been studied and classified in [8], [13], and their permutation automorphism groups have been characterized in [7], [12].

A *binary Kerdock code* of length $n = 2^{m+1}$ is the Gray map image of a quaternary Kerdock code $\mathcal{K}(m)$, which is a quaternary linear code of length 2^m, type 4^{m+1} and minimum Lee distance $2^m - 2^{\lfloor m/2 \rfloor}$. For $m \geq 2$, it is well known that these $\mathbb{Z}_4$-linear Kerdock codes are nonlinear and better than any linear code with the same parameters [6].

This work has been partially supported by the Spanish MINECO under Grant TIN2013-40524-P and by the Catalan AGAUR under Grant 2014SGR-691.

In [5], it is shown how to find s-PD-sets of minimum size $s+1$ that satisfy the Gordon-Schönheim bound for partial permutation decoding for the binary simplex code of length 2^m-1 for all $m \geq 4$ and $1 < s \leq \lfloor \frac{2^m-m-1}{m} \rfloor$. In [1], [2], following the same technique, similar results for binary linear and $\mathbb{Z}_4$-linear Hadamard codes are established. Specifically, for the binary linear Hadamard code H_m of length 2^m, $m \geq 4$, s-PD-sets of size $s+1$ for all $1 < s \leq \lfloor \frac{2^m-m-1}{m+1} \rfloor$ are given. For the $\mathbb{Z}_4$-linear Hadamard codes, the permutation automorphism group $\mathrm{PAut}(\mathcal{H}_{\gamma,\delta})$ of a quaternary linear Hadamard code $\mathcal{H}_{\gamma,\delta}$ of length $\beta = 2^{m-1}$ and type $2^\gamma 4^\delta$ is regarded as a certain subset of $\mathrm{GL}(\gamma+\delta, \mathbb{Z}_4)$. Then the question of whether a subset $\mathcal{S} \subseteq \mathrm{PAut}(\mathcal{H}_{\gamma,\delta})$ leads to a valid s-PD-set of size $s+1$ for the $\mathbb{Z}_4$-linear Hadamard code $H_{\gamma,\delta} = \Phi(\mathcal{H}_{\gamma,\delta})$ is addressed by searching for a set of invertible matrices from $\mathrm{GL}(\gamma+\delta, \mathbb{Z}_4)$ fulfilling certain conditions. Finally, for the code $H_{\gamma,\delta}$, s-PD-sets of size $s+1$ for all $\delta \geq 3$ and $1 < s \leq \left\lfloor \frac{2^{2\delta-2}-\delta}{\delta} \right\rfloor$ are constructed. In this paper, we obtain new s-PD-sets of size $s+1$ for $H_{\gamma,\delta}$. These sets are generated by a permutation, unlike the s-PD-sets given in [2].

This correspondence is organized as follows. In Section II, we introduce the main theorem that states sufficient conditions for a permutation $\sigma \in \mathrm{PAut}(C)$ to generate an s-PD-set $S = \{\sigma^i \,:\, 1 \leq i \leq s+1\}$ of size $s+1$ for a $\mathbb{Z}_4$-linear code C. In Section III, by using the main theorem, we obtain s-PD-sets of size $s+1$ for the $\mathbb{Z}_4$-linear Hadamard code $\mathcal{H}_{\gamma,\delta}$ for all $\delta \geq 4$ and $1 < s \leq 2^\delta - 3$. Finally, in Section IV, we obtain s-PD-sets of size $s+1$, for all $m \geq 4$ and $1 < s \leq \lambda - 1$, for the binary Kerdock code of length 2^{m+1} such that $2^m - 1$ is not prime, where λ is the greatest divisor of 2^m-1 satisfying $\lambda \leq 2^m/(m+1)$.

II. s-PD-SETS OF SIZE $s+1$ FOR $\mathbb{Z}_4$-LINEAR CODES

Let $\mathcal{C}$ be a quaternary linear code of length β and type $2^\gamma 4^\delta$, and let $C = \Phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_4$-linear code of length 2β. Let $\Phi : \mathrm{Sym}(\beta) \to \mathrm{Sym}(2\beta)$ be the map defined as

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

for all $\tau \in \mathrm{Sym}(\beta)$ and $i \in \{1, \ldots, 2\beta\}$. Given a subset $\mathcal{S} \subseteq \mathrm{Sym}(\beta)$, we define the set $\Phi(\mathcal{S}) = \{\Phi(\tau) : \tau \in \mathcal{S}\} \subseteq \mathrm{Sym}(2\beta)$. It is easy to see that if $\mathcal{S} \subseteq \mathrm{PAut}(\mathcal{C}) \subseteq \mathrm{Sym}(\beta)$, then $\Phi(\mathcal{S}) \subseteq \mathrm{PAut}(C) \subseteq \mathrm{Sym}(2\beta)$.

Lemma 2.1: The map $\Phi : \mathrm{Sym}(\beta) \to \mathrm{Sym}(2\beta)$ is a group monomorphism.

An ordered set $\mathcal{I} = \{i_1, \ldots, i_{\gamma+\delta}\} \subseteq \{1, \ldots, \beta\}$ of $\gamma+\delta$ coordinate positions is said to be a *quaternary information set* for a quaternary linear code $\mathcal{C}$ of type $2^\gamma 4^\delta$ if $|\mathcal{C}_\mathcal{I}| = 2^\gamma 4^\delta$. If the elements of $\mathcal{I}$ are ordered in such a way that $|\mathcal{C}_{\{i_1,\ldots,i_\delta\}}| = 4^\delta$, then it is easy to see that the set $\Phi(\mathcal{I})$, defined as

$$\Phi(\mathcal{I}) = \{2i_1-1, 2i_1, \ldots, 2i_\delta-1, 2i_\delta, 2i_{\delta+1}-1, \ldots, 2i_{\delta+\gamma}-1\},$$

is an information set for $C = \Phi(\mathcal{C})$.

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, $S = \{\sigma_0, \ldots, \sigma_s\}$, such that $S_i = \{\sigma_0, \ldots, \sigma_i\} \subseteq S$ is an i-PD-set of size $i+1$ for all $i \in \{0, \ldots, s\}$. Note that $S_i \subset S_j$ if $0 \leq i < j \leq s$ and $S_s = S$.

Theorem 2.2: Let $\mathcal{C}$ be a quaternary linear code of length β and type $2^\gamma 4^\delta$ with quaternary information set $\mathcal{I}$ and let s be a positive integer. If $\tau \in \mathrm{PAut}(\mathcal{C})$ 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 $C = \Phi(\mathcal{C})$ with information set $\Phi(\mathcal{I})$. Moreover, any ordering of the elements of S gives a nested r-PD-set for any $r \in \{1, \ldots, s\}$.

Proof: The permutation $\tau \in \mathrm{PAut}(\mathcal{C})$ can be written as

$$\begin{aligned} \tau = \quad & (i_1, x_2, \ldots, x_{(s+1)})(i_2, x_{(s+1)+2}, \ldots, x_{2(s+1)}) \cdots \\ & (i_{\gamma+\delta}, x_{(\gamma+\delta-1)(s+1)+2}, \ldots, x_{(\gamma+\delta)(s+1)})\tau', \end{aligned} \tag{1}$$

where $\mathcal{I} = \{i_1, \ldots, i_{\gamma+\delta}\}$ is the quaternary information set for $\mathcal{C}$ and $\tau' \in \mathrm{Sym}(\beta)$. We consider the elements of $\mathcal{I}$ ordered in such a way that $|\mathcal{C}_{\{i_1,\ldots,i_\delta\}}| = 4^\delta$. Note that each cycle $(i_\epsilon, x_{(\epsilon-1)(s+1)+2}, \ldots, x_{\epsilon(s+1)})$, $\epsilon \in \{1, \ldots, \gamma+\delta\}$, of $\tau \in \mathrm{PAut}(\mathcal{C})$ splits into two disjoint cycles of the same length via Φ, that is,

$$\begin{aligned} & \Phi((i_\epsilon, x_{(\epsilon-1)(s+1)+2}, \ldots, x_{\epsilon(s+1)})) = \\ & (2i_\epsilon - 1, 2x_{(\epsilon-1)(s+1)+2} - 1, \ldots, 2x_{\epsilon(s+1)} - 1) \\ & (2i_\epsilon, 2x_{(\epsilon-1)(s+1)+2}, \ldots, 2x_{\epsilon(s+1)}). \end{aligned}$$

Furthermore, the information positions of the set $I = \Phi(\mathcal{I})$ are also placed in different cycles of length $s+1$ of the permutation $\sigma = \Phi(\tau)$. There is again one information position per cycle of length $s+1$, with the exception of the cycles of the form $(2i_\epsilon, 2x_{(\epsilon-1)(s+1)+2} - 1, \ldots, 2x_{\epsilon(s+1)})$ for all $\epsilon \in \{\delta+1, \ldots, \gamma+\delta\}$.

Let $S = \{\sigma^i\}_{i=1}^{s+1}$ and let $P = \{1, \ldots, 2\beta\}$ be the set of all coordinate positions. We define the set $A_i = \{j \in P : \sigma^i(j) \in I\}$ for each $i \in \{1, \ldots, s+1\}$. Note that $|A_i| = \gamma + 2\delta$ and $A_i \cap A_j = \emptyset$ for all $i, j \in \{1, \ldots, s+1\}$, $i \neq j$. We have to prove that every s-set of coordinate positions, denoted by $J = \{j_1, \ldots, j_s\} \subseteq P$, is moved out of I by at least one element of S. Note that a coordinate position in J cannot be in two different sets A_i, $i \in \{1, \ldots, s+1\}$. In the worst-case scenario, for each $k \in \{1, \ldots, s\}$, $j_k \in A_{l_k}$ for some $l_k \in \{1, \ldots, s+1\}$. However, since $|J| = s$ and $|S| = s+1$, we can always assure that there is $\varphi \in S$ such that $\varphi(J) \cap I = \emptyset$. Thus, by Lemma 2.1, $S = \{\Phi(\tau)^i\}_{i=1}^{s+1} = \{\Phi(\tau^i)\}_{i=1}^{s+1}$ is an s-PD-set of size $s+1$ for the $\mathbb{Z}_4$-linear code $C = \Phi(\mathcal{C})$ with information set $I = \Phi(\mathcal{I})$. ■

Corollary 2.3: Let S be an s-PD-set of size $s+1$ for a $\mathbb{Z}_4$-linear code $C = \Phi(\mathcal{C})$ of length 2β and type $2^\gamma 4^\delta$ as in Theorem 2.2. Then $s+1$ divides the order of $\mathrm{PAut}(\mathcal{C})$ and $s \leq f_\mathcal{C}$, where $f_\mathcal{C} = \lfloor (\beta - \gamma - \delta)/(\gamma+\delta) \rfloor$.

Let $\mathcal{H}_{\gamma,\delta}$ be the quaternary linear Hadamard code of length $\beta = 2^{m-1}$ and type $2^\gamma 4^\delta$, where $m = \gamma + 2\delta - 1$. Let $H_{\gamma,\delta} = \Phi(\mathcal{H}_{\gamma,\delta})$ be the corresponding $\mathbb{Z}_4$-linear code of length $2\beta =$

2^m. A generator matrix $\mathcal{G}_{\gamma,\delta}$ for $\mathcal{H}_{\gamma,\delta}$ can be constructed by using the following recursive constructions:

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

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

starting from $\mathcal{G}_{0,1} = (1)$. First, the matrix $\mathcal{G}_{0,\delta}$ is obtained from $\mathcal{G}_{0,1}$ by using recursively $\delta - 1$ times construction (3), and then $\mathcal{G}_{\gamma,\delta}$ is constructed from $\mathcal{G}_{0,\delta}$ by using γ times construction (2).

It is known that if $S = \Phi(\mathcal{S})$, $\mathcal{S} \subseteq \mathrm{PAut}(\mathcal{H}_{\gamma,\delta})$, is an s-PD-set of size $s+1$ for $H_{\gamma,\delta}$, then $s \leq f_{\gamma,\delta}$, where $f_{\gamma,\delta} = \lfloor (2^{\gamma+2\delta-2} - \gamma - \delta)/(\gamma+\delta) \rfloor$. Furthermore, if $S \subseteq \mathrm{PAut}(H_{\gamma,\delta})$ is an s-PD-set of size $s+1$ for $H_{\gamma,\delta}$, then $s \leq f_m$, where $f_m = \lfloor (2^m - m - 1)/(1+m) \rfloor$ [2]. Note that $f_{\gamma,\delta} \leq f_m$, where $m = \gamma + 2\delta - 1$. Moreover, $f_{\mathcal{H}_{\gamma,\delta}} = f_{\gamma,\delta}$ despite the fact that $f_{\mathcal{H}_{\gamma,\delta}}$ takes into account the restrictions given by Theorem 2.2. In practice, to require that $s+1$ divides $|\mathrm{PAut}(\mathcal{H}_{\gamma,\delta})|$ is more restrictive than the condition $s \leq f_{\mathcal{H}_{\gamma,\delta}}$, as we can see in the following example.

Example 1: Let $\mathcal{H}_{0,3}$ be the quaternary linear Hadamard code of length 16 and type $2^0 4^3$ with generator matrix $\mathcal{G}_{0,3} =$

$$\begin{pmatrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3 \\ 0&0&0&0&1&1&1&1&2&2&2&2&3&3&3&3 \end{pmatrix}$$

obtained by applying (3) two times starting from $\mathcal{G}_{0,1} = (1)$. Let $\tau = (1,16,11,6)(2,7,12,13)(3,14,9,8)(4,5,10,15) \in \mathrm{PAut}(\mathcal{H}_{0,3}) \subseteq \mathrm{Sym}(16)$ [12]. Note that τ has four disjoint cycles of length four. It is easy to see that $\mathcal{I} = \{1,2,5\}$ is a quaternary information set for $\mathcal{H}_{0,3}$ [2]. Moreover, note that each quaternary information position in $\mathcal{I}$ is in a different cycle of τ. Let $\sigma = \Phi(\tau) \in \mathrm{PAut}(H_{0,3}) \subseteq \mathrm{Sym}(32)$, where $H_{0,3} = \Phi(\mathcal{H}_{0,3})$. Thus, by Lemma 2.1 and Theorem 2.2, $S = \{\sigma, \sigma^2, \sigma^3, \sigma^4\} \subseteq \mathrm{PAut}(H_{0,3})$ is a 3-PD-set of size 4 for the $\mathbb{Z}_4$-linear Hadamard code $H_{0,3}$ with information set $\Phi(\mathcal{I}) = \{1,2,3,4,9,10\}$. Note that $H_{0,3}$ is the smallest $\mathbb{Z}_4$-linear Hadamard code which is nonlinear.

We have that $f_5 = f_{0,3} = 4$. In [2], a 4-PD-set of size 5 for $H_{0,3}$ is found. Moreover, it is enough to consider permutations in the subgroup $\Phi(\mathrm{PAut}(\mathcal{H}_{0,3})) \leq \mathrm{PAut}(H_{0,3})$ to achieve f_5. However, note that this 4-PD-set can not be generated by a permutation $\sigma \in \mathrm{PAut}(H_{0,3})$. By using Theorem 2.2, it is not possible to obtain 4-PD-sets of size 5, since 5 does not divide $|\mathrm{PAut}(\mathcal{H}_{0,3})| = 2^9 \cdot 3$ [12].

Example 2: Let $\mathcal{H}_{1,3}$ be the quaternary linear Hadamard code of length 32 and type $2^1 4^3$ with generator matrix

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

obtained by applying construction (2) over the matrix $\mathcal{G}_{0,3}$ given in Example 1. Let $\tau \in \mathrm{PAut}(\mathcal{H}_{1,3}) \subseteq \mathrm{Sym}(32)$ be

$$\begin{aligned} \tau = \; & (1,24,26,15,3,22,28,13)(2,23,27,14,4,21,25,16) \\ & (5,11,32,20,7,9,30,18)(6,10,29,19,8,12,31,17), \end{aligned}$$

which has four disjoint cycles of length eight. It is also easy to see that $\mathcal{I} = \{1,2,5,17\}$ is a quaternary information set for $\mathcal{H}_{1,3}$ [2], and each quaternary information position in $\mathcal{I}$ is in a different cycle of τ. Let $\sigma = \Phi(\tau) \in \mathrm{PAut}(H_{1,3}) \subseteq \mathrm{Sym}(64)$, where $H_{1,3} = \Phi(\mathcal{H}_{1,3})$. Thus, by Lemma 2.1 and Theorem 2.2, $S = \{\sigma^i\}_{i=1}^{8}$ is a 7-PD-set of size 8 for the $\mathbb{Z}_4$-linear Hadamard code $H_{1,3}$ with information set $\Phi(\mathcal{I}) = \{1,2,3,4,9,10,33\}$. Note that $H_{1,3}$ is a binary nonlinear code.

Since $f_{1,3} = 7$, in this case, no better s-PD-sets of size $s+1$ can be found by using permutations in the subgroup $\Phi(\mathrm{PAut}(\mathcal{H}_{1,3})) \leq \mathrm{PAut}(H_{1,3})$. However, an 8-PD-set of size 9 could be theoretically found in $\mathrm{PAut}(H_{1,3})$ since $f_6 = 8$.

III. Construction of s-PD-sets of size $s+1$ for $\mathbb{Z}_4$-linear Hadamard codes

In this section, we give a construction of s-PD-sets of size $s+1$ for $\mathbb{Z}_4$-linear Hadamard codes $H_{\gamma,\delta}$, by finding a permutation $\tau \in \mathrm{PAut}(\mathcal{H}_{0,\delta})$ that satisfies the conditions of Theorem 2.2. Note that high order permutations are more suitable candidates to obtain better s-PD-sets.

The permutation automorphism group $\mathrm{PAut}(\mathcal{H}_{0,\delta})$ of $\mathcal{H}_{0,\delta}$ is isomorphic to the following set of matrices over $\mathbb{Z}_4$:

$$\left\{ \begin{pmatrix} 1 & \eta \\ \mathbf{0} & A \end{pmatrix} : A \in \mathrm{GL}(\delta-1, \mathbb{Z}_4),\ \eta \in \mathbb{Z}_4^{\delta-1} \right\}$$

[2]. Let $\mathrm{ord}(A)$ be the order of $A \in \mathrm{GL}(\delta-1, \mathbb{Z}_4)$. It is known that $\max\{\mathrm{ord}(A) : A \in \mathrm{GL}(\delta-1, \mathbb{Z}_4)\} = 2(2^{\delta-1}-1)$ [11]. Moreover, if $\eta = \mathbf{0}$, then

$$\mathrm{ord}(\begin{pmatrix} 1 & \eta \\ \mathbf{0} & A \end{pmatrix}) = \mathrm{ord}(A).$$

Thus, our aim is to obtain matrices A of order $2(2^{\delta-1}-1)$. Although we can characterize when a matrix $\mathcal{M} \in \mathrm{PAut}(\mathcal{H}_{0,\delta})$ has maximum order, we do not know its cyclic structure, regarded as a permutation $\tau \in \mathrm{Sym}(\beta)$. Recall that, in order to apply Theorem 2.2, we need a permutation $\tau \in \mathrm{PAut}(\mathcal{H}_{0,\delta}) \subseteq \mathrm{Sym}(\beta)$ with at least δ disjoint cycles of the same length. Next, we show how some known results on maximum length sequences over $\mathbb{Z}_4$ can be used to solve this question.

Let $\mathbb{Z}_4[x]$ and $\mathbb{Z}_2[x]$ be the polynomial ring over $\mathbb{Z}_4$ and $\mathbb{Z}_2$, respectively. Let $\mu : \mathbb{Z}_4[x] \to \mathbb{Z}_2[x]$ be the map that performs a modulo 2 reduction of the coefficients of $f(x) \in \mathbb{Z}_4[x]$. A monic polynomial $f(x) \in \mathbb{Z}_4[x]$ is said to be a *primitive basic irreducible* polynomial if $\mu(f(x))$ is primitive over $\mathbb{Z}_2[x]$.

Let $f(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_1 x - a_0 \in \mathbb{Z}_4[x]$. Consider the kth-order homogeneous linear recurrence relation over $\mathbb{Z}_4$ with characteristic polynomial $f(x)$, that is,

$$s_{n+k} = a_{k-1}s_{n+k-1} + \cdots + a_1 s_{n+1} + a_0 s_n, \quad n = 0,1,\ldots \tag{4}$$

The *companion matrix* A_f of the polynomial $f(x)$ is the $k \times k$ matrix defined as

$$A_f = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{k-1} \end{pmatrix}. \tag{5}$$

The set of all nonzero sequences $\{s_n\}_{n=0}^{\infty}$ over $\mathbb{Z}_4$ satisfying (4) whose characteristic polynomial $f(x)$ is a primitive basic irreducible polynomial dividing $x^{2(2^k-1)}-1$ in $\mathbb{Z}_4[x]$ is called Family $\mathcal{B}$ in [14]. It is known that there are $2^{k-1}+1$ cyclically distinct periodic sequences in each Family $\mathcal{B}$: 2^{k-1} of them with common least period $2(2^k-1)$ and one with period 2^k-1 [4]. Moreover, the sequence with period 2^k-1 is the unique containing only zero-divisors. Examples of primitive basic irreducible polynomials $f(x) \in \mathbb{Z}_4[x]$ suitable for constructing sequences of Family $\mathcal{B}$ for degrees 3 to 10 can be found in [4], [14].

Let $\{s_n\}_{n=0}^{\infty}$ be a nonzero sequence over $\mathbb{Z}_4$ satisfying (4). For each $n \geq 0$, we define the tuple $\mathbf{s}_n = (s_n, \dots, s_{n+k-1})$ over $\mathbb{Z}_4$. In the language of feedback shift registers, $\mathbf{s}_n$ is called the *n-state vector.* Note that if A_f is the companion matrix of the polynomial $f(x)$ associated with (4), then it holds that $\mathbf{s}_n = \mathbf{s}_0 A_f^n$. Let $\overline{\mathcal{G}_{0,\delta}}$ denote the generator matrix $\mathcal{G}_{0,\delta}$ without the first row, $(1,\dots,1)$. Note that each state vector represents a column vector of $\overline{\mathcal{G}_{0,\delta}}$. Moreover, we can label the ith coordinate position of $\mathcal{H}_{0,\delta}$, with the ith column vector w_i of $\overline{\mathcal{G}_{0,\delta}}$. Thus, any matrix A_f can be seen as a permutation of coordinate positions $\tau \in \mathrm{Sym}(\beta)$, such that $\tau(i) = j$ as long as $w_j = w_i A_f$. Furthermore, the ordered set of all different state vectors $\mathbf{s}_0, \mathbf{s}_0 A_f, \dots$ from the same sequence $\{s_n\}_{n=0}^{\infty}$ over $\mathbb{Z}_4$ represents a disjoint cycle τ_i of the permutation $\tau \in \mathrm{Sym}(\beta)$ associated with $A_f \in \mathrm{GL}(\delta-1, \mathbb{Z}_4)$. Finally, we have that $\mathrm{ord}(A_f) = \mathrm{ord}(\tau) = \mathrm{lcm}(\{\mathrm{ord}(\tau_i) : 1 \leq i \leq 2^{\delta-2}+1\}) = \mathrm{lcm}(\{2(2^{\delta-1}-1), 2^{\delta-1}-1\}) = 2(2^{\delta-1}-1)$.

Let $\mathcal{M}_f$ be the matrix

$$\mathcal{M}_f = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & A_f \end{pmatrix}.$$

It is clear that $\mathcal{M}_f \in \mathrm{PAut}(\mathcal{H}_{0,\delta})$ and its order is equal to the order of the matrix A_f. The matrix $\mathcal{M}_f$ will be denoted by τ_f if it is considered as an element in $\mathrm{Sym}(\beta)$. Then we have the following result:

Proposition 3.1: Let $f(x) = x^{\delta-1} - a_{\delta-2}x^{\delta-2} - \cdots - a_1 x - a_0 \in \mathbb{Z}_4[x]$ be a primitive basic irreducible polynomial dividing $x^{2(2^{\delta-1}-1)} - 1$ in $\mathbb{Z}_4[x]$ with $\delta \geq 4$. Let $\tau_f \in \mathrm{PAut}(\mathcal{H}_{0,\delta})$ be the permutation associated to $f(x)$. Then $\mathrm{ord}(\tau_f) = 2(2^{\delta-1}-1)$. Moreover, τ_f has $2^{\delta-2}+1$ disjoint cycles, where $2^{\delta-2}$ of them have length $2(2^{\delta-1}-1)$ and one of them has length $2^{\delta-1}-1$.

Corollary 3.2: Let $f(x) = x^{\delta-1} - a_{\delta-2}x^{\delta-2} - \cdots - a_1 x - a_0 \in \mathbb{Z}_4[x]$ be a primitive basic irreducible polynomial dividing $x^{\lambda}-1$ in $\mathbb{Z}_4[x]$, where $\lambda = 2(2^{\delta-1}-1)$ and $\delta \geq 4$. Let $\tau_f \in \mathrm{PAut}(\mathcal{H}_{0,\delta})$ be the permutation associated to $f(x)$. Let $\mathcal{I}$ be a quaternary information set for $\mathcal{H}_{0,\delta}$ with exactly one quaternary information position per cycle of length λ of τ_f. Then $S = \{\Phi(\tau_f^i)\}_{i=1}^{\lambda}$ is a $(\lambda-1)$-PD-set of size λ for $H_{0,\delta} = \Phi(\mathcal{H}_{0,\delta})$ with information set $\Phi(\mathcal{I})$.

Example 3: Consider the linear recurrence relation over $\mathbb{Z}_4$

$$s_{n+3} = 3s_{n+1} + 3s_n, \qquad n = 0, 1, \dots$$

Its characteristic polynomial is $f(x) = x^3 + x + 1 \in \mathbb{Z}_4[x]$. It is easy to see that $\mu(f(x)) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ is primitive over $\mathbb{Z}_2[x]$ and $f(x)$ divides $x^{14}-1$ over $\mathbb{Z}_4[x]$. Therefore, we have that the companion matrix of $f(x)$,

$$A_f = \begin{pmatrix} 0 & 0 & 3 \\ 1 & 0 & 3 \\ 0 & 1 & 0 \end{pmatrix},$$

has order 14 in $\mathrm{GL}(3, \mathbb{Z}_4)$. Since the matrix $\mathcal{M}_f$ leads to a valid permutation $\tau_f \in \mathrm{PAut}(\mathcal{H}_{0,4}) \in \mathrm{Sym}(64)$ that preserves the order of A_f, by Propisition 3.1, τ_f has also order 14. In addition, its cyclic structure behaves as follows: four disjoint cycles of length 14 and one cycle of length 7.

$$\begin{aligned} \tau_f = \; & (2,49,13,20,21,54,46,12,51,45,28,55,30,8) \\ & (3,33,9,35,41,43,11) \\ & (4,17,5,50,61,32,40,10,19,37,58,31,56,14) \\ & (6,34,57,47,60,63,64,48,44,59,15,52,29,24) \\ & (7,18,53,62,16,36,25,39,26,23,22,38,42,27). \end{aligned}$$

It is easy to check that $\mathcal{I} = \{2,5,6,18\}$ is a quaternary information set for $\mathcal{H}_{0,4}$ with generator matrix $\mathcal{G}_{0,4}$ obtained by applying (3) three times starting from $\mathcal{G}_{0,1} = (1)$. Note that each quaternary information position in $\mathcal{I}$ is in a different cycle of length 14 of τ_f. By Corollary 3.2, $S = \{\Phi(\tau_f^i)\}_{i=1}^{14}$ is a 13-PD-set of size 14 for the $\mathbb{Z}_4$-linear Hadamard code $H_{0,4}$ with information set $I = \Phi(I) = \{3,4,9,10,11,12,35,36\}$. In practice, it is not difficult to find such a set $\mathcal{I}$. For example, computations in MAGMA software package shows that there are 10752 suitable quaternary information sets.

In terms of state vectors, if we take $\mathbf{s}_0 = (0,0,1)$, we obtain the sequence 00103312012313001... over $\mathbb{Z}_4$. Note that $\mathbf{s}_1 = (0,1,0) = \mathbf{s}_0 A_f$. Since $\mathbf{s}_0$ and $\mathbf{s}_1$ are, respectively, the 17th and 5th column vectors of $\overline{\mathcal{G}_{0,4}}$, we obtain that $\tau_f(17) = 5$. All different state vectors of the previous sequence represent the cycle $(4,17,5,50,61,32,40,10,19,37,58,31,56,14)$ of τ_f.

Given two permutations $\sigma_1 \in \mathrm{Sym}(n_1)$ and $\sigma_2 \in \mathrm{Sym}(n_2)$, we define $(\sigma_1|\sigma_2) \in \mathrm{Sym}(n_1+n_2)$, where σ_1 acts on the coordinates $\{1,\dots,n_1\}$ and σ_2 on $\{n_1+1,\dots,n_1+n_2\}$. The following result can be found in [2] and provides a first approach to obtain s-PD-set of size $s+1$ for the $\mathbb{Z}_4$-linear Hadamard $H_{\gamma,\delta}$.

Proposition 3.3: [2] Let S be an s-PD-set of size l for $H_{\gamma,\delta}$ of length n and type $2^{\gamma}4^{\delta}$ with information set I. Then $(S|S) = \{(\sigma|\sigma) : \sigma \in S\}$ is an s-PD-set of size l for $H_{\gamma+1,\delta}$ of length $2n$ and type $2^{\gamma+1}4^{\delta}$ constructed from (2) and the Gray map, with any information set $I \cup \{i+n\}$, $i \in I$.

We proceed as follows: First, we compute an s-PD-set S of size $s+1$ for $H_{0,\delta}$, for example, by using Corollary 3.2. Then applying Proposition 3.3 recursively γ times over S, we obtain an s-PD-set of size $s+1$ for $H_{\gamma,\delta}$, with $\gamma > 0$.

Example 4: Let $\mathcal{H}_{1,4}$ be the quaternary linear Hadamard code of length 128 and type $2^1 4^4$ with generator matrix $\mathcal{G}_{1,4}$ obtained by applying (2) over the matrix $\mathcal{G}_{0,4}$ given in Example 3. Let $S \subseteq \mathrm{PAut}(H_{0,4})$ and $I \subseteq \{1,\dots,128\}$ as defined in the same example. Then $(S|S)$ is a 13-PD-set of size 14 for the $\mathbb{Z}_4$-linear Hadamard code $H_{1,4}$ with any information set of the form $I \cup \{128+i\}$, where $i \in I$, by Proposition 3.3.

m	2^m	ρ	λ	μ
4	16	3	3	5
6	64	9	9	7
8	256	28	17	15
9	512	51	7	73
10	1024	93	93	11
11	2046	170	89	23
12	4096	315	315	13

TABLE I
VALUES OF PARAMETERS ρ, λ AND μ FOR QUATERNARY KERDOCK CODES $\mathcal{K}(m)$ OF LENGTH 2^m WITH $m \in \{4,6,8,9,10,11,12\}$.

IV. CONSTRUCTION OF s-PD-SETS OF SIZE $s+1$ FOR BINARY KERDOCK CODES

Let $h(x)$ be a primitive basic irreducible polynomial of degree m over $\mathbb{Z}_4$ such that $h(x)$ divides $x^{2^m-1}-1$, and let $g(x)$ be the reciprocal polynomial to the polynomial $(x^{2^m-1}-1)/((x-1)h(x))$. Let $\mathcal{K}(m)^-$ be the quaternary cyclic code of length 2^m-1 with generator polynomial $g(x)$. The quaternary Kerdock code $\mathcal{K}(m)$ is the code obtained from $\mathcal{K}(m)^-$ by adding a zero-sum check symbol at the end of each codeword of $\mathcal{K}(m)^-$. Let $K(m)=\Phi(\mathcal{K}(m))$ be the corresponding binary Kerdock code of length 2^{m+1}, which has size 4^{m+1} and minimum distance $2^m-2^{\lfloor m/2\rfloor}$.

Since $\mathcal{K}(m)^-$ is a cyclic code of length 2^m-1, it is clear that $(1,\dots,2^m-1)\in \mathrm{PAut}(\mathcal{K}(m)^-)$. Therefore, by definition of $\mathcal{K}(m)$, we also have that $(1,\dots,2^m-1)\in \mathrm{PAut}(\mathcal{K}(m))$.

Corollary 4.1: Let $\mathcal{K}(m)$ be the quaternary Kerdock code of length 2^m and type 4^{m+1} such that 2^m-1 is not a prime number. Let $\nu=(1,\dots,2^m-1)\in \mathrm{PAut}(\mathcal{K}(m))\subseteq \mathrm{Sym}(2^m)$. Let λ be the greatest divisor of 2^m-1 such that $\lambda\le 2^m/(m+1)$ and μ satisfying that $\lambda\mu=2^m-1$. Then $S=\{\Phi(\nu^{i\cdot\mu})\}_{i=1}^{\lambda}$ is a $(\lambda-1)$-PD-set of size λ for $K(m)=\Phi(\mathcal{K}(m))$ with information set $I=\{1,\dots,2m+2\}$.

Example 5: Let $\mathcal{K}(4)$ be the quaternary Kerdock code of length 16 and type 4^5 with generator matrix

$$\begin{pmatrix} 1&1&3&0&3&3&0&2&1&2&1&0&0&0&0&3\\ 0&1&1&3&0&3&3&0&2&1&2&1&0&0&0&3\\ 0&0&1&1&3&0&3&3&0&2&1&2&1&0&0&3\\ 0&0&0&1&1&3&0&3&3&0&2&1&2&1&0&3\\ 0&0&0&0&1&1&3&0&3&3&0&2&1&2&1&3 \end{pmatrix},$$

where $h(x)=x^4+2x^2+3x+1$. Note that $\mathcal{I}=\{1,2,3,4,5\}$ is a quaternary information set for $\mathcal{K}(4)$. In this case, we have that $\lambda=3$ and $\mu=5$. Let $\mathcal{S}=\{\nu^5,\nu^{10},\nu^{15}\}$, where $\nu=(1,\dots,15)$. Note that

$$\tau=\nu^5=(1,6,11)(2,7,12)(3,8,13)(4,9,14)(5,10,15)$$

has 5 disjoint cycles of length 3, where each quaternary information position in $\mathcal{I}$ is placed in a different cycle of τ. Hence, $S=\Phi(\mathcal{S})$ is a 2-PD-set of size 3 for the binary Kerdock code $K(4)$ of length 32 with information set $\Phi(\mathcal{I})=\{1,\dots,10\}$.

Theorem 2.2 provides the best s-PD-sets when the permutation $\tau\in\mathrm{PAut}(\mathcal{C})$ has the minimum number of disjoint cycles $|\mathcal{I}|=\gamma+\delta$, each one being of maximum length. Note that the parameters μ and λ, considered in Corollary 4.1, denote the number of disjoint cycles and the length of the cycles of the permutation $\tau=\nu^\mu$, respectively. Therefore, this corollary yields the best $(\lambda-1)$-PD-sets of size λ when $\mu=m+1$, or equivalently, when $\lambda=\rho$, where $\rho=\lfloor 2^m/(m+1)\rfloor$. For example, when $m=4,6,10$ or 12 as shown in Table I. Note that $f_{\mathcal{K}(m)}=\lfloor(2^m-m-1)/(m+1)\rfloor=\rho-1$.

Prime numbers of type 2^m-1 are known as Mersenne primes and have been extensively studied. It is known that if m is not prime, then 2^m-1 is not a Mersenne prime. Hence, Corollary 4.1 can be applied to all nonprime values of m. Despite this, there are also some prime values of m (for example, $m=11$) for which 2^m-1 is not a prime number, so Corollary 4.1 can also be applied. Moreover, even for values of m for which we can not apply this corollary, there are permutations that verify the conditions of Theorem 2.2, as shown in the following example.

Example 6: Let $\mathcal{K}(5)$ be the quaternary Kerdock code of length 32 and type 4^6. Note that $\mathcal{I}=\{1,2,3,4,5,6\}$ is a quaternary information set for $\mathcal{K}(5)$. The conditions of Corollary 4.1 are not fulfilled since 31 is a Mersenne prime. Nevertheless,

$$\begin{aligned}\tau=\ &(1,32,9,19,25)(2,18,24,15,31)(3,27,23,28,12)\\ &(4,8,20,30,26)(5,14,16,21,13)(6,10,17,29,22)\end{aligned}$$

satisfies the conditions of Theorem 2.2 for $s=4$. Thus, $S=\{\Phi(\tau^i)\}_{i=1}^5$ is a 4-PD-set of size 5 for the binary Kerdock code $K(5)$ of length 64 with information set $\Phi(\mathcal{I})$.

REFERENCES

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

[2] R. D. Barrolleta and M. Villanueva, "Partial permutation decoding for binary linear and $\mathbb{Z}_4$-linear Hadamard codes, submitted to *Des. Codes and Cryptogr.*, 2016. arXiv:1512.01839

[3] 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.*, vol. 76(2), 269–277, 2015.

[4] S. Botzas, R. Hammons, and P. V. Kumar, "4-phase sequences with near-optimum correlations propierties," *IEEE Trans. Inform. Theory*, vol. 38, 1101–1113, 1992.

[5] 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.

[6] A. R. Hammons, Jr, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inform. Theory*, vol. 40(2), 301–319, 1994.

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

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

[9] F. J. MacWilliams, "Permutation decoding of systematics codes," *Bell System Tech. J.*, vol. 43, 485–505, 1964.

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, Amsterdam, 1977.

[11] M. W. Maxfield, "The order of a matrix under multiplication (modulo m)," *Duke Math. J.*, vol. 18(3), 619–621, 1951.

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

[13] K.T. Phelps, 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. Inform. Theory*, vol. 52(1), 316–319, 2005.

[14] H.-J. Zepernick and A. Finger, *Pseudo Random Signal Processing: Theory and Application*, John Wiley & Sons Ltd, 2015.