Postprint of: Barrolleta, Roland D. et al. “Partial permutation decoding for binary linear and Z_4-linear Hadamard codes” in *Designs Codes and Cryptography* (2017). The final version is available at DOI 10.1007/s10623-017-0342-8

Partial permutation decoding for binary linear and Z_4-linear Hadamard codes

Roland D. Barrolleta · Mercè Villanueva

Received: date / Accepted: date

Abstract In this paper, s-PD-sets of minimum size $s+1$ for partial permutation decoding for the binary linear Hadamard code H_m of length 2^m, for all $m \geq 4$ and $2 \leq s \leq \lfloor \frac{n-2}{1+m} \rfloor - 1$, are constructed. Moreover, recursive constructions to obtain s-PD-sets of size $l \geq s+1$ for H_{m+1} of length 2^{m+1}, from an s-PD-set of the same size for H_m, are also described. These results are generalized to find s-PD-sets for the Z_4-linear Hadamard codes $H_{\gamma,\delta}$ of length 2^m, $m = \gamma + 2\delta - 1$, which are binary Hadamard codes (not necessarily linear) obtained as the Gray map image of quaternary linear codes of type $2^\gamma 4^\delta$. Specifically, s-PD-sets of minimum size $s+1$ for $H_{\gamma,\delta}$, for all $\delta \geq 3$ and $2 \leq s \leq \lfloor \frac{2^\delta - 2}{\delta} \rfloor - 1$, are constructed and recursive constructions are described.

Keywords automorphism group · permutation decoding · PD-set · Hadamard code · Z_4-linear code

Mathematics Subject Classiftcation (2010) 94B05 · 94B35 · 94B60

1 Introduction

A *binary Hadamard code* of length n is a binary code with $2n$ codewords and minimum distance $n/2$ [16, Ch.2. §3.]. It is well known that there is a unique *binary linear Hadamard code* H_m of length $n = 2^m$, for any $m \geq 2$, which is the dual of the extended Hamming code of length 2^m and also coincides with the first order Reed-Muller code of the same length [16, Ch.13. §3]. Binary

This work was partially supported by the Spanish MINECO under Grants TIN2016-77918-P and MTM2015-69138-REDT, and by the Catalan AGAUR under Grant 2014SGR-691. The material in this paper was presented in part at IX “Jornadas de Matemática Discreta y Algorítmica” in Tarragona, Spain, 2014 [1].

Departament d’Enginyeria de la Informació i de les Comunicacions
Universitat Autònoma de Barcelona
E-mail: rolanddavid.barrolleta@uab.cat, merce.villanueva@uab.cat

Hadamard codes of length 2^m which are obtained as the Gray map image of quaternary linear codes of length 2^{m-1} and type $2^\gamma 4^\delta$, where $m = \gamma+2\delta-1$, are called $\mathbb{Z}_4$-*linear Hadamard codes* and denoted by $H_{\gamma,\delta}$. These quaternary linear codes are called *quaternary linear Hadamard codes* and denoted by $H_{\gamma,\delta}$, that is, $H_{\gamma,\delta} = \Phi(H_{\gamma,\delta})$, where Φ is the Gray map. The $\mathbb{Z}_4$-linear Hadamard codes have been studied and classified in [14, 18], and their automorphism groups have been characterized in [13, 17]. They can be seen as a generalization of the binary linear Hadamard codes, since when $\delta \in \{1, 2\}$ they are linear, so isomorphic to H_m, but when $\delta \geq 3$ they are nonlinear. In general, $\mathbb{Z}_4$-linear codes have become important since 1994, when it was shown that several well-known families of binary nonlinear codes can be simply constructed as binary images under the Gray map of linear codes over $\mathbb{Z}_4$ [9].

Permutation decoding is a technique introduced by Prange [19] and developed by MacWilliams [15] for linear codes that involves finding a special subset, called a PD-set, of the automorphism group of a code. This method is described in detail in [16, Ch.16. §9.] and [7, Section 8].

For linear codes, in [5], it is shown how to find s-PD-sets of size $s + 1$ that satisfy the Gordon-Schönheim bound for (partial) permutation decoding up to s errors for the binary simplex code of length $2^m - 1$ for all $m \geq 4$ and $\frac{1}{2}(m + m + 4) < s \leq \left\lfloor \frac{2^m - 1}{m} \right\rfloor - 1$. In [21], 2-PD-sets of size 5 and 4-PD-sets of size $\frac{1}{2}(m + m + 4)$ are found for H_m for $m \geq 5$. In [10], the method used in [21] is extended to find $(m-1)$-PD-sets of size $\frac{1}{2}(m^2+m+4)$ for H_m for $m \geq 5$, and $(m+1)$-PD-sets of size $\frac{1}{6}(m^3+5m+12)$ for H_m for $m \geq 6$. Small PD-sets that satisfy the Gordon-Schönheim bound have also been found for binary Golay codes [6, 22] and for the binary simplex code S_4 [12]. In [2], a new permutation decoding method for $\mathbb{Z}_4$-linear codes (not necessarily linear) was introduced. The determination of PD-sets for those that are nonlinear remained an open problem.

In this paper, following the same technique as for the binary simplex codes in [5], we establish similar results for binary linear and $\mathbb{Z}_4$-linear Hadamard codes. More specifically, this paper is organized as follows. In Section 3, we first notice that the Gordon-Schönheim bound can be adapted to systematic codes, not necessarily linear (see Proposition 1). Furthermore, we apply this result to obtain a bound f_m on the maximum value of s for which s-PD-sets of minimum size $s+1$ may be found for binary linear and $\mathbb{Z}_4$-linear Hadamard codes, which are systematic and nonlinear in general (see Proposition 2). In Section 4, we regard the permutation automorphism group of H_m as a certain subgroup of the general linear group $\mathrm{GL}(m + 1, 2)$ and we provide a criterion on subsets of matrices of this subgroup to be an s-PD-set of minimum size $s + 1$ for H_m (see Theorem 1). Then, we give s-PD-sets of size $s + 1$ for all $m \geq 4$ and $2 \leq s \leq \left\lfloor \frac{m^2}{4m} \right\rfloor - 1 = f_m$ (see Theorem 2). In Section 5, we define recursive constructions to obtain s-PD-sets of size $l \geq s + 1$ for H_{m+1} from an s-PD-set of the same size for H_m (see Propositions 3 and 4).

Regarding the results for binary linear Hadamard codes, we remark that Theorem 2 has also earlier been proved independently in [11, Corollary 4], as it was pointed out to us by one of the referees in the review process of

this paper. Moreover, most of the results given in Sections 3, 4 and 5 appear without proofs in our conference paper [1], but the main Theorem 2 and the recursive construction shown in Proposition 4 are novel contributions.

In Sections 6 and 7, we establish similar results for (nonlinear) Z_4-linear Hadamard codes $H_{\gamma,\delta}$ of length 2^m and type $2^\gamma 4^\delta$, where $m = \gamma + 2\delta - 1$. They represent the first s-PD-sets for a family of nonlinear codes. Specifically, in Section 6, we regard the permutation automorphism group of $H_{\gamma,\delta}$ as a certain subset of $\mathrm{GL}(\gamma+\delta, Z_4)$ and we provide a criterion on subsets of matrices of this group to be an s-PD-set of minimum size $s + 1$ for $H_{\gamma,\delta} = \Phi(H_{\gamma,\delta})$ (see Theorem 3). Moreover, we obtain a new bound $f_{\gamma,\delta}$ on the maximum value of s for which s-PD-sets of minimum size $s + 1$ can be found for these codes by using this theorem (see Corollary 4). Then, for all these codes, we give s-PD-sets of size $s + 1$ for all $\delta \geq 3$ and $2 \leq s \leq \lfloor \frac{2^\delta - 2}{\delta} \rfloor - 1 = f_{0,\delta}$ (see Theorem 4 and Corollary 5). In Section 7, we also define recursive constructions to obtain s-PD-sets of size $l \geq s + 1$ for $H_{\gamma+i,\delta+j}$, for any $i, j \geq 0$, from an s-PD-set of the same size for $H_{\gamma,\delta}$ (see Proposition 6 and Corollary 6).

In Section 8, we give some computational results and a new example, which improve the explicit construction given by Corollary 5 for $H_{\gamma,\delta}$ with $\gamma > 0$. Actually, we can found easily some s-PD-sets of size $s+1$ for $f_{0,\delta} < s \leq f_{\gamma,\delta}$ by computer search. It is also worth mentioning that most of the concepts and results described in this paper have been implemented as new functions in Magma extending its functionality for linear and Z_4-linear codes. Magma version 2.22 (from May 2016) and later contains these functions by default [4, Chapters 158 and 162], and they can also be downloaded from http://ccsg.uab.cat. Finally, in Section 9, we give the conclusions.

2 Terminology and deftnitions

Let Z_2 and Z_4 be the rings of integers modulo 2 and modulo 4, respectively. Let Z_2^n denote the set of all binary vectors of length n and let Z_4^n be the set of all n-tuples over the ring Z_4. The *Hamming weight* $\mathrm{wt}(v)$ of a vector $v \in Z_2^n$ is the number of nonzero coordinates in v. The *Hamming distance* $d(u, v)$ between two vectors $u, v \in Z_2^n$ is the number of coordinates in which u and v differ, that is, $d(u, v) = \mathrm{wt}(u + v)$. Let e_i be the binary vector or n-tuple over Z_4 with a 1 in the ith coordinate and zeros elsewhere. Let $\mathbf{0}$, $\mathbf{1}$, $\mathbf{2}$ and $\mathbf{3}$ be the binary vectors or n-tuples over Z_4 having 0, 1, 2 and 3, respectively, repeated in each coordinate. It will be clear by the context whether we refer to binary vectors or n-tuples over Z_4.

Any nonempty subset C of Z_2^n is a *binary code* and a subgroup of Z_2^n is called a *binary linear code*. Similarly, any nonempty subset C of Z_4^n is a *quaternary code* and a subgroup of Z_4^n is called a *quaternary linear code*. Quaternary codes can be viewed as binary codes under the usual Gray map $\Phi : Z_4^n \to Z_2^{2n}$ defined as $\Phi((y_1, \ldots, y_n)) = (\varphi(y_1), \ldots, \varphi(y_n))$, where $\varphi(0) = (0, 0)$, $\varphi(1) = (0, 1)$, $\varphi(2) = (1, 1)$, $\varphi(3) = (1, 0)$, for all $y = (y_1, \ldots, y_n) \in Z_4^n$. If C is a quaternary linear code, then the binary code $C = \Phi(C)$ is said to be a Z_4-*linear*

code. Moreover, since C is a subgroup of Z_4^n it is isomorphic to an abelian group $Z_2^\gamma \times Z_4^\delta$ and we say that C (or equivalently, the corresponding Z_4-linear code $C = \Phi(C)$) is of type $2^\gamma 4^\delta$, see for example [9], [8, Chapter 12], or [23].

Let C be a binary code of length n and size $|C| = 2^k$. For a vector $v \in Z_2^n$ and a set $I \subseteq \{1, \ldots, n\}$, $|I| = k$, we denote the restriction of v to the coordinates in I by $v_I \in Z_2^k$ and the set $\{v_I : v \in C\}$ by C_I. 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*. For each information set I of size k, the set $\{1, \ldots, n\} \setminus I$ of the remaining $n - k$ coordinate positions is called a *check set* for C.

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 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 Z_2^n or 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 C or $C = \Phi(C)$, denoted by $\mathrm{PAut}(C)$ or $\mathrm{PAut}(C)$, respectively, is the group generated by all permutations that preserve the set of codewords [7].

Let C be a binary systematic t-error-correcting code C with information set I. 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 $1 \le s \le t$. When $s = t$, S is said to be a PD-*set*.

3 Minimum size of s-PD-sets for Hadamard codes

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 to 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*

$$|S| \ge \binom{n}{r} \Big/ \binom{n-1}{r-1} \Big/ \cdots \Big/ \binom{n-t+1}{r-t+1}. \tag{1}$$

The above inequality (1) is often called the *Gordon-Schönheim bound* [6, 20]. The result given by Proposition 1 is quoted and proved for linear codes in [7]. We can follow the same proof, since the linearity of the code is only used to guarantee that the code is systematic. In [2], it is shown that Z_4-linear codes are systematic and a systematic encoding is given for these codes. Therefore, the result can be applied to any Z_4-linear code, not necessarily linear.

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 binary linear or Z_4-linear Hadamard code of length $n = 2^m$ is $t_m = \lfloor (d-1)/2 \rfloor = \lfloor (2^{m-1} - 1)/2 \rfloor = 2^{m-2} - 1$ [16, Ch.1. §3]. Moreover, all

these codes are systematic and have size $2n = 2^{m+1}$. Therefore, the right-hand side of the bound given by (1) for s-PD-sets, for binary linear and Z_4-linear Hadamard codes of length 2^m and for all $1 \le s \le t_m$, becomes

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

We compute the minimum value of $g_m(s)$ in the following lemma.

Lemma 1 *Let m be an integer, $m \ge 4$. Then $g_m(s) \ge s + 1$ for all $1 \le s \le t_m = 2^{m-2} - 1$.*

Proof We need to prove that $g_m(s) \ge s+1$. This fact is clear, since the central term $|(2^m - s + 1)/(2^m - m - s)| = 2$, for all $s \in \{1, \ldots, 2^{m-2} - 1\}$, and in each stage of the ceiling function working from inside, $g_m(s)$ increases its value by at least 1. *H*

The smaller the size of the PD-set is, the more efficient permutation decoding becomes. In this paper, we study the simple case, when we have that $g_m(s) = s + 1$. For each binary linear and Z_4-linear Hadamard code of length 2^m, $m \ge 4$, we define the integer $f_m = \max\{s : 2 \le s, g_m(s) = s + 1\}$, which represents the greater s in which we can find s-PD-sets of size $s + 1$. The following result characterize this parameter from the value of m. Note that for $m = 3$, since the error-correcting capability is $t_3 = 1$, the permutation decoding becomes unnecessary and we do not take it into account in the results.

Proposition 2 *Let m be an integer, $m \ge 4$. Then, $f_m = \left\lceil \frac{2^m}{1+m} \right\rceil - 1$.*

Proof By Lemma 1 and an argument similar to the proof of Lemma 2 in [5]. *H*

4 Construction of s-PD-sets of size $s + 1$ for binary linear Hadamard codes

For any $m \ge 2$, there is a unique linear Hadamard code H_m of length 2^m, which is also the first order Reed-Muller code with parameters $[2^m, m+1, 2^{m-1}]_2$ [16, Ch.13. §3]. A generator matrix tt_m for H_m can be constructed as follows:

$$tt_m = \begin{bmatrix} 1 & \mathbf{1} \\ \mathbf{0} & tt^r \end{bmatrix}, \qquad (2)$$

where tt^r is any matrix having as column vectors the $2^m - 1$ nonzero vectors from Z_2^m, with the vectors e_i, $i \in \{1, \ldots, m\}$, in the first m positions. Note that tt^r can be seen as a generator matrix of the simplex code of length $2^m - 1$.

By construction, from (2), it is clear that $I_m = \{1, \ldots, m + 1\}$ is an information set for H_m. Let w_i be the ith column vector of tt_m, $i \in \{1, \ldots, 2^m\}$. By labelling the coordinate positions with the columns of tt_m, we can take as

an information set I_m for H_m the first $m+1$ column vectors of tt_m considered as row vectors, that is, $I_m = \{w_1, \ldots, w_{m+1}\} = \{e_1, e_1+e_2, \ldots, e_1+e_{m+1}\}$. Then, depending on the context, I_m will be taken as a subset of $\{1, \ldots, 2^m\}$ or $\{1\} \times Z_2^m$.

It is known that the permutation automorphism group PAut(H_m) of H_m is isomorphic to the general affine group AGL(m, 2) [16, Ch.13. §9]. Let GL(m, 2) be the general linear group over Z_2. Recall that AGL(m, 2) consists of all mappings $\alpha : Z_2^m \to Z_2^m$ of the form $\alpha(x) = Ax + b$ for $x \in Z_2^m$, where $A \in$ GL(m, 2) and $b \in {}_2Z^m$, together with the function composition as the group operation. The monomorphism

$$\phi : \mathrm{AGL}(m, 2) \longrightarrow \mathrm{GL}(m+1, 2)$$

$$(b, A) \longrightarrow \begin{bmatrix} 1 & b \\ \mathbf{0} & A \end{bmatrix}$$

defines an isomorphism between AGL(m, 2) and the subgroup of GL($m+1$, 2) consisting of all nonsingular matrices whose first column is e_1. Therefore, from now on, we also regard PAut(H_m) as this subgroup. Note that any matrix $M \in$ PAut(H_m) can be seen as a permutation of coordinate positions, that is, as an element of Sym(2^m). By multiplying the ith column vector w_i of tt_m by M, we obtain another column vector $w_j = w_i M$, which means that the ith coordinate position moves to the jth coordinate position, $i, j \in \{1, \ldots, 2^m\}$.

Let M be a binary matrix with r rows and let m_i be the ith row of M, $i \in \{1, \ldots, r\}$. We define M^* as the matrix

$$M^* = \begin{bmatrix} m_1 \\ m_1 + m_2 \\ \vdots \\ m_1 + m_r \end{bmatrix}. \tag{3}$$

An s-PD-set of size $s+1$ for H_m meets the Gordon-Schönheim bound if $2 \le s \le f_m$. The following theorem provides us a condition on sets of matrices of PAut(H_m) in order to be s-PD-sets of size $s+1$ for H_m.

Theorem 1 *Let H_m be the binary linear Hadamard code of length 2^m, with $m \ge 4$. Let $P_s = \{M_i : 0 \le i \le s\}$ be a set of $s+1$ matrices in* PAut(H_m). *Then, P_s is an s-PD-set of size $s+1$ for H_m with information set I_m if and only if no two matrices $(M_i^{-1})^*$ and $(M_j^{-1})^*$ for $i \neq j$ have a row in common. Moreover, any subset $P_k \subseteq P_s$ of size $k+1$ is a k-PD-set for $k \in \{1, \ldots, s\}$.*

Proof Suppose that the set $P_s = \{M_i : 0 \le i \le s\}$ satisfies that no two matrices $(M_i^{-1})^*$ and $(M_j^{-1})^*$ for $i \neq j$ have a row in common. Let $E = \{v_1, \ldots, v_s\} \subseteq \{1\} \times Z_2^m$ be a set of s different column vectors of the generator matrix tt_m regarded as row vectors, which represents a set of s error positions. Assume we cannot move all the error positions to the check set by any element of P_s. Then, for each $i \in \{0, \ldots, s\}$, there is a $v \in E$ such that $vM_i \in I_m$. In other words, there is at least one error position that remains in the information

set I_m after applying any permutation of P_s. Note that there are $s+1$ values for i, but only s elements in E. Therefore, $vM_i \in I_m$ and $vM_j \in I_m$ for some $v \in E$ and $i \neq j$. Suppose $vM_i = w_r$ and $vM_j = w_t$ for $w_r, w_t \in I_m$. Then, $v = w_r M_i^{-1} = w_t M_j^{-1}$. Thus, we obtain that $(M_i^{-1})^*$ and $(M_j^{-1})^*$ have a row in common, contradicting our assumption. Let $P_k \subseteq P_s$ of size $k+1$. If this set satisfies the condition on the inverse matrices and we suppose that it is not a k-PD-set, we arrive at a contradiction in the same way as before.

Conversely, suppose that the set $P_s = \{M_i : 0 \leq i \leq s\}$ forms an s-PD-set for H_m, but does not satisfy the condition on the inverse matrices. Thus, some $v \in \{w_1, \ldots, w_{2^m}\}$ must be the rth row of $(M_i^{-1})^*$ and the tth row of $(M_j^{-1})^*$ for some $r, t \in \{1, \ldots, m+1\}$, $i, j \in \{0, \ldots, s\}$. In other words, we have that $v = e_r(M_i^{-1})^* = e_t(M_j^{-1})^*$. Therefore, $v = w_r M_i^{-1} = w_t M_j^{-1}$, where $w_r, w_t \in I_m$, and thus $vM_i = w_r$ and $vM_j = w_t$. These equalities implies that the vector v, which represents an error position, cannot be moved to the check set by the permutations defined by the matrices M_i and M_j. Let $L = \{l : 0 \leq l \leq s, l \neq i, j\}$. For each $l \in L$, choose a row v_l of $(M_l^{-1})^*$. It is clear that $v_l = e_h(M_l^{-1})^* = w_h M_l^{-1}$ for some $h \in \{1, \ldots, m+1\}$, so $v_l M_l = w_h \in I_m$. Finally, since some of the v_l may repeat, we obtain a set $E = \{v_l : l \in L\} \cup \{v\}$ of size at most s. Nevertheless, no matrix in P_s will map every member of E into the check set, a fact that contradicts our assumption. H

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 $S_s = S$. From Theorem 1, we have two important consequences. The first one is related to how to obtain nested s-PD-sets and the second one provides another proof of Proposition 2.

Corollary 1 *Let m be an integer, $m \geq 4$. If P_s is an s-PD-set of size $s+1$ for the binary linear Hadamard code H_m, then any ordering of the elements of P_s gives nested k-PD-sets for $k \in \{1, \ldots, s\}$.*

Corollary 2 *Let m be an integer, $m \geq 4$. If P_s is an s-PD-set of size $s+1$ for the binary linear Hadamard code H_m, then $s \leq f_m = \left\lfloor \frac{2^m}{1+m} \right\rfloor - 1$.*

Proof Following the condition on sets of matrices to be s-PD-sets of size $s+1$, given by Theorem 1, we have to obtain certain $s+1$ matrices with no rows in common. Note that the number of possible vectors of length $m+1$ over Z_2 with 1 in the first coordinate is 2^m. Thus, taking this fact into account and counting the number of rows of each one of these $s+1$ matrices, we have that $(s+1)(m+1) \leq 2^m$, so $s+1 \leq \frac{2^m}{m+1}$ and finally $s \leq f_m$. H

Next, by using Theorem 1, we give an explicit construction of s-PD-sets of minimum size $s+1$ for H_m, for all $m \geq 4$ and $2 \leq s \leq f_m$. We follow a similar technique to the one described for simplex codes in [5].

Lemma 2 *Let $K = Z_2[x]/(f(x))$, where $f(x) \in Z_2[x]$ is a primitive polynomial of degree m. Let $\alpha \in K$ be a root of $f(x)$. Then $\alpha^{i+1} - \alpha^i, \ldots, \alpha^{i+m} - \alpha^i$ are linearly independent over Z_2 for all $i \in \{0, \ldots, 2^m - 2\}$.*

Proof It is straightforward to see that $\alpha^{i+1} - \alpha^i, \ldots, \alpha^{i+m} - \alpha^i$ are linearly independent over Z_2 for all $i \in \{0, \ldots, 2^m - 2\}$, if and only if $\alpha - 1, \ldots, \alpha^m - 1$ are linearly independent over Z_2, since $\alpha^i \in K \setminus \{0\}$.

Note that $\alpha^m - 1 = \sum_{j=1}^{m-1} \mu_j \alpha^j$ for some $\mu_j \in \{0, 1\}$. Moreover, this summation has an odd number of nonzero terms, since $f(x)$ is irreducible. Let $\mu = (\mu_1, \ldots, \mu_{m-1}) \in Z_2^{m-1}$. Note that in vectorial notation $\alpha^j - 1 = e_1 + e_{j+1}$, $j \in \{1, \ldots, m-1\}$, and $\alpha^m - 1 = \sum_{j=1}^{m-1} \mu_j e_{j+1}$. Finally, it is easy to see that the $m \times m$ binary matrix

$$\begin{bmatrix} 1 & \\ 0 & \mu \end{bmatrix} \mathrm{Id}_{m-1},$$

which has as rows $\alpha - 1, \ldots, \alpha^m - 1$, has determinant $\sum_{j=1}^{m-1} \mu_j = 1 \neq 0$. ∎

For $i \in \{1, \ldots, f_m\}$, we consider the $(m+1) \times (m+1)$ binary matrices

$$N_0 = \begin{bmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & \ddots & \\ & & & \alpha^{m-1} \end{bmatrix} \quad \text{and} \quad N_i = \begin{bmatrix} 1 & \alpha^{(m+1)i-1} & & \\ 0 & \alpha^{(m+1)i} - \alpha^{(m+1)i-1} & & \\ & & \ddots & \\ & & & \alpha^{(m+1)i+m-1} - \alpha^{(m+1)i-1} \end{bmatrix}.$$

Theorem 2 *Let $P_s = \{M_i : 0 \leq i \leq s\}$, where $M_i = N_i^{-1}$. Then, P_s is an s-PD-set of size $s+1$ for the binary linear Hadamard code H_m of length 2^m with information set I_m, for all $m \geq 4$ and $2 \leq s \leq f_m$.*

Proof Clearly, $N_0 \in \mathrm{PAut}(H_m)$. By Lemma 2, $N_i \in \mathrm{PAut}(H_m)$ for all $i \in \{1, \ldots, f_m\}$. The rows of the matrices $N_0^*, \ldots, N_{f_m}^*$, constructed as in (3), are the elements of the form $(1, a)$ for all $a \in \{0, 1, \alpha, \ldots, \alpha^{f_m(m+1)+m-1}\}$. They are all different, since α is primitive and $f_m(m+1) + m - 1 \leq 2^m - 2$. By Theorem 1, the result follows. ∎

Note 1 The construction of the matrices in Theorem 2 is virtually identical to a construction submitted earlier in [11, Corollary 4].

Example 1 Let H_4 be the binary linear Hadamard code of length 16 with a generator matrix constructed as in (2). Let $K = Z_2[x]/(x^4 + x + 1)$ and α be a root of $x^4 + x + 1$. We have that $f_4 = 2$. Let

$$N_1 = \begin{bmatrix} 1 & \alpha^4 \\ 0 & \alpha^5 - \alpha^4 \\ 0 & \alpha^6 - \alpha^4 \\ 0 & \alpha^7 - \alpha^4 \\ 0 & \alpha^8 - \alpha^4 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \quad \text{and} \quad N_2 = \begin{bmatrix} 1 & \alpha^9 \\ 0 & \alpha^{10} - \alpha^9 \\ 0 & \alpha^{11} - \alpha^9 \\ 0 & \alpha^{12} - \alpha^9 \\ 0 & \alpha^{13} - \alpha^9 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

The matrices $N_0 = \mathrm{Id}_5$, where Id_5 is the 5×5 identity matrix, N_1 and N_2 are elements of $\mathrm{PAut}(H_4)$. By Theorem 2, $P_2 = \{N_0^{-1}, N_1^{-1}, N_2^{-1}\}$ is a 2-PD-set of size 3 for H_4. It is straightforward to check that the matrices N_0^*,

$$N_1^* = \begin{bmatrix} 1&1&1&0&0 \\ 1&0&1&1&0 \\ 1&0&0&1&1 \\ 1&1&1&0&1 \\ 1&1&0&1&0 \end{bmatrix} \quad \text{and} \quad N_2^* = \begin{bmatrix} 1&0&1&0&1 \\ 1&1&1&1&0 \\ 1&0&1&1&1 \\ 1&1&1&1&1 \\ 1&1&0&1&1 \end{bmatrix}$$

have no rows in common. Finally, note that no s-PD-set of size $s+1$ can be found for $s \geq 3$ since $f_4 = 2$.

5 Recursive constructions of s-PD-sets for binary linear Hadamard codes

Given a matrix $M \in \mathrm{PAut}(H_m)$ and an integer $\kappa \geq 1$, we define the matrix $M(\kappa) \in \mathrm{PAut}(H_{m+\kappa})$ as

$$M(\kappa) = \begin{bmatrix} M & \mathbf{0} \\ \mathbf{0} & \mathrm{Id}_\kappa \end{bmatrix},$$

where Id_κ denotes the $\kappa \times \kappa$ identity matrix.

Proposition 3 *Let m be an integer, $m \geq 4$, and let $P_s = \{M_i : 0 \leq i \leq s\}$ be an s-PD-set of size $s+1$ for H_m with information set I_m. Then, $Q_s = \{M_i(\kappa) : 0 \leq i \leq s\}$ is an s-PD-set of size $s+1$ for $H_{m+\kappa}$ with information set $I_{m+\kappa}$, for any $\kappa \geq 1$.*

Proof Since P_s is an s-PD-set for H_m, matrices $(M_1^{-1})^*, \ldots, (M_s^{-1})^*$, constructed as in (3), have no rows in common by Theorem 1. Therefore, it is straightforward to check that matrices $(M_1^{-1}(\kappa))^*, \ldots, (M_s^{-1}(\kappa))^*$ have no rows in common either. Moreover, $M_i^{-1}(\kappa) \in \mathrm{PAut}(H_{m+\kappa})$ for all $i \in \{1, \ldots, s\}$. Thus, applying again Theorem 1 and the fact that $M_i(\kappa)^{-1} = M_i^{-1}(\kappa)$, we have that Q_s is an s-PD-set for $H_{m+\kappa}$. H

Note that the bound f_{m+1} for H_{m+1} cannot be achieved recursively from an s-PD-set for H_m, since the recursive construction given by Proposition 3 works for a given fixed s, while increasing the length of the Hadamard code.

Next, we show a second recursive construction which holds when the size of the s-PD-set is any integer l, $l \geq s+1$, unlike the first recursive construction. Now, the elements of $\mathrm{PAut}(H_m)$ will be regarded as permutations of coordinate positions, that is, as elements of $\mathrm{Sym}(2^m)$ instead of matrices of $\mathrm{GL}(m+1, 2)$.

It is well known that a generator matrix tt_{m+1} for the binary linear Hadamard code H_{m+1} of length 2^{m+1} can be constructed as follows:

$$tt_{m+1} = \begin{bmatrix} tt_m & tt_m \\ \mathbf{0} & \mathbf{1} \end{bmatrix}, \tag{4}$$

where tt_m is a generator matrix for the binary linear Hadamard code H_m of length 2^m. 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 $\{1,\ldots,n_1\}$ and σ_2 on $\{n_1+1,\ldots,n_1+n_2\}$.

Proposition 4 *Let m be an integer, $m \geq 4$, and S be an s-PD-set of size I for H_m with information set I. Then, $(S|S) = \{(\sigma|\sigma) : \sigma \in S\}$ is an s-PD-set of size I for H_{m+1} constructed from (4), with any information set $I^r = I \cup \{i + 2^m\}$, $i \in I$.*

Proof Since I is an information set for H_m, we have that $|(H_m)_I| = 2^{m+1}$. Since H_{m+1} is constructed from (4), it follows that $H_{m+1} = \{(x, x), (x, \bar{x}) : x \in H_m\}$, where $\bar{x}$ is the complementary vector of x. A vector and its complementary have different values in each coordinate, so $|(H_{m+1})_{I\cup\{i\}})| = 2^{m+2}$, for all $i \in \{2^m+1,\ldots,2^{m+1}\}$. Thus, any set of the form $I^r = I \cup \{i+2^m\}$, $i \in I$, is an information set for H_{m+1}.

If $\sigma \in \mathrm{PAut}(H_m)$, then $\sigma(x) = z \in H_m$ for all $x \in H_m$. Therefore, since $(\sigma|\sigma)(x, x) = (z, z)$ and $(\sigma|\sigma)(x, \bar{x}) = (z, z + \sigma(\mathbf{1})) = (z, \bar{z})$, we can conclude that $(\sigma|\sigma) \in \mathrm{PAut}(H_{m+1})$.

Let $e = (a, b) \in Z_2^{2n}$, where $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n) \in Z_2^n$, and $n = 2^m$. Finally, we will prove that for every $e \in Z_2^{2n}$ with $\mathrm{wt}(e) \leq s$, there is $(\sigma|\sigma) \in (S|S)$ such that $(\sigma|\sigma)(e)_{I^t} = \mathbf{0}$. Let $c = (c_1, \ldots, c_n)$ be the binary vector defined as follows: $c_i = 1$ if and only if $a_i = 1$ or $b_i = 1$, for all $i \in \{1, \ldots, n\}$. Note that $\mathrm{wt}(c) \leq s$, since $\mathrm{wt}(e) \leq s$. Taking into account that S is an s-PD-set with respect to I, there is $\sigma \in S$ such that $\sigma(c)_I = \mathbf{0}$. Therefore, we also have that $(\sigma|\sigma)(a, b)_{I\cup J} = \mathbf{0}$, where $J = \{i + n : i \in I\}$. The result follows trivially since $I^r \subseteq I \cup J$. *H*

6 Construction of s-PD-sets of size $s + 1$ for Z_4-linear Hadamard codes

A Z_4-linear Hadamard code $H_{\gamma,\delta}$ of length 2^m is a binary Hadamard code obtained as the Gray map image of a quaternary linear code of length $\beta = 2^{m-1}$ and type $2^\gamma 4^\delta$ with $m = \gamma + 2\delta - 1$ [14]. Note that they have the same parameters $(2^m, 2^{m+1}, 2^{m-1})_2$ as the binary 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) Z_4-linear Hadamard code of length 2^m. Moreover, for a fixed m, all these codes are pairwise nonequivalent, except for $\delta = 1$ and $\delta = 2$, since these ones are equivalent to the binary linear Hadamard code H_m of length 2^m [14]. Therefore, the number of nonequivalent Z_4-linear Hadamard codes of length 2^m is $\lfloor \frac{m-1}{2} \rfloor$ for all $m \geq 3$. Note that when $\delta \geq 3$, the Z_4-linear Hadamard codes are nonlinear.

Let $H_{\gamma,\delta}$ be the quaternary linear Hadamard code of length $\beta = 2^{m-1}$ and type $2^\gamma 4^\delta$, where $m = \gamma + 2\delta - 1$, and let $H_{\gamma,\delta} = \Phi(H_{\gamma,\delta})$ be the corresponding Z_4-linear code of length $2\beta = 2^m$. A generator matrix $G_{\gamma,\delta}$ for $H_{\gamma,\delta}$ of size

$(\gamma + \delta) \times \beta$ can be constructed by using the following recursive constructions:

$$G_{\gamma+1,\delta} = \begin{matrix} G_{\gamma,\delta} & G_{\gamma,\delta} \\ \mathbf{0} & \mathbf{2} \end{matrix}, \tag{5}$$

$$G_{\gamma,\delta+1} = \begin{matrix} G_{\gamma,\delta} & G_{\gamma,\delta} & G_{\gamma,\delta} & G_{\gamma,\delta} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \end{matrix}, \tag{6}$$

starting from $G_{0,1} = (1)$. Note that different matrices $G_{\gamma,\delta}$ are obtained, depending on the chosen order applying γ times (5) and $\delta - 1$ times (6). Since all of them generate permutation equivalent codes, from now on, we consider the one constructed as follows: first, the matrix $G_{0,\delta}$ is obtained from $G_{0,1}$ by using recursively $\delta - 1$ times (6), and then $G_{\gamma,\delta}$ is constructed from $G_{0,\delta}$ by using γ times (5). Considering the rows of $G_{\gamma,\delta}$ as elements in the group $(Z_4^\beta, +)$, note that, following this construction, the rows of order four remain in the upper part of $G_{\gamma,\delta}$ while those of order two stay in the lower part.

Example 2 The quaternary linear Hadamard code $H_{0,3}$ of length 16 has generator matrix $G_{0,3}$ obtained by applying (6) two times to $G_{0,1} = (1)$, where

$$G_{0,3} = \begin{matrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3 \\ 0&0&0&0&1&1&1&1&2&2&2&2&3&3&3&3 \end{matrix}.$$

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

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

is an information set for $C = \Phi(C)$. For example, the set $I = \{1\}$ is a quaternary information set for $H_{0,1}$, so $\Phi(I) = \{1, 2\}$ is an information set for $H_{0,1} = \Phi(H_{0,1})$. In general, there is not a unique way to obtain a quaternary information set for $H_{\gamma,\delta}$. The following result provides a recursive and simple form to obtain such a set.

Proposition 5 *Let I be a quaternary information set for the quaternary linear Hadamard code $H_{\gamma,\delta}$ of length $\beta = 2^{m-1}$ and type $2^\gamma 4^\delta$, where $m = \gamma + 2\delta - 1$. Then $I \cup \{\beta + 1\}$ is a quaternary information set for the codes $H_{\gamma+1,\delta}$ and $H_{\gamma,\delta+1}$, which are obtained from $H_{\gamma,\delta}$ by applying (5) and (6), respectively.*

Proof Since $|H_{\gamma+1,\delta}| = 2^{\gamma+1}4^\delta$ and $|H_{\gamma,\delta+1}| = 2^\gamma 4^{\delta+1}$, it is clear that a quaternary information set for codes $H_{\gamma+1,\delta}$ and $H_{\gamma,\delta+1}$ should have $\gamma+\delta+1 = |I|+1$ coordinate positions.

Taking into account that $H_{\gamma,\delta+1}$ is constructed from (6), we have that $H_{\gamma,\delta+1} = \{(u, u, u, u), (u, u + \mathbf{1}, u + \mathbf{2}, u + \mathbf{3}), (u, u + \mathbf{2}, u, u + \mathbf{2}), (u, u + \mathbf{3}, u + \mathbf{2}, u + \mathbf{1}) : u \in H_{\gamma,\delta}\}$. Vectors u, $u + \mathbf{1}$, $u + \mathbf{2}$, and $u + \mathbf{3}$ have different values

in each coordinate, so $|(H_{\gamma,\delta+1})_{I\cup\{i\}}| = 2^{\gamma}4^{\delta+1}$ for all $i \in \{\beta+1, \ldots, 2\beta, 3\beta+1, \ldots, 4\beta\}$. In particular, $I\cup\{\beta+1\}$ is a quaternary information set for $H_{\gamma,\delta+1}$.

A similar argument holds for $H_{\gamma+1,\delta}$. Since $H_{\gamma+1,\delta}$ is constructed from (5), we have that $H_{\gamma+1,\delta} = \{(u, u), (u, u+\mathbf{2}) : u \in H_{\gamma,\delta}\}$. Vectors u and $u+\mathbf{2}$ have different values in each coordinate, so $|(H_{\gamma+1,\delta})_{I\cup\{i\}}| = 2^{\gamma+1}4^{\delta}$ for all $i \in \{\beta+1, \ldots, 2\beta\}$. Thus, $I \cup \{\beta+1\}$ is a quaternary information set for $H_{\gamma+1,\delta}$. H

Although the quaternary information set $I\cup\{\beta+1\}$, given by Proposition 5, is the same for $H_{\gamma+1,\delta}$ and $H_{\gamma,\delta+1}$, the information set for the corresponding binary codes $H_{\gamma+1,\delta}$ and $H_{\gamma,\delta+1}$ are different, $I^r = \Phi(I) \cup \{2\beta+1\}$ and $I^{rr} = \Phi(I) \cup \{2\beta+1, 2\beta+2\}$, respectively. As for binary linear codes, we can label the ith coordinate position of a quaternary linear code C, with the ith column of a generator matrix G of C. Thus, any quaternary information set I for C can also be considered as a set of vectors representing the positions in I. Then, by Proposition 5, we have that the set $I_{\gamma,\delta} = \{e_1, e_1+e_2, \ldots, e_1+e_\delta, e_1+2e_{\delta+1}, \ldots, e_1+2e_{\gamma+\delta}\}$ is a suitable quaternary information set for $H_{\gamma,\delta}$. Depending on the context, $I_{\gamma,\delta}$ will be considered as a subset of $\{1, \ldots, \beta\}$ or $\{1\} \times \mathbb{Z}_4^{\delta-1} \times \{0, 2\}^{\gamma}$.

Example 3 The set $I_{0,3} = \{1, 2, 5\}$, or equivalently the set of vectors $I_{0,3} = \{(1,0,0), (1,1,0), (1,0,1)\}$, is a quaternary information set for the code $H_{0,3}$ given in Example 2. By applying (5) and (6) over $G_{0,3}$, we obtain matrices $G_{1,3}$ and $G_{0,4}$ that generate the codes $H_{1,3}$ and $H_{0,4}$ of length 32 and 64, respectively. By Proposition 5, it follows that $I_{0,3} \cup \{17\} = \{1, 2, 5, 17\}$ is a quaternary information set for $H_{1,3}$ and $H_{0,4}$. Although the quaternary information set is the same for both codes $H_{1,3}$ and $H_{0,4}$, it is important to note that in terms of vectors representing these positions, we have that $I_{1,3} = \{(1,0,0,0), (1,1,0,0), (1,0,1,0), (1,0,0,2)\}$ and $I_{0,4} = \{(1,0,0,0), (1,1,0,0), (1,0,1,0), (1,0,0,1)\}$. Finally, $I^r = \Phi(I_{0,3}) \cup \{33\} = \{1, 2, 3, 4, 9, 10, 33\}$ and $I^{rr} = \Phi(I_{0,3}) \cup \{33, 34\} = \{1, 2, 3, 4, 9, 10, 33, 34\}$ are information sets for the $\mathbb{Z}_4$-linear Hadamard codes $H_{1,3}$ and $H_{0,4}$, respectively.

Let C be a quaternary linear code of length β and type $2^{\gamma}4^{\delta}$, and let $C = \Phi(C)$ 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

$$\Phi(\tau)(i) = \begin{cases} 2\tau(i/2), & \text{if } i \text{ is even,} \\ 2\tau((i+1)/2) - 1 & \text{if } i \text{ is odd,} \end{cases} \tag{7}$$

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

Let $\mathrm{GL}(k, \mathbb{Z}_4)$ be the general linear group of degree k over $\mathbb{Z}_4$. Let L be the set consisting of all matrices over $\mathbb{Z}_4$ of the following form:

$$\begin{pmatrix} 1 & \eta & 2\theta \\ \mathbf{0} & A & 2X \\ \mathbf{0} & Y & B \end{pmatrix},$$

where $A \in \mathrm{GL}(\delta-1, Z_4)$, $B \in \mathrm{GL}(\gamma, Z_4)$, X is a matrix over Z_4 of size $(\delta-1)\times\gamma$, Y is a matrix over Z_4 of size $\gamma \times (\delta-1)$, $\eta \in Z_4^{\delta-1}$ and $\theta \in Z_4^{\gamma}$.

Lemma 3 *The set L is a subgroup of* $\mathrm{GL}(\gamma+\delta, Z_4)$.

Proof We first need to check that $L \subseteq \mathrm{GL}(\gamma+\delta, Z_4)$, i.e., that $\det(M) \in \{1, 3\}$ for all $M \in L$. Note that if $M^r \in \mathrm{GL}(k, Z_4)$, then $M = M^r + 2R \in \mathrm{GL}(k, Z_4)$ for any R. Thus, since $\det(M^r) \in \{1, 3\}$, we have that $\det(M) \in \{1, 3\}$, where

$$M^r = \begin{array}{c} \cdot \\ \cdot \\ \cdot \end{array} \begin{array}{c} \begin{array}{ccc} 1 & \eta & \mathbf{0} \end{array} \\ \begin{array}{ccc} \mathbf{0} & A & \mathbf{0} \end{array} \\ \begin{array}{ccc} \mathbf{0} & Y & B \end{array} \end{array} \begin{array}{c} \cdot \\ \cdot \\ \cdot \end{array}.$$

It is straightforward to check that $MN \in L$ for all $M, N \in L$. *H*

Let ζ be the map from Z_4 to Z_4 defined as $\zeta(0) = \zeta(2) = 0$, $\zeta(1) = \zeta(3) = 1$. This map can be extended to matrices over Z_4 by applying ζ to each one of their entries. Let π be the map from L to L defined as

$$\pi(M) = \begin{array}{c} \cdot \\ \cdot \\ \cdot \end{array} \begin{array}{c} \begin{array}{ccc} 1 & \eta & 2\theta \end{array} \\ \begin{array}{ccc} \mathbf{0} & A & 2X \end{array} \\ \begin{array}{ccc} \mathbf{0} & \zeta(Y) & \zeta(B) \end{array} \end{array} \begin{array}{c} \cdot \\ \cdot \\ \cdot \end{array},$$

and let $\pi(L) = \{\pi(M) : M \in L\} \subseteq \mathrm{GL}(\gamma+\delta, Z_4)$. By Lemma 3, it is clear that $\pi(L)$ is a group with the operation $*$ defined as $M * N = \pi(MN)$ for all $M, N \in \pi(L)$. By the proof of Theorem 2 in [13], it is easy to see that the permutation automorphism group $\mathrm{PAut}(H_{\gamma,\delta})$ is isomorphic to $\pi(L)$. Thus, from now on, we identify $\mathrm{PAut}(H_{\gamma,\delta})$ with this group. Recall that we can label the ith coordinate position of $H_{\gamma,\delta}$ with the ith column vector w_i of the generator matrix $G_{\gamma,\delta}$ constructed via (5) and (6), $i \in \{1, \ldots, \beta\}$. Therefore, again, any matrix $M \in \mathrm{PAut}(H_{\gamma,\delta})$ can be seen as a permutation of coordinate positions $\tau \in \mathrm{Sym}(\beta)$, such that $\tau(i) = j$ as long as $w_j = w_i M$, $i, j \in \{1, \ldots, \beta\}$. For any $M \in \mathrm{PAut}(H_{\gamma,\delta})$, we define $\Phi(M) = \Phi(\tau) \in \mathrm{Sym}(2\beta)$, where $\Phi(\tau)$ is defined as in (7), and for any $P \subseteq \mathrm{PAut}(H_{\gamma,\delta})$, we consider $\Phi(P) = \{\Phi(M) : M \in P\} \subseteq \mathrm{Sym}(2\beta)$.

Lemma 4 *Let $H_{\gamma,\delta}$ be the quaternary linear Hadamard code of length β and type $2^\gamma 4^\delta$ and let $P \subseteq \mathrm{PAut}(H_{\gamma,\delta})$. Then, $\Phi(P)$ is an s-PD-set for $H_{\gamma,\delta}$ with information set $\Phi(I_{\gamma,\delta})$ if and only if for every s-set E of column vectors of $G_{\gamma,\delta}$ there is $M \in P$ such that $\{gM : g \in E\} \cap I_{\gamma,\delta} = \emptyset$.*

Proof If $\Phi(P)$ is an s-PD-set with respect to the information set $\Phi(I_{\gamma,\delta})$, then for every s-set $E \subseteq \{1, \ldots, 2\beta\}$, there is $\tau \in P \subseteq \mathrm{Sym}(\beta)$ such that $\Phi(\tau)(E) \cap \Phi(I_{\gamma,\delta}) = \emptyset$. For every s-set $E \subseteq \{1, \ldots, \beta\}$, let $E_o = \{2i-1 : i \in E\}$. We know that there is $\tau \in P$ such that $\Phi(\tau)(E_o) \cap \Phi(I_{\gamma,\delta}) = \emptyset$. By the definition of Φ, we also have that $\tau(E) \cap I_{\gamma,\delta} = \emptyset$, which is equivalent to the statement.

Conversely, we assume that for every s-set $E \subseteq \{1, \ldots, \beta\}$, there is $\tau \in P \subseteq \mathrm{Sym}(\beta)$ such that $\tau(E) \cap I_{\gamma,\delta} = \emptyset$. For every s-set $E \subseteq \{1, \ldots, 2\beta\}$, let E_o be an s-set such that $\{i : \phi_1(i) \in E \text{ or } \phi_2(i) \in E\} \subseteq E_o$, where $\phi_1(i) = 2i - 1$ and $\phi_2(i) = 2i$. Since there is $\tau \in P$ such that $\tau(E_o) \cap I_{\gamma,\delta} = \emptyset$, we have that $\Phi(\tau)(E) \cap \Phi(I_{\gamma,\delta}) = \emptyset$. *H*

Let $M \in \mathrm{PAut}(H_{\gamma,\delta})$ and let m_i be the ith row of M, $i \in \{1, \ldots, \delta+\gamma\}$. We define M^* as the matrix where the first row is m_1 and the ith row is $m_1 + m_i$ for $i \in \{2, \ldots, \delta\}$ and $m_1 + 2m_i$ for $i \in \{\delta+1, \ldots, \delta+\gamma\}$.

Theorem 3 *Let $H_{\gamma,\delta}$ be the quaternary linear Hadamard code of type $2^\gamma 4^\delta$. Let $P_s = \{M_i : 0 \le i \le s\}$ be a set of $s+1$ matrices in $\mathrm{PAut}(H_{\gamma,\delta})$. Then, $\Phi(P_s)$ is an s-PD-set of size $s+1$ for $H_{\gamma,\delta}$ with information set $\Phi(I_{\gamma,\delta})$ if and only if no two matrices $(M_i^{-1})^*$ and $(M_j^{-1})^*$ for $i \neq j$ have a row in common.*

Proof By Lemma 4 and an argument similar to the proof of Theorem 1. *H*

Corollary 3 *Let P_s be a set of $s+1$ matrices in $\mathrm{PAut}(H_{\gamma,\delta})$. If $\Phi(P_s)$ is an s-PD-set of size $s+1$ for $H_{\gamma,\delta}$, then any ordering of elements in $\Phi(P_s)$ provides nested k-PD-sets for $k \in \{1, \ldots, s\}$.*

Corollary 4 *Let P_s be a set of $s+1$ matrices in $\mathrm{PAut}(H_{\gamma,\delta})$. If $\Phi(P_s)$ is an s-PD-set of size $s+1$ for $H_{\gamma,\delta}$, then $s \le f_{\gamma,\delta} = \left\lfloor \frac{2^{\gamma+2\delta-2}}{\gamma+\delta} \right\rfloor - 1$.*

Proof Following the condition on sets of matrices to be s-PD-sets of size $s+1$, given by Theorem 3, we have to obtain certain $s+1$ matrices with no rows in common. Since the rows of length $\delta+\gamma$ must have 1 in the first coordinate, and elements from $\{0, 2\}$ in the last γ coordinates, the number of possible rows is $4^{\delta-1}2^\gamma = 2^{\gamma+2\delta-2}$. Thus, taking this fact into account and counting the number of rows of each one of these $s+1$ matrices, we have that $(s+1)(\gamma+\delta) \le 2^{\gamma+2\delta-2}$, and the result follows. *H*

We know that the Z_4-linear Hadamard codes $H_{\gamma,\delta}$ of length 2^m with $\delta = 1$ or $\delta = 2$ are equivalent to the binary linear Hadamard codes H_m of length 2^m [14]. However, the results given in Section 4 for these codes will always be better than the ones obtained by using Theorem 3, since $f_{\gamma,\delta} \le f_m$, where $m = \gamma + 2\delta - 1$.

Example 4 In Example 1, a 2-PD-set of size 3 for H_4 is given. The code H_4 is equivalent to both Z_4-linear Hadamard codes $H_{1,2}$ and $H_{3,1}$. However, a 2-PD-set of size 3 is not achievable by using Theorem 3, since $f_{1,2} = f_{3,1} = 1$.

Example 5 A 4-PD-set of size 5 for H_5 can be constructed by Theorem 2, since $f_5 = 4$. However, considering H_5 as the Gray map image of $H_{2,2}$ or $H_{4,1}$, no more than a 3-PD-set of size 4 can be found by using Theorem 3, since $f_{4,1} = 2$ and $f_{2,2} = 3$.

Next, by using Theorem 3, we give an explicit construction of s-PD-sets of minimum size $s+1$ for $H_{0,\delta}$, for all $\delta \ge 3$ and $2 \le s \le f_{0,\delta}$. Let $R = \mathrm{GR}(4^{\delta-1})$ be the Galois extension of dimension $\delta - 1$ over Z_4. It is known that R is isomorphic to $Z_4[x]/(h(x))$, where $h(x)$ is a monic basic irreducible polynomial of degree $\delta - 1$. Let $f(x) \in Z_2[x]$ be a primitive polynomial of degree $\delta - 1$. Let $A = 2^{\delta-1} - 1$. There is a unique primitive basic irreducible polynomial $h(x)$ dividing $x^A - 1$ in $Z_4[x]$ and such that $\mu(h(x)) = f(x)$, where μ is the map that

performs modulo 2 to all coefficients of $h(x)$. Let $T = \{0, 1, \alpha, \ldots, \alpha^{A-1}\} \subseteq R$, where α is a root of $h(x)$. It is well known that any $r \in R$ can be written uniquely as $r = a + 2b$, where $a, b \in T$. We take R as the ordered set:

$$R = \{r_1, \ldots, r_{4\delta^{-1}}\}$$
$$= \{0 + 2 \cdot 0, \ldots, \alpha^{A-1} + 2 \cdot 0, \ldots, 0 + 2 \cdot \alpha^{A-1}, \ldots, \alpha^{A-1} + 2 \cdot \alpha^{A-1}\}.$$

Since $|R|/\delta = f_{0,\delta} + 1$, we can form $f_{0,\delta} + 1$ disjoints sets of R of size δ. For $i \in \{0, \ldots, f_{0,\delta}\}$, we consider the $\delta \times \delta$ quaternary matrices

$$N_i^* = \begin{bmatrix} & & 1 & r_{\delta i+1} & \\ & \iddots & \vdots & & \vdots \\ 1 & r_{\delta(i+1)} & & & \end{bmatrix}.$$

Theorem 4 *Let $P_s = \{M_i : 0 \le i \le s\}$, where $M_i = N_i^{-1}$. Then, $\Phi(P_s)$ is an s-PD-set of size $s + 1$ for the Z_4-linear Hadamard code $H_{0,\delta}$ of length $2^{2\delta-1} = 2^m$ with information set $\Phi(I_{0,\delta})$, for all $\delta \ge 3$ and $2 \le s \le f_{0,\delta} = f_m$.*

Proof We need to prove that $r_{\delta i+2} - r_{\delta i+1}, \ldots, r_{\delta(i+1)} - r_{\delta i+1}$ are linearly independent over Z_4, for all $i \in \{0, \ldots, f_{0,\delta}\}$, in order to guarantee that $N_i \in \mathrm{PAut}(H_{0,\delta})$. Note that these vectors are not zero divisors [9]. Since $\alpha^A = 1$, $\{r_{\delta i+2} - r_{\delta i+1}, \ldots, r_{\delta(i+1)} - r_{\delta i+1}\}$ is one of the following three sets:

$L_1 = \{1, \ldots, \alpha^{\delta-2}\}$,
$L_2 = \{\alpha^{k+1} - \alpha^k, \ldots, \alpha^{k+\delta-1} - \alpha^k\}$, for some $k \in \{0, \ldots, A - 1\}$,
$L_3 = \{\alpha^{k+1} - \alpha^k, \ldots, \alpha^{A-1} - \alpha^k, -\alpha^k + 2(b_j - b_i), \alpha^A - \alpha^k + 2(b_j - b_i), \ldots,$
$\alpha^{k+\delta-2} - \alpha^k + 2(b_j - b_i)\}$, for some $b_i, b_j \in T$ and $k \in \{0, \ldots, A - 1\}$.

The elements in L_1 are clearly linearly independent over Z_4. Now, we prove that the same property is satisfied in L_2. Assume on the contrary that there are some $\lambda_i \ne 0, i \in \{1, \ldots, \delta-1\}$, such that $\sum \lambda_i(\alpha^{k+i} - \alpha^k) = 0$. If $\lambda_i \in \{1, 3\}$ for at least one $i \in \{1, \ldots, \delta-1\}$, we get a contradiction. Indeed, if we take modulo 2 in the previous linear combination, we obtain that $\sum \bar{\lambda}_i(\bar{\alpha}^{k+i} - \bar{\alpha}^k) = 0$, where $\bar{\lambda}_i \in Z_2$ and at least one $\bar{\lambda}_i \ne 0$. This is a contradiction by Lemma 2. On the other hand, if $\lambda_i \in \{0, 2\}$ for all $i \in \{1, \ldots, \delta - 1\}$ and there is at least one $\lambda_i = 2$, then $\sum 2\lambda'_i(\alpha^{k+i} - \alpha^k) = 2[\sum \lambda'_i(\alpha^{k+i} - \alpha^k)] = 0$, where $\lambda'_i \in \{0, 1\}$ and at least one $\lambda'_i = 1$. Hence, $\sum \lambda'_i(\alpha^{k+i} - \alpha^k) = 2\lambda$ for some $\lambda \in R$, that is, it is a zero divisor. By taking modulo 2, we obtain a contradiction by Lemma 2.

We show that the elements in $L_3 = \{v_1, \ldots, v_{\delta-1}\}$ are also linearly independent over Z_4 by using a slight modification of the previous argument. Suppose that there is at least one $\lambda_i \ne 0, i \in \{1, \ldots, \delta - 1\}$ such that $\sum \lambda_i v_i = 0$. By taking modulo 2, we obtain that $\bar{\lambda}_{\delta-1}\bar{\alpha}^k + \sum \bar{\lambda}_i(\bar{\alpha}^{k+i} - \bar{\alpha}^k) = \bar{\alpha}^k[\bar{\lambda}_{\delta-1} + \sum \bar{\lambda}_i(\bar{\alpha}^i - 1)] = 0$. Since $\bar{\alpha}^k$ is a unit, it follows that $\lambda_{\delta-1} + \sum \lambda_i(\bar{\alpha} - 1) = 0$, which gives a contradiction if $\lambda_i \in \{1, 3\}$ for at least one index, since $1, \bar{\alpha} - 1, \ldots, \bar{\alpha}^{\delta-2} - 1$ are linearly independent over Z_2. If $\lambda_i \in \{0, 2\}$ for all $i \in \{1, \ldots, \delta - 1\}$, we get a contradiction by applying a similar argument to the one used above.

Finally, by construction, the matrices $N_0^*, \ldots, N_s^*$ have no rows in common and the result follows by Theorem 3. H

The bound f_m is always attained for $H_{0,\delta}$ despite the elements of the f_m-PD-set belong to the subgroup $\Phi(\mathrm{PAut}(H_{0,\delta})) \leq \mathrm{PAut}(H_{0,\delta})$, since $f_m = f_{0,\delta}$.

Example 6 Let $H_{0,3}$ be the quaternary linear Hadamard code of length 16 and type $2^0 4^3$. Let $R = \mathbb{Z}_4[x]/(h(x))$, where $h(x) = x^2 + x + 1$. Note that $h(x)$ is a primitive basic irreducible polynomial dividing $x^3 - 1$ in $\mathbb{Z}_4[x]$. Let α be a root of $h(x)$. Then, $T = \{0, 1, \alpha, \alpha^2\}$ and $R = \{r_1, \ldots, r_{16}\} = \{0, 1, \alpha, 3+3\alpha, 2, 3, 2+\alpha, 1+3\alpha, 2\alpha, 1+2\alpha, 3\alpha, 3+\alpha, 2+2\alpha, 3+2\alpha, 2+3\alpha, 1+\alpha\}$. Let $P_4 = \{N_0^{-1}, N_1^{-1}, N_2^{-1}, N_3^{-1}, N_4^{-1}\}$, where $N_0 = \mathrm{Id}_3$,

$$N_1 = \begin{bmatrix} 1 & 3 & 3 \\ 0 & 3 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \quad N_2 = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 3 & 2 \\ 0 & 2 & 1 \end{bmatrix}, \quad N_3 = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 3 & 1 \\ 0 & 2 & 3 \end{bmatrix}, \text{ and } N_4 = \begin{bmatrix} 1 & 2 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Note that $P_4 \subseteq \mathrm{PAut}(H_{0,3})$. By Theorem 4, $\Phi(P_4)$ is a 4-PD-set of size 5 for $H_{0,3}$. Note that the matrices $N_0^* = \mathrm{Id}_3^*$ and N_i^*, $i \in \{1, \ldots, 4\}$, have no rows in common, where

$$N_1^* = \begin{bmatrix} 1 & 3 & 3 \\ 1 & 2 & 0 \\ 1 & 3 & 0 \end{bmatrix}, \quad N_2^* = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 1 & 3 \\ 1 & 0 & 2 \end{bmatrix}, \quad N_3^* = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 0 & 3 \\ 1 & 3 & 1 \end{bmatrix}, \text{ and } N_4^* = \begin{bmatrix} 1 & 2 & 2 \\ 1 & 3 & 2 \\ 1 & 2 & 3 \end{bmatrix}.$$

7 Recursive constructions of s-PD-sets for $\mathbb{Z}_4$-linear Hadamard codes

Given a matrix $M \in \mathrm{PAut}(H_{\gamma,\delta})$ and an integer $\kappa \geq 1$, we define

$$M(\kappa) = \begin{bmatrix} 1 & \eta & \mathbf{0} & 2\theta \\ \mathbf{0} & A & \mathbf{0} & 2X \\ \mathbf{0} & \mathbf{0} & \mathrm{Id}_\kappa & \mathbf{0} \\ \mathbf{0} & \zeta(Y) & \mathbf{0} & \zeta(B) \end{bmatrix}.$$

Proposition 6 *Let $P_s = \{M_0, \ldots, M_s\} \subseteq \mathrm{PAut}(H_{\gamma,\delta})$ such that $\Phi(P_s)$ is an s-PD-set of size $s+1$ for $H_{\gamma,\delta}$ with information set $\Phi(I_{\gamma,\delta})$. Then, $Q_s = \{(M_0^{-1}(\kappa))^{-1}, \ldots, (M_s^{-1}(\kappa))^{-1}\} \subseteq \mathrm{PAut}(H_{\gamma+i,\delta+j})$ and $\Phi(Q_s)$ is an s-PD-set of size $s+1$ for $H_{\gamma+i,\delta+j}$ with information set $\Phi(I_{\gamma+i,\delta+j})$, for any $i, j \geq 0$ such that $i + j = \kappa \geq 1$.*

Proof Note that if $M \in \mathrm{PAut}(H_{\gamma,\delta})$, then $M(\kappa) \in \mathrm{GL}(\gamma + \delta + \kappa, \mathbb{Z}_4)$. Taking this into account, together with the fact that Id_κ can split as

$$\mathrm{Id}_\kappa = \begin{bmatrix} \mathrm{Id}_j & \mathbf{0} \\ \mathbf{0} & \mathrm{Id}_i \end{bmatrix},$$

where $i + j = \kappa \geq 1$, it is clear that $M^{-1}(\kappa) \in \mathrm{PAut}(H_{\gamma+i,\delta+j})$ and so its inverse. Thus, $Q_s \subseteq \mathrm{PAut}(H_{\gamma+i,\delta+j})$. Finally, repeated rows in the matrices $(M_0^{-1}(\kappa))^*, \ldots, (M_s^{-1}(\kappa))^*$ cannot occur, since this fact would imply repeated rows in the matrices $(M_0^{-1})^*, \ldots, (M_s^{-1})^*$ by construction. The result follows from Theorem 3. H

Example 7 Let $P_4 = \{M_0, \ldots, M_4\} \subseteq \mathrm{PAut}(H_{0,3})$ be the set, given in Example 6, such that $\Phi(P_4)$ is a 4-PD-set of size 5 for $H_{0,3}$. By Proposition 6, $Q_4 = \{M_i^{-1}(1))^{-1} : 0 \le i \le 4\}$ is contained in both $\mathrm{PAut}(H_{1,3})$ and $\mathrm{PAut}(H_{0,4})$. Moreover, $\Phi(Q_4)$ is a 4-PD-set of size 5 for $H_{1,3}$ and $H_{0,4}$. Nevertheless, note that the construction of $(M_i^{-1}(1))^*$ depends on the group where $M_i^{-1}(1)$ is considered.

As for binary linear Hadamard codes, a second recursive construction considering the elements of $\mathrm{PAut}(H_{\gamma,\delta})$ as permutations of coordinate positions, that is as elements of $\mathrm{Sym}(2^m)$, can also be provided. Given four permutations $\sigma_i \in \mathrm{Sym}(n_i)$, $i \in \{1, \ldots, 4\}$, we define $(\sigma_1|\sigma_2|\sigma_3|\sigma_4) \in \mathrm{Sym}(n_1+n_2+n_3+n_4)$ in the same way as we defined $(\sigma_1|\sigma_2) \in \mathrm{Sym}(n_1 + n_2)$ in Section 5.

Proposition 7 *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 (5) and the Gray map, with any information set $I^r = I \cup \{i + n\}$, $i \in I$.*

Proof Since $H_{\gamma+1,\delta} = \{(x, x), (x, \bar{x}) : x \in H_{\gamma,\delta}\}$, where $\bar{x}$ is the complementary vector of x, the result follows using the same argument as in the proof of Proposition 4. By the proof of Proposition 5, we can add any of the coordinate positions of $\{i + n : i \in I\}$ to I in order to form a suitable information set I^r for $H_{\gamma+1,\delta}$. H

Let $2S = 2^1S$ denote the set $(S|S)$ and, recursively, $2^iS = 2(2^{i-1}S)$.

Corollary 5 *Let $P_s = \{M_i : 0 \le i \le s\}$, where $M_i = N_i^{-1}$. Then, $2^\gamma \Phi(P_s)$ is an s-PD-set of size $s + 1$ for the Z_4-linear Hadamard code $H_{\gamma,\delta}$, for all $\gamma \ge 0$, $\delta \ge 3$ and $2 \le s \le f_{0,\delta}$.*

Proof By Theorem 4 and Proposition 7, we can construct $f_{0,\delta}$-PD-sets of size $f_{0,\delta}+1$ for $H_{\gamma,\delta}$, for all $\gamma \ge 0$ and $\delta \ge 3$. H

Proposition 7 cannot be generalized directly for Z_4-linear Hadamard codes $H_{\gamma,\delta+1}$ constructed from (6) and the Gray map. Note that if S is an s-PD-set for $H_{\gamma,\delta}$, then $(S|S|S|S) = \{(\sigma|\sigma|\sigma|\sigma) : \sigma \in S\}$ is not always an s-PD-set for $H_{\gamma,\delta+1}$, since in general $(\sigma|\sigma|\sigma|\sigma) \notin \mathrm{PAut}(H_{\gamma,\delta})$. For example, $\sigma = (1, 5)(2, 8, 3, 6, 4, 7) \in \mathrm{PAut}(H_{0,2}) \subseteq \mathrm{Sym}(8)$, but $\pi = (\sigma|\sigma|\sigma|\sigma) \notin \mathrm{PAut}(H_{0,3}) \subseteq \mathrm{Sym}(32)$, since $\pi(\Phi((0, 0, 0, 0, 1, 1, 1, 1, 2, 2, 2, 2, 3, 3, 3, 3))) = \Phi((0, 0, 0, 0, 0, 2, 0, 2, 2, 2, 2, 2, 2, 0, 2, 0)) \notin H_{0,3}$.

Proposition 8 *Let $S \subseteq \mathrm{PAut}(H_{\gamma,\delta})$ such that $\Phi(S)$ is 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, $\Phi((S|S|S|S)) = \{\Phi((\tau|\tau|\tau|\tau)) : \tau \in S\}$ is an s-PD-set of size l for $H_{\gamma,\delta+1}$ of length $4n$ and type $2^\gamma 4^{\delta+1}$ constructed from (6) and the Gray map, with any information set $I^{rr} = I \cup \{i + n, j + n\}$, $i, j \in I$ and $i \neq j$.*

Proof Since $H_{\gamma,\delta+1}$ is constructed from (6), $H_{\gamma,\delta+1} = \{(u, u, u, u), (u, u+\mathbf{1}, u+\mathbf{2}, u+\mathbf{3}), (u, u+\mathbf{2}, u, u+\mathbf{2}), (u, u+\mathbf{3}, u+\mathbf{2}, u+\mathbf{1}) : u \in H_{\gamma,\delta}\}$. It is easy to see that if $\tau \in \mathrm{PAut}(H_{\gamma,\delta})$, then $(\tau|\tau|\tau|\tau) \in \mathrm{PAut}(H_{\gamma,\delta+1})$.

Let $\sigma = \Phi(\tau)$. Finally, we need to prove that for every $e \in Z_2^{4n}$ with $\mathrm{wt}(e) \leq s$, there is $(\sigma|\sigma|\sigma|\sigma) \in \Phi((S|S|S|S))$ such that $(\sigma|\sigma|\sigma|\sigma)(e)_{I^{rr}} = \mathbf{0}$, where $I^{rr} \subseteq \{1, \ldots, 4n\}$ is an information set for $H_{\gamma,\delta+1}$ with $\gamma + 2(\delta + 1)$ coordinate positions. Using a similar argument to that given in the proofs of Propositions 4 and 7, the result follows. Moreover, by the proof of Proposition 5, any $I^{rr} = I \cup \{i + n, j + n\}$ with $i, j \in I$ and $i \neq j$ is an information set for $H_{\gamma,\delta+1}$. ∎

Corollary 6 *Let $S \subseteq \mathrm{PAut}(H_{\gamma,\delta})$ such that $\Phi(S)$ is an s-PD-set of size l for $H_{\gamma,\delta}$ of length 2^m and type $2^\gamma 4^\delta$ with information set I. Then, $\Phi(2^{i+2j}S)$ is an s-PD-set of size l for $H_{\gamma+i,\delta+j}$ of length 2^{m+i+2j} and type $2^{\gamma+i}4^{\delta+j}$ with information set obtained by applying recursively Proposition 5, for all $i, j \geq 0$.*

Proof The result comes trivially by applying Propositions 5, 7 and 8. ∎

8 Computational results

Magma software supports the basic facilities for linear codes over finite fields, integer residue rings and Galois rings [4]. A new package that expands the current functionality for binary linear and Z_4-linear codes, including functions to decode using different methods, has been developed by the authors. It includes functions to perform permutation decoding, to obtain the s-PD-sets described in the previous sections, and to check whether or not a set of permutations is an s-PD-set with respect to an information set. Magma version 2.22 (from May 2016) and later contains these functions by default [4, Chapters 158 and 162], and they can also be downloaded from http://ccsg.uab.cat.

Using the functions implemented in this package, it is possible to easily improve the result given by Corollary 5 for $H_{\gamma,\delta}$ with $\gamma > 0$, that is, to obtain s-PD-sets of size $s + 1$ for $f_{0,\delta} < s \leq f_{\gamma,\delta}$ by using a nondeterministic method. Table 1 summarizes these computational results for the codes $H_{\gamma,\delta}$ with $3 \leq \delta \leq 6$ and $1 \leq \gamma \leq 5$. Specifically, for each one of these codes, the values of $f_{0,\delta}$ and $f_{\gamma,\delta}$ are shown, together with the maximum s for which an s-PD-set of size $s+1$ has been found. Note that all these found s-PD-sets are constructed by using only elements from $\Phi(\mathrm{PAut}(H_{\gamma,\delta}))$, which is a subgroup of the whole automorphism group of $H_{\gamma,\delta}$.

Even when the nondeterministic method fails to quickly find a $f_{\gamma,\delta}$-PD-set of minimum size $f_{\gamma,\delta} + 1$, the bound $f_{\gamma,\delta}$ may be attained by using only elements in $\Phi(\mathrm{PAut}(H_{\gamma,\delta}))$ as shown in Example 8. Nevertheless, we have not been able to generalize this example to find an explicit construction in this case. The monomial automorphism group $\mathrm{MAut}(H_{\gamma,\delta})$ and the permutation automorphism group $\mathrm{PAut}(H_{\gamma,\delta})$ may be considered to achieve this goal.

Example 8 Let the ordered set R and the matrices $N^*, \ldots, N^*$ be as in Example 6. Define $\bar{r} = (1, r) \in \{1\} \times Z_4^2$ for all $r \in R$. Let $P_7 = \{A_i^{3-1} : 0 \leq i \leq 7\}$,

δ	γ	$f_{0,\delta}$	s	$f_{\gamma,\delta}$
3	1	4	6	7
	2	4	10	11
	3	4	16	20
	4	4	26	35
	5	4	42	63
4	1	15	23	24
	2	15	36	41
	3	15	56	72
	4	15	91	127
	5	15	150	226

δ	γ	$f_{0,\delta}$	s	$f_{\gamma,\delta}$
5	1	50	72	84
	2	50	116	145
	3	50	187	255
	4	50	312	454
	5	50	518	818
6	1	169	230	291
	2	169	377	511
	3	169	630	909
	4	169	1040	1637
	5	169	1784	2977

Table 1 Maximum s-PD-sets found computationally for some codes $H_{\gamma,\delta}$

where A_i^* are the following matrices:

$$\begin{bmatrix} N_0^* & \mathbf{0} \\ r_{13} & 2 \end{bmatrix}, \quad \begin{bmatrix} N_1^* & \mathbf{0} \\ r_{16} & 2 \end{bmatrix}, \quad \begin{bmatrix} N_2^* & \mathbf{0} \\ r_{15} & 2 \end{bmatrix}, \quad \begin{bmatrix} N_3^* & \mathbf{0} \\ \bar{r}_{14} & 2 \end{bmatrix},$$

$$\begin{bmatrix} N_0^* & \mathbf{2} \\ r_{13} & 0 \end{bmatrix}, \quad \begin{bmatrix} N_1^* & \mathbf{2} \\ r_{16} & 0 \end{bmatrix}, \quad \begin{bmatrix} N_2^* & \mathbf{2} \\ r_{15} & 0 \end{bmatrix}, \quad \begin{bmatrix} N_3^* & \mathbf{2} \\ \bar{r}_{14} & 0 \end{bmatrix}.$$

By Theorem 3, one can easily check that $\Phi(P_7) \subseteq \mathrm{PAut}(H_{1,3})$ is a 7-PD-set of size 8 for $H_{1,3}$ of length 64 with information set $\Phi(I_{1,3}) = \{1, 2, 3, 4, 9, 10, 33\}$. Since $f_{1,3} = 7$, no better s-PD-sets of size $s + 1$ can be provided for $H_{1,3}$ by using Theorem 3. However, an 8-PD-set of size 9 could be theoretically found in $\mathrm{PAut}(H_{1,3})$ since $f_6 = 8$.

9 Conclusions

An alternative permutation decoding method that can be applied to Z_2Z_4-linear codes [3], which include Z_4-linear codes, was presented in [2]. However, the determination of PD-sets for some families of Z_2Z_4-linear codes remained an open question. In this paper, s-PD-sets of minimum size $s+1$ for binary linear and Z_4-linear Hadamard codes are constructed. This approach establishes equivalent results to the ones obtained for simplex codes in [5]. For binary linear codes H_m and (nonlinear) Z_4-linear Hadamard codes $H_{0,\delta}$ of length 2^m, s-PD-sets of size $s + 1$ with s up to the upper bound $f_m = f_{0,\delta}$ are constructed. Moreover, for (nonlinear) Z_4-linear Hadamard codes $H_{\gamma,\delta}$, s-PD-sets of size $s + 1$ up to $f_{0,\delta}$ are given. However, it still remains to find an explicit construction of s-PD-sets of size $s + 1$ for $H_{\gamma,\delta}$ with $\gamma > 0$ and $\delta \geq 3$ for $f_{0,\delta} < s \leq f_{\gamma,\delta}$.

References

1. R. D. Barrolleta and M. Villanueva, "Partial permutation decoding for binary linear Hadamard codes," *Electron. Note Discr. Math.* **46**, 35–42 (2014).

2. J. J. Bernal, J. Borges, C. Fernández-Córboda, and M. Villanueva, "Permutation decoding of Z_2Z_4-linear codes," *Des. Codes and Cryptogr.* **76**(2), 269–277 (2015).
3. J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. Villanueva, "Z_2Z_4-linear codes: generator matrices and duality," *Des. Codes and Cryptogr.* **54**(2), 167–179 (2010).
4. W. Bosma, J. J. Cannon, C. Fieker, and A. Steel (Eds.), "Handbook of Magma Functions," Edition 2.22, 5669 pages (2016).
5. W. Fish, J. D. Key, and E. Mwambene, "Partial permutation decoding for simplex codes," *Adv. Math. Commun.* **6**(4), 505–516 (2012).
6. D. M. Gordon, "Minimal permutation sets for decoding the binary Golay codes," *IEEE Trans. Inf. Theory* **28**(3), 541–543 (1982).
7. W. C. Huffman, "Codes and groups", *Handbook of Coding Theory*, eds. V. S. Pless and W. C. Huffman, Elsevier (1998).
8. W.C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press (2003).
9. 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. Inf. Theory* **40**(2), 301–319 (1994).
10. J. D. Key, T. P. McDonough, and V. C. Mavron, "Reed-Muller codes and permutation decoding," *Discrete Math.* **310**(22), 3114–3119 (2010).
11. J. D. Key, T. P. McDonough, and V. C. Mavron, "Improved partial permutation decoding for Reed-Muller codes," *Discrete Math.* **340**(4), 722–728 (2017).
12. H.-J. Kroll and R. Vincenti, "PD-sets for binary RM-codes and the codes related to the Klein quadric and to the Schubert variety of PG(5,2)," *Discrete Math.* **308**(2–3), 408–414 (2008).
13. D. S. Krotov and M. Villanueva "Classification of the Z_2Z_4-linear Hadamard codes and their automorphism groups," *IEEE Trans. Inf. Theory* **61**(2), 887–894 (2015).
14. D. S. Krotov, "Z_4-linear Hadamard and extended perfect codes," *Electron. Note Discr. Math.* **6**, 107-112 (2001).
15. F. J. MacWilliams, "Permutation decoding of systematics codes," *Bell System Tech. J.* **43**, 485–505 (1964).
16. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company (1977).
17. 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).
18. K.T. Phelps, J. Rifà, and M. Villanueva, "On the additive (Z_4-linear and non-Z_4-linear) Hadamard codes: rank and kernel," *IEEE Trans. Inf. Theory* **52**(1), 316–319 (2006).
19. E. Prange, "The use of information sets in decoding cyclic codes," *IRE Trans. Inf. Theory* **8**(5), 5–9 (1962).
20. J. Schönheim, "On coverings," *Pacific J. Math.* **14**, 1405–1411 (1964).
21. P. Seneviratne, "Partial permutation decoding for the first-order Reed–Muller codes," *Discrete Math.* **309**(8), 1967–1970 (2009).
22. J. Wolfmann, "A permutation decoding of the (24,12,8) Golay code," *IEEE Trans. Inf. Theory* **29**(5), 748–750 (1983).
23. Z.-X. Wan, *Quaternary Codes*, World Scientific (1997).