Finite Fields and Their Applications 93 (2024) 102316

Contents lists available at ScienceDirect

Finite Fields and Their Applications

journal homepage: www.elsevier.com/locate/ffa

Partial permutation decoding and PD-sets for $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes ☆,☆☆

Adrián Torres-Martín *, Mercè Villanueva

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

ARTICLE INFO

Article history:
Received 6 March 2023
Received in revised form 20 September 2023
Accepted 5 October 2023
Available online 20 October 2023
Communicated by Gary L. Mullen

MSC:
94B25
94B60

Keywords:
Permutation decoding
PD-set
Automorphism group
Generalized Hadamard code
$\mathbb{Z}_{p^s}$-linear code
Gray map

ABSTRACT

It is known that $\mathbb{Z}_{p^s}$-linear codes, which are the Gray map image of $\mathbb{Z}_{p^s}$-additive codes (linear codes over $\mathbb{Z}_{p^s}$), are systematic and a systematic encoding has been found. This makes $\mathbb{Z}_{p^s}$-linear codes suitable to apply the permutation decoding method. This technique is also based on the existence of r-PD-sets, which are subsets of the permutation automorphism group of the code. In this paper, we study the permutation automorphism group of $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes of type $(n; t_1, \ldots, t_s)$ and show how to construct r-PD-sets of size $r+1$, for all r up to an upper bound, in order to be able to perform a partial permutation decoding for these codes.

☆ This work has been partially supported by the Spanish Ministerio de Ciencia e Innovación under Grants PID2019-104664GB-I00, PID2022-137924NB-I00, and RED2022-134306-T (AEI / 10.13039/501100011033) and by the Agència de Gestió d'Ajuts Universitaris i de Recerca, Generalitat de Catalunya grant 2021SGR 00643.

☆☆ The material in this paper was presented in part at the 2022 IEEE Information Theory Workshop in Mumbai, India, November 2022 [33].

* Corresponding author.
E-mail address: adrian.torres@uab.cat (A. Torres-Martín).

https://doi.org/10.1016/j.ffa.2023.102316

1. Introduction

Let $\mathbb{Z}_{p^s}$ be the ring of integers modulo p^s with $s \geq 1$ and p prime, and $\mathbb{Z}_{p^s}^n$ be the set of n-tuples over $\mathbb{Z}_{p^s}$. In this paper, the elements of $\mathbb{Z}_{p^s}^n$ are also called vectors over $\mathbb{Z}_{p^s}$ of length n. A *code* over $\mathbb{Z}_p$ of length n is a nonempty subset of $\mathbb{Z}_p^n$, and it is *linear* if it is a subspace of $\mathbb{Z}_p^n$. A nonempty subset of $\mathbb{Z}_{p^s}^n$ is a $\mathbb{Z}_{p^s}$*-additive code* if it is a subgroup of $\mathbb{Z}_{p^s}^n$. Note that, when $p = 2$ and $s = 1$, a $\mathbb{Z}_{p^s}$-additive code is a binary linear code and, when $p = 2$ and $s = 2$, it is a quaternary linear code or a linear code over $\mathbb{Z}_4$.

Let $\mathcal{S}_n$ be the *symmetric group of permutations* on the set $\{1, \ldots, n\}$. Two codes over $\mathbb{Z}_p$ of length n, C_1 and C_2, are said to be *permutation equivalent* if there is a permutation of coordinates $\pi \in \mathcal{S}_n$ such that $C_2 = \{\pi(\mathbf{c}) : \mathbf{c} \in C_1\}$. Two $\mathbb{Z}_{p^s}$-additive codes of length n, $\mathcal{C}_1$ and $\mathcal{C}_2$, are said to be *permutation equivalent* if they differ only by a permutation of coordinates, that is, if there is a permutation of coordinates $\pi \in \mathcal{S}_n$ such that $\mathcal{C}_2 = \{\pi(\mathbf{c}) : \mathbf{c} \in \mathcal{C}_1\}$.

The *Hamming weight* of a vector $\mathbf{u} \in \mathbb{Z}_p^n$, denoted by $\mathrm{wt}_H(\mathbf{u})$, is the number of nonzero coordinates of $\mathbf{u}$. The *Hamming distance* of two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_p^n$, denoted by $d_H(\mathbf{u}, \mathbf{v})$, is the number of coordinates in which they differ. Note that $d_H(\mathbf{u}, \mathbf{v}) = \mathrm{wt}_H(\mathbf{v} - \mathbf{u})$. The *minimum distance* of a code C over $\mathbb{Z}_p$ is $d(C) = \min\{d_H(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\}$. For elements of $\mathbb{Z}_{p^s}$, we consider the following metric, defined in [12], and also used in [19,31]:

$$\mathrm{wt}^*(x) = \begin{cases} 0 & \text{if } x = 0, \\ p^{s-1} & \text{if } x \in p^{s-1}\mathbb{Z}_{p^s} \setminus \{0\}, \\ (p-1)p^{s-2} & \text{otherwise.} \end{cases} \tag{1}$$

The *weight* of a vector $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{Z}_{p^s}^n$ is $\mathrm{wt}^*(\mathbf{u}) = \sum_{j=1}^n \mathrm{wt}^*(u_j) \in \mathbb{Z}_{p^s}$; and the *distance* between two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_{p^s}^n$ is $d^*(\mathbf{u}, \mathbf{v}) = \mathrm{wt}^*(\mathbf{u} - \mathbf{v})$. The *minimum distance* of a code $\mathcal{C}$ over $\mathbb{Z}_{p^s}$ is $d^*(\mathcal{C}) = \min\{d^*(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in \mathcal{C}, \mathbf{u} \neq \mathbf{v}\}$.

In [20,27], a *Gray map* from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ is defined as $\phi(0) = (0,0)$, $\phi(1) = (0,1)$, $\phi(2) = (1,1)$ and $\phi(3) = (1,0)$. There exist different generalizations of this Gray map, which go from $\mathbb{Z}_{2^s}$ to $\mathbb{Z}_2^{2^{s-1}}$ [10,13,23]. The one given by Krotov in [23] is defined in terms of the codewords of a Hadamard code, and the one given by Carlet in [10] is a particular case of Krotov's one satisfying $\sum \lambda_i \phi_s(2^i) = \phi_s(\sum \lambda_i 2^i)$ [15]. In this paper, we consider a generalization of Carlet's Gray map, denoted by ϕ_s and defined as follows:

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

where $u \in \mathbb{Z}_{p^s}$, $[u_0, u_1, \ldots, u_{s-1}]_p$ is the p-ary expansion of u, that is $u = \sum_{i=0}^{s-1} p^i u_i$ ($u_i \in \mathbb{Z}_p$), and Y_{s-1} is a matrix of size $(s-1) \times p^{s-1}$ whose columns are the elements of $\mathbb{Z}_p^{s-1}$. Note that the rows of Y_{s-1} form a basis of a first order Reed-Muller code after adding the all-one row. This Gray map ϕ_s is an isometric embedding from $(\mathbb{Z}_{p^s}, d^*)$ into $(\mathbb{Z}_p^{p^{s-1}}, d_H)$ [19,31]. If $s = 1$, then ϕ_s is the identity map. In order to simplify the

notation, we write ϕ instead of ϕ_s, when s is clear from the context. Then, we define $\Phi : \mathbb{Z}_{p^s}^n \to \mathbb{Z}_p^{np^{s-1}}$ as the component-wise extension of ϕ.

Let $\mathcal{C}$ be a $\mathbb{Z}_{p^s}$-additive code of length n. We say that its Gray map image, $C = \Phi(\mathcal{C})$, is a $\mathbb{Z}_{p^s}$*-linear code* of length $p^{s-1}n$. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_{p^s}^n$, it is isomorphic to an abelian structure $\mathbb{Z}_{p^s}^{t_1} \times \mathbb{Z}_{p^{s-1}}^{t_2} \times \cdots \times \mathbb{Z}_p^{t_s}$, and we say that $\mathcal{C}$, or equivalently $C = \Phi(\mathcal{C})$, is of *type* $(n; t_1, \ldots, t_s)$. Note that $|\mathcal{C}| = p^{st_1}p^{(s-1)t_2} \cdots p^{t_s}$. Unlike linear codes over finite fields, linear codes over rings do not have a basis, but there exists a generator matrix for these codes having minimum number of rows, that is, $t_1 + \cdots + t_s$ rows.

A *generalized Hadamard* (GH) *matrix* $H(p, \lambda) = (h_{ij})$ of order $N = p\lambda$ over $\mathbb{Z}_p$ is a $p\lambda \times p\lambda$ matrix with entries in $\mathbb{Z}_p$ with the property that, for every i, j, $1 \leq i < j \leq p\lambda$, each of the multisets $\{h_{ik} - h_{jk} : 1 \leq k \leq p\lambda\}$ contains every element of $\mathbb{Z}_p$ exactly λ times [22]. Two GH matrices H_1 and H_2 of order N are said to be *equivalent* if one can be obtained from the other by a permutation of the rows and columns and adding the same element of $\mathbb{Z}_p$ to all the coordinates in a row or in a column. We can always change the first row and column of a GH matrix into zeros, obtaining an equivalent GH matrix which is called *normalized*. From a GH matrix H, the *generalized Hadamard* (GH) *code* is $C_H = \bigcup_{\alpha \in \mathbb{Z}_p}(F_H + \alpha\mathbf{1})$, where $F_H + \alpha\mathbf{1} = \{\mathbf{h} + \alpha\mathbf{1} : \mathbf{h} \in F_H\}$, F_H is the code consisting of the rows of H, and $\mathbf{1}$ denotes the all-one vector [14]. Note that C_H is not necessarily linear as a code over $\mathbb{Z}_p$.

A $\mathbb{Z}_{p^s}$-additive code $\mathcal{C}$ such that $\Phi(\mathcal{C})$ is a GH code is called a $\mathbb{Z}_{p^s}$*-additive GH code* and $\Phi(\mathcal{C})$ is called a $\mathbb{Z}_{p^s}$*-linear GH code*. Note that a GH code over $\mathbb{Z}_p$ of length N has pN codewords and minimum distance $(p-1)N/p$. The $\mathbb{Z}_4$-linear Hadamard codes of length 2^t have been studied and classified in [24,29], and their automorphism groups have been characterized in [25,28]. For $s > 2$, $\mathbb{Z}_{2^s}$-linear Hadamard codes where first introduced in [23]. A full classification of $\mathbb{Z}_8$-linear Hadamard codes is provided in [16]. For $s > 3$, a partial classification and bounds on the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t can be found in [15]. More generally, for any $s \geq 2$ and p prime, $\mathbb{Z}_{p^s}$-linear GH codes are studied and partially classified in [5,6]. Moreover, it is proved that, for $p \geq 3$, the $\mathbb{Z}_{p^s}$-linear GH codes of type $(n; 1, 0, \ldots, 0, t_s)$ are the only ones which are linear [5]. For $p = 2$, they are only linear when their type is $(n; 1, 0, \ldots, 0, t_s)$ or $(n; 1, 0, \ldots, 0, 1, t_s)$ [15].

Let C be a code over $\mathbb{Z}_p$ of length n with p^k codewords. For a vector $\mathbf{u} \in \mathbb{Z}_p^n$ and a set $I \subseteq \{1, \ldots, n\}$, we denote the projection of $\mathbf{u}$ to the coordinates of I by $\mathbf{u}|_I$. We say that C is a *systematic code* if there is a set $I \subseteq \{1, \ldots, n\}$ of k coordinate positions such that $|C_I| = p^k$, where $C_I = \{\mathbf{u}|_I : \mathbf{u} \in C\}$. The set I is called an *information set* for C and $\{1, \ldots, n\} \backslash I$ a *redundancy set*.

Permutation decoding is a technique, introduced by Prange [30] and developed by MacWilliams [26] for linear codes, that involves finding a subset of the permutation automorphism group of a code in order to assist in decoding. In [4], a new permutation decoding method for $\mathbb{Z}_4$-linear codes (not necessarily linear), based on having a systematic encoding for these codes, was introduced. Actually, it is also proved that this method can be used for any nonlinear binary code, as long as it has a systematic en-

coding. This can be generalized easily to systematic nonlinear codes over $\mathbb{Z}_p$ [32]. Then, since any $\mathbb{Z}_{p^s}$-linear code is systematic, as shown in [32] by giving a systematic encoding, the permutation decoding method can also be used for these codes.

The idea behind the permutation decoding technique is to move all errors in a received vector out of the information positions by using a permutation that preserves the code. Let C be a t-error-correcting code over $\mathbb{Z}_p$ and denote by $\mathrm{PAut}(C)$ its permutation automorphism group. Then, it is necessary to find a subset $S \subseteq \mathrm{PAut}(C)$, with respect to an information set for C, such that every r-set of coordinate positions is moved out of the information coordinates by at least one element in S, where $1 \leq r \leq t$. The set S is called an *r-PD-set* and, if $r = t$, it is called a *PD-set*.

The efficiency of the permutation decoding method depends on the size of the r-PD-set $S \subseteq \mathrm{PAut}(C)$, since it needs to find the suitable permutation in S, for each received vector. In general, determining the structure of $\mathrm{PAut}(C)$ is very complex, making the search for r-PD-sets or PD-sets a difficult task. However, there are results that show how to find r-PD-sets of small size for certain families of codes [2,3,11,18]. More specifically, in [2], it is shown how to find r-PD-sets of size $r + 1$ for binary linear Hadamard codes and (nonlinear) $\mathbb{Z}_4$-linear Hadamard codes. A similar result for Hadamard codes over the field $\mathbb{F}_4$ is presented in [11]. In this paper, we generalize these results to $\mathbb{Z}_{p^s}$-linear GH codes with $s \geq 2$ and p prime.

The paper is organized as follows. In Section 2, we recall the recursive construction of $\mathbb{Z}_{p^s}$-additive GH codes. In Section 3, we study the permutation automorphism group for these codes and show that it is isomorphic to a group formed by matrices of the general linear group over $\mathbb{Z}_{p^s}$. In Section 4, we give an information set for the corresponding $\mathbb{Z}_{p^s}$-linear GH codes and establish a criterion to find r-PD-sets of size $r + 1$. In Sections 5 and 6, explicit and recursive constructions of r-PD-sets of this size, up to a given upper bound, are described. In Section 7, we present some computational results on a random search of these sets for the codes where the upper bound is not reached. Finally, in Section 8, some conclusions and further research on this topic are included.

2. Construction of $\mathbb{Z}_{p^s}$-additive GH codes

Generator matrices having minimum number of rows for $\mathbb{Z}_4$-additive Hadamard codes, as well as a recursive construction of these matrices, are given in [24]. In [23], $\mathbb{Z}_{2^s}$-additive Hadamard codes with $s > 2$ are introduced and generator matrices with minimum number of rows are also given. A recursive construction for these matrices is presented in [15]. More recently, $\mathbb{Z}_{p^s}$-additive GH codes are considered in [5] generalizing these results to any $p \geq 3$ prime. In this section, we recall the construction of $\mathbb{Z}_{p^s}$-additive GH codes with $s \geq 2$ and p prime.

Let t_1, t_2,...,t_s be nonnegative integers with $t_1 \geq 1$. Consider the matrix $\mathcal{G}^{t_1,\ldots,t_s}$ whose columns are exactly all the vectors of the form $\mathbf{z}^T$, $\mathbf{z} \in \{1\} \times \mathbb{Z}_{p^s}^{t_1-1} \times (p\mathbb{Z}_{p^s})^{t_2} \times \cdots \times \left(p^{s-1}\mathbb{Z}_{p^s}\right)^{t_s}$.

Example 2.1. For $p = 3$ and $s = 3$, we have the following matrices over $\mathbb{Z}_{27}$:

$$\mathcal{G}^{1,0,1} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 9 & 18 \end{pmatrix}, \quad \mathcal{G}^{1,1,0} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 \end{pmatrix},$$

$$\mathcal{G}^{2,0,0} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 \end{pmatrix},$$

$$\mathcal{G}^{1,1,1} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 & 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 & 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9 & 9 & 9 & 9 & 9 & 9 & 9 & 9 & 9 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 \end{pmatrix},$$

$$\mathcal{G}^{2,0,1} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & 26 & 0 & 1 & 2 & \cdots & 26 & 0 & 1 & 2 & \cdots & 26 \\ 0 & 0 & 0 & \cdots & 0 & 9 & 9 & 9 & \cdots & 9 & 18 & 18 & 18 & \cdots & 18 \end{pmatrix}.$$

Let $\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \mathbf{p^s - 1}$ be the vectors having the same element $0, 1, 2, \ldots, p^s - 1$ from $\mathbb{Z}_{p^s}$ in all its coordinates, respectively. The *order* of a vector $\mathbf{u}$ over $\mathbb{Z}_{p^s}$, denoted by $\mathrm{ord}(\mathbf{u})$, is the smallest positive integer m such that $m\mathbf{u} = \mathbf{0}$.

Any matrix $\mathcal{G}^{t_1,\ldots,t_s}$ can also be obtained by applying the following recursive construction. We start with $\mathcal{G}^{1,0,\ldots,0} = (1)$. Then, if we have a matrix $\mathcal{G} = \mathcal{G}^{t_1,\ldots,t_s}$, for any $i \in \{1, \ldots, s\}$, we may construct the matrix

$$\mathcal{G}_i = \begin{pmatrix} \mathcal{G} & \mathcal{G} & \cdots & \mathcal{G} \\ 0 \cdot \mathbf{p^{i-1}} & 1 \cdot \mathbf{p^{i-1}} & \cdots & (p^{s-i+1} - 1) \cdot \mathbf{p^{i-1}} \end{pmatrix}. \tag{3}$$

Finally, permuting the rows of $\mathcal{G}_i$, we obtain a matrix $\mathcal{G}^{t'_1,\ldots,t'_s}$, where $t'_j = t_j$ for $j \neq i$ and $t'_i = t_i + 1$. Note that any permutation of columns of $\mathcal{G}_i$ gives also a matrix $\mathcal{G}^{t'_1,\ldots,t'_s}$.

Example 2.2. From the matrix $\mathcal{G}^{1,0,0} = (1)$, we obtain the matrix $\mathcal{G}^{2,0,0}$; and from $\mathcal{G}^{2,0,0}$ we can construct $\mathcal{G}^{2,0,1}$, where $\mathcal{G}^{2,0,0}$ and $\mathcal{G}^{2,0,1}$ are the matrices given in Example 2.1. Note that we can also generate another matrix $\mathcal{G}^{2,0,1}$ as follows: from $\mathcal{G}^{1,0,0} = (1)$ we obtain the matrix $\mathcal{G}^{1,0,1}$ given in Example 2.1, and from $\mathcal{G}^{1,0,1}$ we can construct the matrix

$$\mathcal{G}_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 9 & 18 & 0 & 9 & 18 & 0 & 9 & 18 & \cdots & 0 & 9 & 18 & 0 & 9 & 18 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & \cdots & 25 & 25 & 25 & 26 & 26 & 26 \end{pmatrix}.$$

Then, after permuting the rows of $\mathcal{G}_1$, we have the matrix

$$\mathcal{G}^{2,0,1} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & \cdots & 25 & 25 & 25 & 26 & 26 & 26 \\ 0 & 9 & 18 & 0 & 9 & 18 & 0 & 9 & 18 & \cdots & 0 & 9 & 18 & 0 & 9 & 18 \end{pmatrix},$$

which is different to the matrix $\mathcal{G}^{2,0,1}$ given in Example 2.1. Note that these two matrices $\mathcal{G}^{2,0,1}$ generate permutation equivalent codes.

In this paper, we assume that the matrices $\mathcal{G}^{t_1,\dots,t_s}$ are constructed recursively starting from $\mathcal{G}^{1,0,\dots,0}$ in the following way. First, we obtain $\mathcal{G}^{t_1,0,\dots,0}$ by adding t_1-1 rows of order p^s; then $\mathcal{G}^{t_1,t_2,0,\dots,0}$ is generated by adding t_2 rows of order p^{s-1}; and so on, until $\mathcal{G}^{t_1,\dots,t_s}$ is reached by adding t_s rows of order p.

We denote by $\mathcal{H}^{t_1,\dots,t_s}$ the $\mathbb{Z}_{p^s}$-additive code of type $(n;t_1,\dots,t_s)$ generated by $\mathcal{G}^{t_1,\dots,t_s}$, where $t_1,\dots,t_s$ are nonnegative integers with $t_1\geq 1$. Note that $n=p^{t-s+1}$, where $t=(\sum_{i=1}^{s}(s-i+1)\cdot t_i)-1$. Let $H^{t_1,\dots,t_s}=\Phi(\mathcal{H}^{t_1,\dots,t_s})$ denote the corresponding $\mathbb{Z}_{p^s}$-linear code, which is a GH code of length p^t [5]. Thus, we say that $\mathcal{H}^{t_1,\dots,t_s}$ is a $\mathbb{Z}_{p^s}$-additive GH code, and $H^{t_1,\dots,t_s}$ a $\mathbb{Z}_{p^s}$-linear GH code.

3. Permutation automorphism group of $\mathbb{Z}_{p^s}$-additive GH codes

The structure of the permutation automorphism group of $\mathbb{Z}_4$-additive Hadamard codes is described in [25,28]. In this section, we describe the structure of the permutation automorphism group of the $\mathbb{Z}_{p^s}$-additive GH code $\mathcal{H}^{t_1,\dots,t_s}$, that is, the structure of $\mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$. In particular, an isomorphism between $\mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$ and a certain group of matrices of the general linear group over $\mathbb{Z}_{p^s}$ is found, and the order of $\mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$ is computed.

Let $\mathrm{GL}(\kappa,\mathbb{Z}_{p^s})$ denote the *general linear group* of degree κ over $\mathbb{Z}_{p^s}$ and let $\mathcal{L}$ be the set consisting of all matrices over $\mathbb{Z}_{p^s}$ of the following form:

$$\begin{pmatrix} 1 & a_1 & pa_2 & p^2a_3 & \cdots & p^{s-2}a_{s-1} & p^{s-1}a_s \\ \mathbf{0} & A_{1,1} & pA_{1,2} & p^2A_{1,3} & \cdots & p^{s-2}A_{1,s-1} & p^{s-1}A_{1,s} \\ \mathbf{0} & A_{2,1} & A_{2,2} & pA_{2,3} & \cdots & p^{s-3}A_{2,s-1} & p^{s-2}A_{2,s} \\ \mathbf{0} & A_{3,1} & A_{3,2} & A_{3,3} & \cdots & p^{s-4}A_{3,s-1} & p^{s-3}A_{3,s} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & A_{s-1,1} & A_{s-1,2} & A_{s-1,3} & \cdots & A_{s-1,s-1} & pA_{s-1,s} \\ \mathbf{0} & A_{s,1} & A_{s,2} & A_{s,3} & \cdots & A_{s,s-1} & A_{s,s} \end{pmatrix}, \tag{4}$$

where $A_{1,1}\in \mathrm{GL}(t_1-1,\mathbb{Z}_{p^s})$, $A_{i,i}\in \mathrm{GL}(t_i,\mathbb{Z}_{p^s})$ for $i\in\{2,\dots,s\}$, $A_{i,j}$ are matrices over $\mathbb{Z}_{p^s}$, for $i\neq j$, $a_1\in\mathbb{Z}_{p^s}^{t_1-1}$ and $a_j\in\mathbb{Z}_{p^s}^{t_j}$, for $j\in\{2,\dots,s\}$.

Lemma 3.1. *The set $\mathcal{L}$ is a subgroup of* $\mathrm{GL}(t_1+\cdots+t_s,\mathbb{Z}_{p^s})$.

Proof. We first need to check that $\mathcal{L}\subseteq \mathrm{GL}(t_1+\cdots+t_s,\mathbb{Z}_{p^s})$, i.e., that $\det(\mathcal{M})\in\mathbb{Z}_{p^s}\backslash p\mathbb{Z}_{p^s}$ for all $\mathcal{M}\in\mathcal{L}$. Note that if $\mathcal{M}'\in\mathrm{GL}(\kappa,\mathbb{Z}_{p^s})$, then $\mathcal{M}=\mathcal{M}'+p\mathcal{R}\in\mathrm{GL}(\kappa,\mathbb{Z}_{p^s})$ for any $\mathcal{R}$. Thus, since $\det(\mathcal{M}')\in\mathbb{Z}_{p^s}\backslash p\mathbb{Z}_{p^s}$, we have that $\det(\mathcal{M})\in\mathbb{Z}_{p^s}\backslash p\mathbb{Z}_{p^s}$, where

$$\mathcal{M}' = \begin{pmatrix} 1 & a_1 & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & A_{1,1} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & A_{2,1} & A_{2,2} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & A_{3,1} & A_{3,2} & A_{3,3} & \cdots & \mathbf{0} & \mathbf{0} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & A_{s-1,1} & A_{s-1,2} & A_{s-1,3} & \cdots & A_{s-1,s-1} & \mathbf{0} \\ \mathbf{0} & A_{s,1} & A_{s,2} & A_{s,3} & \cdots & A_{s,s-1} & A_{s,s} \end{pmatrix}.$$

Finally, we prove that $\mathcal{L}$ is a subgroup. Let us denote by $\mathcal{M}_{i,j}$, for $i,j \in \{1,\dots,s+1\}$, the submatrix in the ith row and jth column of the block matrix $\mathcal{M} \in \mathcal{L}$ as given in (4). Note that $\mathcal{M}_{1,j}$ is a multiple of p^{j-2} for $j \in \{2,\dots,s+1\}$, and $\mathcal{M}_{i,j}$ is a multiple of p^{j-i} for $i,j \in \{2,\dots,s+1\}$ and $j > i$. Then, consider the submatrix $\mathcal{Q}_{i,j}$ of $\mathcal{Q} = \mathcal{M}\mathcal{N}$, for $\mathcal{M},\mathcal{N} \in \mathcal{L}$. Clearly, $\mathcal{Q}_{1,1} = 1$ and $\mathcal{Q}_{i,1} = \mathbf{0}$ for $i \in \{2,\dots,s+1\}$. For the first row, we have $\mathcal{Q}_{1,j} = \sum_{k=1}^{s+1} \mathcal{M}_{1,k}\mathcal{N}_{k,j}$ for $j \in \{2,\dots,s+1\}$. Note that $\mathcal{M}_{1,1}\mathcal{N}_{1,j} = \mathcal{N}_{1,j}$ is a multiple of p^{j-2}, $\mathcal{M}_{1,k}\mathcal{N}_{k,j}$ is a multiple of $p^{k-2}p^{j-k} = p^{j-2}$ for $k \in \{2,\dots,j\}$, and a multiple of p^{k-2} for $k \in \{j+1,\dots,s+1\}$. Therefore, $\mathcal{Q}_{i,j}$ is a multiple of p^{j-2}. For the rest of the rows, $\mathcal{Q}_{i,j} = \sum_{k=2}^{s+1} \mathcal{M}_{i,k}\mathcal{N}_{k,j}$ for $i,j \in \{2,\dots,s+1\}$ and $j > i$. Note that $\mathcal{M}_{i,k}\mathcal{N}_{k,j}$ is a multiple of p^{j-k} for $k \in \{2,\dots,i-1\}$, a multiple of $p^{k-i}p^{j-k} = p^{j-i}$ for $k \in \{i,\dots,j\}$, and a multiple of p^{k-i} for $k \in \{j+1,\dots,s+1\}$. Therefore, $\mathcal{Q}_{i,j}$ is also a multiple of p^{j-i}. Finally, the block submatrices in the diagonal are $\mathcal{Q}_{i,i} = \sum_{k=2}^{s+1} \mathcal{M}_{i,k}\mathcal{N}_{k,i}$ for $i \in \{2,\dots,s+1\}$. Note that $\mathcal{M}_{i,i}\mathcal{N}_{i,i} \in \mathrm{GL}(t_i, \mathbb{Z}_{p^s})$ and $\mathcal{M}_{i,k}\mathcal{N}_{k,i}$ is a multiple of p^{i-k} for $k < i$ and a multiple of p^{k-i} for $k > i$, hence $\mathcal{Q}_{i,i} \in \mathrm{GL}(t_i, \mathbb{Z}_{p^s})$. □

Let ζ_i be the map from $\mathbb{Z}_{p^s}$ to $\mathbb{Z}_{p^s}$ defined as $\zeta_i(a) = a \mod p^i$, $i \in \{1,\dots,s-1\}$. This map can be extended to matrices over $\mathbb{Z}_{p^s}$ by applying ζ_i to each one of their entries. Let π be the map from $\mathcal{L}$ to $\mathcal{L}$ defined as

$$\pi(\mathcal{M}) = \begin{pmatrix} 1 & a_1 & pa_2 & \cdots & p^{s-2}a_{s-1} & p^{s-1}a_s \\ \mathbf{0} & A_{1,1} & pA_{1,2} & \cdots & p^{s-2}A_{1,s-1} & p^{s-1}A_{1,s} \\ \mathbf{0} & \zeta_{s-1}(A_{2,1}) & \zeta_{s-1}(A_{2,2}) & \cdots & \zeta_{s-1}(p^{s-3}A_{2,s-1}) & \zeta_{s-1}(p^{s-2}A_{2,s}) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \zeta_2(A_{s-1,1}) & \zeta_2(A_{s-1,2}) & \cdots & \zeta_2(A_{s-1,s-1}) & \zeta_2(pA_{s-1,s}) \\ \mathbf{0} & \zeta_1(A_{s,1}) & \zeta_1(A_{s,2}) & \cdots & \zeta_1(A_{s,s-1}) & \zeta_1(A_{s,s}) \end{pmatrix}, \quad (5)$$

for any matrix $\mathcal{M} \in \mathcal{L}$ as given in (4). Let $\pi(\mathcal{L}) = \{\pi(\mathcal{M}) : \mathcal{M} \in \mathcal{L}\} \subseteq \mathrm{GL}(t_1 + \cdots + t_s, \mathbb{Z}_{p^s})$. By Lemma 3.1, it is clear that $\pi(\mathcal{L})$ is a group with the operation $*$ defined as $\mathcal{M} * \mathcal{N} = \pi(\mathcal{M}\mathcal{N})$ for all $\mathcal{M},\mathcal{N} \in \pi(\mathcal{L})$. Note that the group operation $*$ is well defined, since $\pi(\mathcal{L}) \subseteq \mathcal{L}$. By a generalization of the proof of Theorem 2 in [25], one can show the following theorem.

Theorem 3.1. *Let $\mathcal{H}^{t_1,\dots,t_s}$ be the $\mathbb{Z}_{p^s}$-additive GH code of type $(n; t_1,\dots,t_s)$. Then,* $\mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$ *is isomorphic to $\pi(\mathcal{L})$.*

Proof. Let R be the set $\mathbb{Z}_{p^s}^{t_1-1} \times \mathbb{Z}_{p^{s-1}}^{t_2} \times \cdots \times \mathbb{Z}_p^{t_s}$ and denote by $\mathcal{B}$ the set of all affine functions from R to $\mathbb{Z}_{p^s}$. We can see these $\mathbb{Z}_{p^s}$-valued affine functions as words of length $n = p^{s(t_1-1)+(s-1)t_2+\cdots+t_s}$ over $\mathbb{Z}_{p^s}$ by considering the image of all elements in the domain. Let us define $B = \{x : R \longrightarrow \mathbb{Z}_p^{p^{s-1}} \,|\, x(\cdot) = \phi(f(\cdot)) \text{ for some } f \in \mathcal{B}\}$. That is, the image of the words in $\mathcal{B}$ by the generalized Gray map Φ. By a straightforward generalization of Lemma 1 in [25], we know that B is a $\mathbb{Z}_{p^s}$-linear GH code of type $(n; t_1, t_2, \ldots, t_s)$. This means that $\mathcal{H}^{t_1,\ldots,t_s} = \mathcal{B}$ and $H^{t_1,\ldots,t_s} = B$, and we can see the elements of $\mathcal{H}^{t_1,\ldots,t_s}$ as affine functions.

Note that an affine function $f \in \mathcal{B}$ can be seen as a word w_f of length n over $\mathbb{Z}_{p^s}$, with the elements of R playing the role of coordinate positions. A permutation $\sigma \in \mathcal{S}_n$ acting on w_f, by permuting its coordinates, gives a word $\sigma(w_f)$ which corresponds to the function $f \circ \sigma^{-1}$ by considering $f(\sigma^{-1}(v))$ for any $v \in R$. Therefore, a permutation σ is said to be in $\mathrm{PAut}(\mathcal{B})$ if and only if $f \circ \sigma^{-1}$ is an affine function for any $f \in \mathcal{B}$. Naturally, $\mathrm{PAut}(\mathcal{B}) = \mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$.

Now, we use an adaptation of Theorem 2 in [25] to prove that $\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$, or equivalently $\mathrm{PAut}(\mathcal{B})$, consists of all affine permutations of R. First, we have that any affine permutation belongs to $\mathrm{PAut}(\mathcal{B})$ since the composition of an affine permutation and an affine function is also an affine function. Next, we see that any permutation $\sigma \in \mathrm{PAut}(\mathcal{B})$ is affine. Let

$$\begin{aligned} \sigma_1^{(1)}, \ldots, \sigma_{t_1-1}^{(1)} &: \quad R \longrightarrow \mathbb{Z}_{p^s}, \\ \sigma_1^{(2)}, \ldots, \sigma_{t_2}^{(2)} &: \quad R \longrightarrow \mathbb{Z}_{p^{s-1}}, \\ &\vdots \\ \sigma_1^{(s)}, \ldots, \sigma_{t_s}^{(s)} &: \quad R \longrightarrow \mathbb{Z}_p, \end{aligned}$$

be the components of σ^{-1}. That is,

$$\sigma^{-1}(v) = (\sigma_1^{(1)}(v), \ldots, \sigma_{t_1-1}^{(1)}(v), \sigma_1^{(2)}(v), \ldots, \sigma_{t_2}^{(2)}(v), \ldots, \sigma_1^{(s)}(v), \ldots, \sigma_{t_s}^{(s)}(v))$$

for any $v \in R$. Consider the following functions defined from R to $\mathbb{Z}_{p^s}$:

$$f_i^{(j)}(x_1^{(1)}, \ldots, x_{t_1-1}^{(1)}, x_1^{(2)}, \ldots, x_{t_2}^{(2)}, \ldots, x_1^{(s)}, \ldots, x_{t_s}^{(s)}) = p^{j-1} x_i^{(j)},$$
$$\begin{cases} \text{for } i \in \{1, \ldots, t_1 - 1\} \text{ if } j = 1, \\ \text{for } i \in \{1, \ldots, t_j\} \text{ if } j \in \{2, \ldots, s\}. \end{cases}$$

Note that $p^{j-1}x_i^{(j)}$ defines the inclusion of $x_i^{(j)} \in \mathbb{Z}_{p^{s-j+1}}$ in $\mathbb{Z}_{p^s}$. These functions are affine, hence $f_i^{(j)} \in \mathcal{B}$ and, since $\sigma \in \mathrm{PAut}(\mathcal{B})$, we have that $f_i^{(j)} \circ \sigma^{-1} \in \mathcal{B}$. Moreover, $f_i^{(j)}(\sigma^{-1}(v)) = p^{j-1}\sigma_i^{(j)}(v)$, therefore $\sigma_i^{(j)}$ is affine. Since all components are affine, σ^{-1} and σ are also affine.

Finally, we show that the group of affine permutations over R is isomorphic to $\pi(\mathcal{L})$. Let us denote the former by $\mathcal{S}$. Then, we see that $\mathcal{S}$ is isomorphic to $\pi(\mathcal{L})$ via the map ψ, defined from $\pi(\mathcal{L})$ to $\mathcal{S}$ as

$$\psi(\pi(\mathcal{M})) = \sigma(u_1, u_2, \dots, u_s) = b + u_1 A_1 + u_2 p A_2 + \cdots + u_s p^{s-1} A_s,$$

where $b = (a_1, pa_2, \dots, p^{s-1}a_s)$ and

$$\begin{aligned} A_1 &= (A_{1,1}, pA_{1,2}, \dots, p^{s-1}A_{1,s}),\\ A_2 &= (\zeta_{s-1}(A_{2,1}), \zeta_{s-1}(A_{2,2}), \dots, \zeta_{s-1}(p^{s-2}A_{2,s})),\\ &\vdots\\ A_s &= (\zeta_1(A_{s,1}), \zeta_1(A_{s,2}), \dots, \zeta_1(A_{s,s})). \end{aligned}$$

Note that $A_1, pA_2, \dots, p^{s-1}A_s$ are matrices over $\mathbb{Z}_{p^s}$ with linearly independent rows of order $p^s, p^{s-1}, \dots, p$, respectively, spanning R. This is ensured due to $A_{j,j}$, for $j \in \{1, \dots, s\}$, being invertible. The map ψ gives an isomorphism between $\pi(\mathcal{L})$ and $\mathcal{S}$, so $\pi(\mathcal{L})$ and $\mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$ are isomorphic. □

Theorem 3.2. *Let $\mathcal{H}^{t_1,\dots,t_s}$ be the $\mathbb{Z}_{p^s}$-additive GH code of type $(n; t_1, \dots, t_s)$, where $n = p^{s(t_1-1)+(s-1)t_2+\cdots+t_s}$. Let $\bar{t}_1 = t_1 - 1$ and $\bar{t}_i = t_i$ for $i \in \{2, \dots, s\}$. The order of its permutation automorphism group is*

$$|\,\mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})| = p^E N_1 \cdots N_s, \tag{6}$$

where $N_i = |\mathrm{GL}(\bar{t}_i, \mathbb{Z}_{p^{s-i+1}})| = p^{(s-i)\bar{t}_i^2 + \frac{\bar{t}_i(\bar{t}_i-1)}{2}} \prod_{j=1}^{\bar{t}_i}(p^j - 1)$ and

$$E = s\bar{t}_1 + (s-1)\bar{t}_2 + \cdots + \bar{t}_s + \sum_{i=1}^{s}\sum_{j=i+1}^{s} 2(s-j+1)\bar{t}_i\bar{t}_j. \tag{7}$$

Proof. The order of $\mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$ can be easily computed with a counting argument over the matrix representation, that is, over the elements of $\pi(\mathcal{L})$, given in (5).

The first row of a matrix $\mathcal{M} \in \pi(\mathcal{L})$ is a random tuple over $\mathbb{Z}_{p^s}^{t_1-1} \times \mathbb{Z}_{p^{s-1}}^{t_2} \times \cdots \times \mathbb{Z}_p^{t_s}$. There are $p^{s(t_1-1)+(s-1)t_2+\cdots+t_s}$ such tuples.

Note that $\zeta_{s-i+1}(p^{j-i}A_{i,j})$, for $i < j$, is a matrix of size $\bar{t}_i \times \bar{t}_j$ defined over $\mathbb{Z}_{p^s}$, with entries among $p^{s-i+1}/p^{j-i} = p^{s-j+1}$ elements in $\mathbb{Z}_{p^s}$. In the case $i = 1$, ζ_s represents the identity map from $\mathbb{Z}_{p^s}$ to $\mathbb{Z}_{p^s}$. Therefore, there are $p^{(s-j+1)\bar{t}_i\bar{t}_j}$ such matrices. Moreover, $\zeta_{s-j+1}(A_{j,i})$, for $i < j$, is a matrix of size $\bar{t}_j \times \bar{t}_i$ with entries among the same number of elements as $\zeta_{s-i+1}(p^{j-i}A_{i,j})$. Then, for each pair $i, j \in \{1, \dots, s\}$ such that $i < j$, we have $p^{2(s-j+1)\bar{t}_i\bar{t}_j}$ different possibilities to choose the corresponding matrices.

All matrices in the diagonal are invertible matrices defined over $\mathbb{Z}_{p^s}$. Moreover, $\zeta_{s-i+1}(A_{i,i})$ can be represented as an invertible matrix over $\mathbb{Z}_{p^{s-i+1}}$ by considering

$\{0,\dots,p^{s-i+1}-1\} \subset \mathbb{Z}_{p^s}$ as elements in $\mathbb{Z}_{p^{s-i+1}}$. Therefore, $\zeta_{s-i+1}(A_{i,i})$ is a matrix in the group $\mathrm{GL}(\bar{t}_i, \mathbb{Z}_{p^{s-i+1}})$. In [21], the order of the general linear group over integers modulo m is given. In particular, the order of $\mathrm{GL}(\kappa, \mathbb{Z}_{p^s})$, denoted by $\nu_\kappa(p^s)$, for p prime and integers κ and $s \geq 2$, satisfies $\nu_\kappa(p^s) = p^{(s-1)\kappa^2}\nu_\kappa(p)$, where $\nu_\kappa(p) = (p^\kappa - 1)(p^\kappa - p)\cdots(p^\kappa - p^{\kappa-1})$ is the order of the general linear group over the field $\mathbb{Z}_p$. Then, the order of $\mathrm{GL}(\bar{t}_i, \mathbb{Z}_{p^{s-i+1}})$ is $\nu_{\bar{t}_i}(\mathbb{Z}_{p^{s-i+1}}) = p^{(s-i)\bar{t}_i^2 + \frac{\bar{t}_i(\bar{t}_i-1)}{2}} \prod_{j=1}^{\bar{t}_i}(p^j - 1)$.

Considering all possible choices of submatrices, the result follows. □

Remark 3.1. If we consider the case with $p = 2$ and $s = 2$, that is, $\mathbb{Z}_4$-additive Hadamard codes of type $(n; t_1, t_2)$, then (7) becomes $E = 2(t_1 - 1) + t_2 + 2(t_1 - 1)t_2$. We also have $N_1 = |\mathrm{GL}(t_1 - 1, \mathbb{Z}_4)| = 2^{(t_1-1)^2 + \frac{(t_1-1)(t_1-2)}{2}} \prod_{j=1}^{t_1-1}(2^j - 1)$ and $N_2 = |\mathrm{GL}(t_2, \mathbb{Z}_2)| = 2^{\frac{t_2(t_2-1)}{2}} \prod_{j=1}^{t_2}(2^j - 1)$. Therefore,

$$|\operatorname{PAut}(\mathcal{H}^{t_1,t_2})| = 2^{\frac{3(t_1-1)^2}{2} + \frac{3(t_1-1)}{2} + 2(t_1-1)t_2 + \frac{t_2^2}{2} + \frac{t_2}{2}} \prod_{j=1}^{t_1-1}(2^j - 1) \prod_{j=1}^{t_2}(2^j - 1).$$

Note that this expression coincides with the one given in [2].

Example 3.1. Consider the $\mathbb{Z}_{27}$-additive GH code $\mathcal{H}^{2,1,1}$. By Theorem 3.1, $\operatorname{PAut}(\mathcal{H}^{2,1,1})$ is isomorphic to the group $\pi(\mathcal{L}) \subseteq \mathrm{GL}(4, \mathbb{Z}_{27})$. The subgroup $\mathcal{L} \subseteq \mathrm{GL}(4, \mathbb{Z}_{27})$ is formed by all matrices in the form

$$\begin{pmatrix} 1 & a_1 & 3a_2 & 9a_3 \\ 0 & A_{1,1} & 3A_{1,2} & 9A_{1,3} \\ 0 & A_{2,1} & A_{2,2} & 3A_{2,3} \\ 0 & A_{3,1} & A_{3,2} & A_{3,3} \end{pmatrix},$$

where $a_1, a_2, a_3, A_{i,j} \in \mathbb{Z}_{27}$, $i, j \in \{1, 2, 3\}$ with $i \neq j$, and $A_{1,1}, A_{2,2}, A_{3,3} \in \mathbb{Z}_{27} \setminus \{0, 3, 6, 9, 12, 15, 18, 21, 24\}$. For example, consider the following two matrices $\mathcal{M}, \mathcal{N} \in \mathcal{L}$:

$$\mathcal{M} = \begin{pmatrix} 1 & 1 & 21 & 9 \\ 0 & 2 & 3 & 18 \\ 0 & 14 & 14 & 0 \\ 0 & 9 & 16 & 22 \end{pmatrix}, \quad \mathcal{N} = \begin{pmatrix} 1 & 19 & 18 & 0 \\ 0 & 8 & 24 & 9 \\ 0 & 18 & 20 & 0 \\ 0 & 16 & 4 & 7 \end{pmatrix}.$$

The function π reduces the third row modulo 9 and the fourth row modulo 3, therefore

$$\pi(\mathcal{M}) = \begin{pmatrix} 1 & 1 & 21 & 9 \\ 0 & 2 & 3 & 18 \\ 0 & 5 & 5 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad \pi(\mathcal{N}) = \begin{pmatrix} 1 & 19 & 18 & 0 \\ 0 & 8 & 24 & 9 \\ 0 & 0 & 2 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Note that, since $\mathcal{L}$ is a group, $\pi(\mathcal{L})$ is also a group with the operation $*$:

$$\pi(\mathcal{M}) * \pi(\mathcal{N}) = \pi(\pi(\mathcal{M})\pi(\mathcal{N})) = \pi\left(\begin{pmatrix} 1 & 9 & 12 & 18 \\ 0 & 7 & 18 & 9 \\ 0 & 13 & 22 & 18 \\ 0 & 1 & 3 & 1 \end{pmatrix}\right) = \begin{pmatrix} 1 & 9 & 12 & 18 \\ 0 & 7 & 18 & 9 \\ 0 & 4 & 4 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Theorem 3.2 gives the order of $\pi(\mathcal{L})$, or equivalently of $\mathrm{PAut}(\mathcal{H}^{2,1,1})$. Following the same notation as in the statement of the theorem, we have that

$$\begin{aligned} N_1 &= |\mathrm{GL}(1, \mathbb{Z}_{27})| = 18, \\ N_2 &= |\mathrm{GL}(1, \mathbb{Z}_9)| = 6, \\ N_3 &= |\mathrm{GL}(1, \mathbb{Z}_3)| = 2, \\ E &= 3 + 2 + 1 + 4 + 2 + 2 = 14. \end{aligned}$$

Therefore, $|\mathrm{PAut}(\mathcal{H}^{2,1,1})| = 3^E N_1 N_2 N_3 = 3^{17} \cdot 2^3 = 1033121304$.

4. r-PD-sets for $\mathbb{Z}_{p^s}$-linear GH codes

In this section, we give an additive information set for the $\mathbb{Z}_{p^s}$-additive GH code $\mathcal{H}^{t_1,\dots,t_s}$, and an information set for the corresponding $\mathbb{Z}_{p^s}$-linear GH code $H^{t_1,\dots,t_s}$. Then, using the result given by Theorem 3.1, we establish a criterion in order to find r-PD-sets of size $r+1$ for $H^{t_1,\dots,t_s}$, with r up to a given upper bound.

An ordered set $\mathcal{I} = \{i_1, \dots, i_{t_1+\cdots+t_s}\} \subseteq \{1, \dots, n\}$ of $t_1 + \cdots + t_s$ coordinate positions is said to be an *additive information set* for a $\mathbb{Z}_{p^s}$-additive code $\mathcal{C}$ of type $(n; t_1, \dots, t_s)$ if $|\mathcal{C}_{\mathcal{I}}| = (p^s)^{t_1}(p^{s-1})^{t_2} \cdots p^{t_s}$. If the elements of $\mathcal{I}$ are ordered in such a way that, for any $k \in \{1, \dots, s\}$, $|\mathcal{C}_{\{i_1,\dots,i_{t_1+\cdots+t_k}\}}| = (p^s)^{t_1}(p^{s-1})^{t_2} \cdots (p^{s-k+1})^{t_k}$, then it can be seen that the set $\Phi(\mathcal{I})$, defined as

$$\begin{aligned} \Phi(\mathcal{I}) = &\Phi^{(1)}(\{i_1, \dots, i_{t_1}\}) \cup \Phi^{(2)}(\{i_{t_1+1}, \dots, i_{t_1+t_2}\}) \cup \\ &\cdots \cup \Phi^{(s)}(\{i_{t_1+\cdots+t_{s-1}+1}, \dots, i_{t_1+\cdots+t_s}\}), \end{aligned}$$

where

$$\begin{aligned} \Phi^{(k)}(I) = \cup_{i \in I} \{ & p^{s-1}(i-1) + 1, \\ & p^{s-1}(i-1) + p^{k-1} + 1, \\ & p^{s-1}(i-1) + p^{k-1+1} + 1, \\ & p^{s-1}(i-1) + p^{k-1+2} + 1, \\ & \dots, \\ & p^{s-1}(i-1) + p^{s-2} + 1\}, \end{aligned}$$

is an information set for $C = \Phi(\mathcal{C})$ [32]. Note that $s - 2 - (k-1) = s - k - 1$, hence $\Phi^{(k)}(I)$ has $s - k + 1$ coordinate positions for each element in I.

Example 4.1. It is easy to see, from the matrix $\mathcal{G}^{1,1,1}$ given in Example 2.1, that the set $\mathcal{I} = \{1, 2, 10\}$ is an additive information set for the $\mathbb{Z}_{27}$-additive GH code $\mathcal{H}^{1,1,1}$, so $\Phi(\mathcal{I}) = \Phi^{(1)}(\{1\}) \cup \Phi^{(2)}(\{2\}) \cup \Phi^{(3)}(\{10\}) = \{1, 2, 4, 10, 13, 82\}$ is an information set for $H^{1,1,1} = \Phi(\mathcal{H}^{1,1,1})$.

In general, there is no unique way to obtain an additive information set for $\mathcal{H}^{t_1,\dots,t_s}$. The following result provides a recursive and simple form to obtain such a set.

Proposition 4.1. *Let $\mathcal{I}$ be an additive information set for the $\mathbb{Z}_{p^s}$-additive GH code $\mathcal{H}^{t_1,\dots,t_s}$ of type $(n; t_1, \dots, t_s)$, where $n = p^{s(t_1-1)+(s-1)t_2+\cdots+t_s}$. Then $\mathcal{I} \cup \{n+1\}$ is an additive information set for the codes $\mathcal{H}^{t_1+1,t_2,\dots,t_s}$, $\mathcal{H}^{t_1,t_2+1,\dots,t_s}$ and so on until $\mathcal{H}^{t_1,t_2,\dots,t_s+1}$, obtained from $\mathcal{H}^{t_1,t_2,\dots,t_s}$ by applying (3).*

Proof. Let $\mathcal{H}_k = \mathcal{H}^{t'_1,t'_2,\dots,t'_s}$, $k \in \{1, \dots, s\}$, where $t'_j = t_j$ for $j \neq k$ and $t'_k = t_k + 1$. It is clear that an additive information set for $\mathcal{H}_k$ should have $t_1 + t_2 + \cdots + t_s + 1 = |\mathcal{I}| + 1$ coordinate positions. Taking into account that $\mathcal{H}_k$ is constructed from $\mathcal{H}^{t_1,t_2,\dots,t_s}$ by applying (3), we have that $|(\mathcal{H}_k)_{\mathcal{I}\cup\{x\}}| = (p^s)^{t_1}(p^{s-1})^{t_2} \cdots p^{t_s} p^{s+1-k}$ for all $x \in \{n+1, \dots, 2n\}$. In particular, $\mathcal{I} \cup \{n+1\}$ is an additive information set for $\mathcal{H}_k$. □

Let $\mathcal{I}$ be an additive information set for $\mathcal{H}^{t_1,\dots,t_s}$ of type $(n; t_1, \dots, t_s)$. Let $\mathcal{H}_k = \mathcal{H}^{t'_1,t'_2,\dots,t'_s}$, $k \in \{1, \dots, s\}$, where $t'_j = t_j$ for $j \neq k$ and $t'_k = t_k + 1$. Although the additive information set $\mathcal{I} \cup \{n+1\}$, given by Proposition 4.1, is the same for all $\mathcal{H}_k$, the information sets for the corresponding $\mathbb{Z}_{p^s}$-linear codes over $\mathbb{Z}_p$, $H_k = \Phi(\mathcal{H}_k)$, differ for every $k \in \{1, \dots, s\}$. In particular,

$$I^{(k)} = \Phi(\mathcal{I}) \cup \{p^{s-1}n + 1, p^{s-1}n + p^{k-1} + 1, p^{k-1}n + p^k + 1, \dots, p^{s-1}n + p^{s-2} + 1\}$$

is an information set for H_k.

We can label the ith coordinate position of a $\mathbb{Z}_{p^s}$-additive GH code $\mathcal{H}^{t_1,\dots,t_s}$, with the ith column of its generator matrix $\mathcal{G}^{t_1,\dots,t_s}$. Note that, by construction, all columns in $\mathcal{G}^{t_1,\dots,t_s}$ are different and there are $n = p^{s(t_1-1)+(s-1)t_2+\cdots+t_s}$ of them. Thus, any additive information set $\mathcal{I}$ for $\mathcal{H}^{t_1,\dots,t_s}$ can also be considered as a set of vectors representing the positions in $\mathcal{I}$. Let e_i be the vector with all coordinates equal to 0 except the one in the ith position, which is equal to 1. Then, by Proposition 4.1, we have that the set

$$\begin{aligned}\mathcal{I}_{t_1,\dots,t_s} =& \{e_1, e_1 + e_2, \dots, e_1 + e_{t_1}\} \cup \{e_1 + pe_{t_1+1}, \dots, e_1 + pe_{t_1+t_2}\} \cup \cdots \cup \\ & \{e_1 + p^{s-1}e_{t_1+t_2+\cdots+t_{s-1}+1}, \dots, e_1 + p^{s-1}e_{t_1+t_2+\cdots+t_s}\}\end{aligned}$$

is a suitable additive information set for $\mathcal{H}^{t_1,\dots,t_s}$. Depending on the context, $\mathcal{I}_{t_1,\dots,t_s}$ is considered as a subset of $\{1, \dots, n\}$ or $\{1\} \times \mathbb{Z}_{p^s}^{t_1-1} \times (p\mathbb{Z}_{p^s})^{t_2} \times \cdots \times (p^{s-1}\mathbb{Z}_{p^s})^{t_s}$.

Example 4.2. Let $\mathcal{H}^{2,0,0}$ be the $\mathbb{Z}_{27}$-additive GH code of length 27 with generator matrix $\mathcal{G}^{2,0,0}$ given in Example 2.1. The set $\mathcal{I}_{2,0,0} = \{1, 2\}$, or equivalently the set of vectors $\mathcal{I}_{2,0,0} = \{e_1, e_1 + e_2\}$, is an additive information set for $\mathcal{H}^{2,0,0}$.

By applying (3) over $\mathcal{G}^{2,0,0}$, we obtain matrices $\mathcal{G}^{3,0,0}$, $\mathcal{G}^{2,1,0}$ and $\mathcal{G}^{2,0,1}$ that generate the $\mathbb{Z}_{27}$-additive GH codes $\mathcal{H}^{3,0,0}$, $\mathcal{H}^{2,1,0}$ and $\mathcal{H}^{2,0,1}$ of length 729, 243 and 81, respectively. By Proposition 4.1, it follows that $\mathcal{I}_{2,0,0} \cup \{28\} = \{1, 2, 28\}$ is an additive information set for $\mathcal{H}^{3,0,0}$, $\mathcal{H}^{2,1,0}$ and $\mathcal{H}^{2,0,1}$. Although this additive information set is the same for these three codes, it is important to note that in terms of vectors representing these positions, we have that

$$\begin{aligned}
\mathcal{I}_{3,0,0} &= \{(1,0,0), (1,1,0), (1,0,1)\},\\
\mathcal{I}_{2,1,0} &= \{(1,0,0), (1,1,0), (1,0,3)\}, \text{and}\\
\mathcal{I}_{2,0,1} &= \{(1,0,0), (1,1,0), (1,0,9)\}.
\end{aligned}$$

Finally,

$$\begin{aligned}
I^{(1)} &= \Phi(\mathcal{I}_{2,0,0}) \cup \{244, 245, 247\} = \{1, 2, 4, 10, 11, 13, 244, 245, 247\},\\
I^{(2)} &= \Phi(\mathcal{I}_{2,0,0}) \cup \{244, 247\} = \{1, 2, 4, 10, 11, 13, 244, 247\}, \text{ and}\\
I^{(3)} &= \Phi(\mathcal{I}_{2,0,0}) \cup \{244\} = \{1, 2, 4, 10, 11, 13, 244\}
\end{aligned}$$

are information sets for the corresponding $\mathbb{Z}_{27}$-linear GH codes $H^{3,0,0}$, $H^{2,1,0}$ and $H^{2,0,1}$, respectively.

Let $\mathcal{C}$ be a $\mathbb{Z}_{p^s}$-additive code of type $(n; t_1, \ldots, t_s)$, and let $C = \Phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_{p^s}$-linear code of length $p^{s-1}n$. Let $\Phi : \mathrm{Sym}(n) \to \mathrm{Sym}(p^{s-1}n)$ be the map defined as

$$\Phi(\tau)(i) = p^{s-1}\tau\left(\frac{i + \chi(i)}{p^{s-1}}\right) - \chi(i), \tag{8}$$

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

Lemma 4.1. *The map $\Phi : \mathrm{Sym}(n) \to \mathrm{Sym}(p^{s-1}n)$ is a group monomorphism.*

Proof. We need to check that $\Phi(\sigma\tau) = \Phi(\sigma)\Phi(\tau)$ for all $\tau, \sigma \in \mathrm{Sym}(n)$. Let i be a coordinate position in $\{1, \ldots, p^{s-1}n\}$ and $\chi(i) = p^{s-1} - (i \bmod p^{s-1})$. Note that $\chi(p^{s-1}a - \chi(i)) = \chi(i)$ for any integer a. Then

$$(\Phi(\sigma)\Phi(\tau))(i) = \Phi(\sigma)\left(p^{s-1}\tau\left(\frac{i + \chi(i)}{p^{s-1}}\right) - \chi(i)\right)$$

$$
\begin{aligned}
&= p^{s-1}\sigma\left(\frac{p^{s-1}\tau\left(\frac{i+\chi(i)}{p^{s-1}}\right)-\chi(i)+\chi(i)}{p^{s-1}}\right)-\chi(i)\\
&= p^{s-1}\sigma\tau\left(\frac{i+\chi(i)}{p^{s-1}}\right)-\chi(i)\\
&= \Phi(\sigma\tau)(i).
\end{aligned}
$$

Finally, it is easy to check that Φ is injective. □

By Theorem 3.1, we identify $\mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$ with the group $\pi(\mathcal{L})$. Recall that we can label the ith coordinate position of $\mathcal{H}^{t_1,\dots,t_s}$ with the ith column w_i of the generator matrix $\mathcal{G}^{t_1,\dots,t_s}$ constructed via (3), $i \in \{1,\dots,n\}$. Any matrix $\mathcal{M} \in \mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$ sends columns of $\mathcal{G}^{t_1,\dots,t_s}$ to other columns of $\mathcal{G}^{t_1,\dots,t_s}$. Therefore, $\mathcal{M}$ can be seen as a permutation of coordinate positions $\tau \in \mathrm{Sym}(n)$, such that for all $i \in \{1,\dots,n\}$

$$
\tau(i) = j \iff w_i\mathcal{M} = w_j, \quad j \in \{1,\dots,n\}. \tag{9}
$$

For any $\mathcal{M} \in \mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$, we define $\Phi(\mathcal{M}) = \Phi(\tau) \in \mathrm{Sym}(p^{s-1}n)$ and, for any $\mathcal{P} \subseteq \mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$, we consider $\Phi(\mathcal{P}) = \{\Phi(\mathcal{M}) : \mathcal{M} \in \mathcal{P}\} \subseteq \mathrm{Sym}(p^{s-1}n)$.

Proposition 4.2. *Let $\mathcal{H}^{t_1,\dots,t_s}$ be the $\mathbb{Z}_{p^s}$-additive GH code of type $(n;t_1,\dots,t_s)$ and let $\mathcal{P} \subseteq \mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$. Then, $\Phi(\mathcal{P})$ is an r-PD-set for $H^{t_1,\dots,t_s}$ with information set $\Phi(\mathcal{I}_{t_1,\dots,t_s})$ if and only if for each r-set $\mathcal{E}$ of column vectors of $\mathcal{G}^{t_1,\dots,t_s}$ there is $\mathcal{M} \in \mathcal{P}$ such that $\{g\mathcal{M} : g \in \mathcal{E}\} \cap \mathcal{I}_{t_1,\dots,t_s} = \emptyset$.*

Proof. If $\Phi(\mathcal{P})$ is an r-PD-set with respect to the information set $\Phi(\mathcal{I}_{t_1,\dots,t_s})$, then, for each r-set $E \subseteq \{1,\dots,p^{s-1}n\}$, there is $\tau \in \mathcal{P} \subseteq \mathrm{Sym}(n)$ such that $\Phi(\tau)(E) \cap \Phi(\mathcal{I}_{t_1,\dots,t_s}) = \emptyset$. For every r-set $\mathcal{E} \subseteq \{1,\dots,n\}$, let $E_o = \{p^{s-1}(i-1)+1 : i \in \mathcal{E}\}$. We know that there is $\tau \in \mathcal{P}$ such that $\Phi(\tau)(E_o) \cap \Phi(\mathcal{I}_{t_1,\dots,t_s}) = \emptyset$. By the definition of Φ, we also have that $\tau(\mathcal{E}) \cap \mathcal{I}_{t_1,\dots,t_s} = \emptyset$, which is equivalent to the statement.

Conversely, we assume that for each r-set $\mathcal{E} \subseteq \{1,\dots,n\}$, there is $\tau \in \mathcal{P} \subseteq \mathrm{Sym}(n)$ such that $\tau(\mathcal{E}) \cap \mathcal{I}_{t_1,\dots,t_s} = \emptyset$. For every r-set $E \subseteq \{1,\dots,p^{s-1}n\}$, let $\mathcal{E}_o \subseteq \{1,\dots,n\}$ be an r-set such that $\{i : \exists k \in \{1,\dots,p^{s-1}\} \text{ s.t. } \varphi_k(i) \in E\} \subseteq \mathcal{E}_o$, where $\varphi_k(i) = p^{s-1}(i-1)+k$. Since there is $\tau \in \mathcal{P}$ such that $\tau(\mathcal{E}_o) \cap \mathcal{I}_{t_1,\dots,t_s} = \emptyset$, we have that $\Phi(\tau)(E) \cap \Phi(\mathcal{I}_{t_1,\dots,t_s}) = \emptyset$. □

A slight modification of the proof of Proposition 4.2 leads to a more general result that holds for any $\mathbb{Z}_{p^s}$-additive code, not only for the family of $\mathbb{Z}_{p^s}$-additive GH codes.

Proposition 4.3. *Let $\mathcal{C}$ be a $\mathbb{Z}_{p^s}$-additive code, let $\mathcal{I}$ be an additive information set for $\mathcal{C}$, and let $\mathcal{S} \subseteq \mathrm{PAut}(\mathcal{C})$. Then, $\mathcal{S}$ satisfies that for each r-set $\mathcal{E} \subseteq \{1,\dots,n\}$ there is $\tau \in \mathcal{S}$ such that $\tau(\mathcal{E}) \cap \mathcal{I} = \emptyset$ if and only if $\Phi(\mathcal{S}) \subseteq \mathrm{PAut}(C)$ satisfies that for each r-set $E \subseteq \{1,\dots,p^{s-1}n\}$ there is $\sigma \in \Phi(\mathcal{S})$ such that $\sigma(E) \cap \Phi(\mathcal{I}) = \emptyset$.*

Definition 4.1. Let $\mathcal{M} \in \mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$ and let m_i be the ith row of $\mathcal{M}$, $i \in \{1,\dots,t_1+\cdots+t_s\}$. We define $\mathcal{M}^*$ over $\mathbb{Z}_{p^s}$ as the matrix where the first row is m_1 and the ith row is m_1+m_i for $i \in \{2,\dots,t_1\}$, m_1+pm_i for $i \in \{t_1+1,\dots,t_1+t_2\}$, $m_1+p^2m_i$ for $i \in \{t_1+t_2+1,\dots,t_1+t_2+t_3\}$ and so on until $m_1+p^{s-1}m_i$ for $i \in \{t_1+\cdots+t_{s-1}+1,\dots,t_1+\cdots+t_s\}$.

Theorem 4.1. *Let $\mathcal{H}^{t_1,\dots,t_s}$ be the $\mathbb{Z}_{p^s}$-additive GH code of type $(n;t_1,\dots,t_s)$. Let $\mathcal{P}_r = \{\mathcal{M}_i : 0 \le i \le r\}$ be a set of $r+1$ matrices in $\mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$. Then, $\Phi(\mathcal{P}_r)$ is an r-PD-set of size $r+1$ for $H^{t_1,\dots,t_s}$ with information set $\Phi(\mathcal{I}_{t_1,\dots,t_s})$ if and only if no two matrices $(\mathcal{M}_i^{-1})^*$ and $(\mathcal{M}_j^{-1})^*$ have a row in common, for $i,j \in \{0,\dots,r\}$ and $i \neq j$.*

Proof. The result can be proved using Proposition 4.2 and is a generalization of a similar result given in [2] for $\mathbb{Z}_4$-linear Hadamard codes. However, we include the detailed proof for the convenience of the reader.

Suppose that the set $\mathcal{P}_r = \{\mathcal{M}_i : 0 \le i \le r\}$ satisfies that no two matrices $(\mathcal{M}_i^{-1})^*$ and $(\mathcal{M}_j^{-1})^*$, for $i,j \in \{0,\dots,r\}$ and $i \neq j$, have a row in common. Assume that $\Phi(\mathcal{P}_r)$ is not an r-PD-set for $H^{t_1,\dots,t_s}$ with information set $\Phi(\mathcal{I}_{t_1,\dots,t_s})$. By Proposition 4.2, it follows that there exists an r-set $\mathcal{E} \subseteq \{1\} \times \mathbb{Z}_{p^s}^{t_1-1} \times (p\mathbb{Z}_{p^s})^{t_2} \times \cdots \times \left(p^{s-1}\mathbb{Z}_{p^s}\right)^{t_s}$, that is, a set of r different column vectors of the generator matrix $\mathcal{G}^{t_1,\dots,t_s}$, such that for each $i \in \{0,\dots,r\}$, there is a $g_i \in \mathcal{E}$ so that $g_i\mathcal{M}_i \in \mathcal{I}_{t_1,\dots,t_s}$. Note that there are $r+1$ values for i, but only r elements in $\mathcal{E}$. Therefore, $g\mathcal{M}_i \in \mathcal{I}_{t_1,\dots,t_s}$ and $g\mathcal{M}_j \in \mathcal{I}_{t_1,\dots,t_s}$ for some $g \in \mathcal{E}$ and $i \neq j$. Suppose $g\mathcal{M}_i = w_h$ and $g\mathcal{M}_j = w_t$, for $w_h, w_t \in \mathcal{I}_{t_1,\dots,t_s}$. Then, $g = w_h\mathcal{M}_i^{-1} = w_t\mathcal{M}_j^{-1}$. Taking into account the form of the vectors in the information set $\mathcal{I}_{t_1,\dots,t_s}$, by multiplying for such inverse matrices $\mathcal{M}_i^{-1}$ and $\mathcal{M}_j^{-1}$, we obtain the first row or a certain addition between the first row and another row of each matrix. Thus, we obtain that $(\mathcal{M}_i^{-1})^*$ and $(\mathcal{M}_j^{-1})^*$ have a row in common, contradicting our assumption. Let $\mathcal{P}_k \subseteq \mathcal{P}_r$ 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 to a contradiction in the same way as before.

Conversely, suppose that $\Phi(\mathcal{P}_r)$ is an r-PD-set for $H^{t_1,\dots,t_s}$ with information set $\Phi(\mathcal{I}_{t_1,\dots,t_s})$, but does not satisfy the condition on the inverse matrices. Thus, there are two matrices $(\mathcal{M}_i^{-1})^*$ and $(\mathcal{M}_j^{-1})^*$, with $i,j \in \{0,\dots,r\}$, such that they share a common row, say the hth row of $(\mathcal{M}_i^{-1})^*$ and the tth row of $(\mathcal{M}_i^{-1})^*$, with $h,t \in \{1,\dots,t_1+\cdots+t_s\}$. In other words, we can define $g = e_h(\mathcal{M}_i^{-1})^* = e_t(\mathcal{M}_j^{-1})^*$. Therefore, $g = w_h\mathcal{M}_i^{-1} = w_t\mathcal{M}_j^{-1}$, where $w_h, w_t \in \mathcal{I}_{t_1,\dots,t_s}$. Finally, we obtain that $g\mathcal{M}_i = w_h$ and $g\mathcal{M}_j = w_t$. Let $L = \{\ell : 0 \le \ell \le r,\ \ell \neq i,j\}$. For each $\ell \in L$, choose a row g_ℓ of the matrix $(\mathcal{M}_\ell^{-1})^*$. It is clear that $g_\ell = e_{h_\ell}(\mathcal{M}_\ell^{-1})^* = w_{h_\ell}\mathcal{M}_\ell^{-1}$, so $g_\ell\mathcal{M}_\ell = w_{h_\ell} \in \mathcal{I}_{t_1,\dots,t_s}$. Finally, since some of the g_ℓ may repeat, we obtain a set $\mathcal{E} = \{g_\ell : \ell \in L\} \cup \{g\}$ of size at most r. Nevertheless, no matrix in $\mathcal{P}_r$ will map every member of $\mathcal{E}$ out of the additive information set $\mathcal{I}_{t_1,\dots,t_s}$, which contradicts our assumption by Proposition 4.2. □

Corollary 4.1. *Let $\mathcal{P}_r$ be a set of $r+1$ matrices in* $\mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$. *If $\Phi(\mathcal{P}_r)$ is an r-PD-set of size $r+1$ for $H^{t_1,\dots,t_s}$, then any ordering of elements in $\Phi(\mathcal{P}_r)$ provides nested k-PD-sets for $k \in \{1,\dots,r\}$.*

Corollary 4.2. *Let $\mathcal{P}_r$ be a set of $r+1$ matrices in* $\mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$. *If $\Phi(\mathcal{P}_r)$ is an r-PD-set of size $r+1$ for $H^{t_1,\dots,t_s}$, then $r \le f_p^{t_1,\dots,t_s}$, where*

$$f_p^{t_1,\dots,t_s} = \left\lfloor \frac{p^{st_1+(s-1)t_2+\cdots+t_s-s} - t_1 - t_2 - \cdots - t_s}{t_1+t_2+\cdots+t_s} \right\rfloor.$$

Proof. Following the condition on sets of matrices to be r-PD-sets of size $r+1$, given by Theorem 4.1, we have to obtain certain $r+1$ matrices with no rows in common. Since the rows of length $t_1+\cdots+t_s$ must have 1 in the first coordinate, elements from $\mathbb{Z}_{p^s}$ in the coordinates from 2 to t_1, and elements from $p^i\mathbb{Z}_{p^s}$ in the coordinates from $t_1+\cdots+t_i+1$ to $t_1+\cdots+t_{i+1}$, for $i \in \{1,\dots,s-1\}$, the number of possible rows is $p^{s(t_1-1)+(s-1)t_2+\cdots+t_s}$. Thus, taking this fact into account and counting the number of rows of each one of these $r+1$ matrices, we have that $(r+1)(t_1+t_2+\cdots+t_s) \le p^{s(t_1-1)+(s-1)t_2+\cdots+t_s}$, and the result follows. □

5. Explicit construction of r-PD-sets of size $r+1$

In this section, by using Theorem 4.1, we create r-PD-sets of size $r+1$ for different infinite families of $\mathbb{Z}_{p^s}$-linear GH codes. First, we give an explicit construction for the $\mathbb{Z}_{p^s}$-linear GH codes $H^{t_1,0,\dots,0}$, with $t_1 \ge 2$ and $r \le f_p^{t_1,0,\dots,0}$. Then, using a similar idea, we give an explicit construction for the $\mathbb{Z}_{p^s}$-linear GH codes $H_i = H^{1,t_2,\dots,t_s}$, where $i \in \{2,\dots,s\}$, $t_j = 0$ for all $j \ne i$, $t_i \ge 1$, and $r \le f_p^{1,t_2,\dots,t_s}$. The main idea behind these constructions is to use a certain ordered set of vectors as rows of a set of matrices $\{\mathcal{N}_0^*,\dots,\mathcal{N}_r^*\}$, such that $\{\mathcal{N}_0^{-1},\dots,\mathcal{N}_r^{-1}\}$ is an r-PD-set. This method is a generalization of the one used in [2] for $\mathbb{Z}_4$-linear Hadamard codes, which, in turn, was based on a similar idea for simplex codes given in [18].

Let $\mathcal{R} = \mathrm{GR}(p^{s(t_1-1)})$ be the *Galois extension* of dimension t_1-1 over $\mathbb{Z}_{p^s}$, which is isomorphic to any ring $\mathbb{Z}_{p^s}[x]/(h(x))$, where $h(x)$ is a monic basic irreducible polynomial over $\mathbb{Z}_{p^s}$ of degree t_1-1. A monic basic polynomial $h(x)$ over $\mathbb{Z}_{p^s}$ is called *irreducible* if $\bar{h}(x)$ is an irreducible polynomial over $\mathbb{Z}_p$, where $\bar{h}(x)$ is the polynomial obtained by taking the coefficients of $h(x)$ modulo p. Moreover, if $\bar{h}(x)$ is primitive, then $h(x)$ is said to be a *monic basic primitive polynomial* over $\mathbb{Z}_{p^s}$. If $f(x)$ is an irreducible polynomial dividing x^n-1 in $\mathbb{Z}_p[x]$, then there is a unique polynomial $h(x)$ over $\mathbb{Z}_{p^s}[x]$ that satisfies $\bar{h}(x) = f(x)$ and that divides x^n-1 in $\mathbb{Z}_{p^s}[x]$, which is called the Hensel lift of $f(x)$ to $\mathbb{Z}_{p^s}$. Moreover, if a polynomial of degree m is the Hensel lift of a monic primitive polynomial over $\mathbb{Z}_p$, then it always has a root of order p^m-1 [34]. Let $h(x)$ be such a polynomial, with $m = t_1-1$. Let $\alpha \in \mathcal{R}$ be a root of $h(x)$ of order $\ell = p^{t_1-1}-1$. Then, the set $T = \{0,1,\alpha,\alpha^2,\dots,\alpha^{\ell-1}\}$ is called the *Teichmüller set*.

We can always represent an element $y \in \mathcal{R}$ in the following form:

$$y = a_1 + pa_2 + p^2 a_3 + \cdots + p^{s-1} a_s,$$

where $a_i \in T$, for $i \in \{1, \ldots, s\}$, which is called the *p-adic representation* of y. Consider T as an ordered set. Then, we consider the following ordering of the elements of $\mathcal{R} = \{y_1, \ldots, y_{p^{s(t_1-1)}}\}$: $a_1 + pa_2 + \cdots + p^{s-1}a_s < b_1 + pb_2 + \cdots + p^{s-1}b_s$ if $a_j < b_j$ for the last j where a_j and b_j differ. We can also represent an element $y \in \mathcal{R}$ as a linear combination of some powers of α:

$$y = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{t_1-2}\alpha^{t_1-2},$$

where $b_j \in \mathbb{Z}_{p^s}$, for $j \in \{0, \ldots, t_1 - 2\}$. This is called the *additive representation* of y and it can be identified with the vector $(b_0, b_1, \ldots, b_{t_1-2}) \in \mathbb{Z}_{p^s}^{t_1-1}$.

Using the ordering given by the p-adic representation, we construct the set $\{\mathcal{N}_0^*, \ldots, \mathcal{N}_r^*\}$ of matrices of size $t_1 \times t_1$, where each one has the following form:

$$\mathcal{N}_i^* = \begin{pmatrix} 1 & y_{t_1 i+1} \\ 1 & y_{t_1 i+2} \\ \vdots & \vdots \\ 1 & y_{t_1(i+1)} \end{pmatrix},$$

with the elements y_j, for $j \in \{1, \ldots, p^{s(t_1-1)}\}$, given as vectors of $t_1 - 1$ components over $\mathbb{Z}_{p^s}$ by using the corresponding additive representation. Note that no two matrices have a row in common, and there are $\lfloor |\mathcal{R}|/t_1 \rfloor = f_p^{t_1,0,\ldots,0} + 1$ such matrices, where $f_p^{t_1,0,\ldots,0} = \lfloor (p^{st_1} - t_1)/t_1 \rfloor$ by Corollary 4.2, so $r \leq f_p^{t_1,0,\ldots,0}$.

Let $n_{i,j}^*$ be the jth row of the matrix $\mathcal{N}_i^*$, for any $i \in \{0, \ldots, r\}$ and $j \in \{1, \ldots, t_1\}$. In the context of the $\mathbb{Z}_{p^s}$-linear GH code $H^{t_1,0,\ldots,0}$, we define $\mathcal{N}_i$ as the matrix that has $n_{i,1}^*$ as the first row and $n_{i,j}^* - n_{i,1}^*$ as the jth row, for $j \in \{2, \ldots, t_1\}$. Note that this is consistent with Definition 4.1. Indeed, in the proof of Theorem 5.1, we see that $\mathcal{N}_0, \ldots, \mathcal{N}_r \subseteq \mathrm{PAut}(\mathcal{H}^{t_1,0,\ldots,0})$.

Lemma 5.1. *Let $K = \mathbb{Z}_p[x]/(f(x))$, where $f(x) \in \mathbb{Z}_p[x]$ is a primitive polynomial of degree m. Let $\alpha \in K$ be a root of $f(x)$. Then, $\alpha - 1, \alpha^2 - 1, \ldots, \alpha^m - 1$ are linearly independent vectors over $\mathbb{Z}_p$.*

Proof. Let $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$, where $a_j \in \mathbb{Z}_p$ for all $j \in \{0, \ldots, m-1\}$. Since α is a root of $f(x)$, then $\alpha^m - 1 = -\sum_{j=0}^{m-1} a_j \alpha^j - 1$. Using the additive representation of the elements of K, we obtain the following vectors over $\mathbb{Z}_p^m$: $\alpha^i - 1 = e_{i+1} - e_1$ for any $i \in \{1, \ldots, m-1\}$, and $\alpha^m - 1 = -\sum_{j=0}^{m-1} a_j e_{j+1} - e_1$. Consider the following $m \times m$ matrix over $\mathbb{Z}_p$ by taking these vectors as rows:

$$\begin{pmatrix} -\mathbf{1} & \mathrm{Id}_{m-1} \\ -a_0 - 1 & -a \end{pmatrix},$$

where $a = (a_1, \ldots, a_{m-1}) \in \mathbb{Z}_p^{m-1}$. This matrix has the following determinant: $(-1)^m(\sum_{j=0}^{m-1} a_j + 1)$. Since $f(x)$ is irreducible, then $f(1) = 1 + \sum_{j=0}^{m-1} a_j \neq 0$. Therefore, the determinant is non-zero and the vectors are linearly independent over $\mathbb{Z}_p$. □

Theorem 5.1. *Let $\mathcal{P}_r = \{\mathcal{N}_0^{-1}, \ldots, \mathcal{N}_r^{-1}\}$. Then, $\Phi(\mathcal{P}_r)$ is an r-PD-set of size $r+1$ for the $\mathbb{Z}_{p^s}$-linear GH code $H^{t_1,0,\ldots,0}$ with information set $\Phi(\mathcal{I}_{t_1,0,\ldots,0})$, for all $t_1 \geq 2$ and $2 \leq r \leq f_p^{t_1,0,\ldots,0}$.*

Proof. By construction, the matrices $\mathcal{N}_0^*, \ldots, \mathcal{N}_r^*$ do not share a row in common. Thus, if we prove that all matrices $\mathcal{N}_0^{-1}, \ldots, \mathcal{N}_r^{-1}$ are in $\mathrm{PAut}(\mathcal{H}^{t_1,0,\ldots,0})$, then $\Phi(\mathcal{P}_r)$, where $\mathcal{P}_r = \{\mathcal{N}_0^{-1}, \ldots, \mathcal{N}_r^{-1}\}$, would be an r-PD-set of size $r+1$ for $H^{t_1,0,\ldots,0}$, by Theorem 4.1. Since $\mathrm{PAut}(\mathcal{H}^{t_1,0,\ldots,0})$ is a group, it is enough to prove that $\mathcal{N}_0, \ldots, \mathcal{N}_r$ are in this group. Note that these matrices are in the form

$$\mathcal{N}_i = \begin{pmatrix} 1 & y_{t_1 i+1} \\ 0 & y_{t_1 i+2} - y_{t_1 i+1} \\ \vdots & \vdots \\ 0 & y_{t_1(i+1)} - y_{t_1 i+1} \end{pmatrix}, \tag{10}$$

for any $i \in \{0, \ldots, r\}$. As shown in (5), the elements in $\mathrm{PAut}(\mathcal{H}^{t_1,0,\ldots,0})$ have the form

$$\begin{pmatrix} 1 & a_1 \\ 0 & A_{1,1} \end{pmatrix}, \tag{11}$$

where $a_1 \in \mathbb{Z}_{p^s}^{t_1-1}$ and $A_{1,1} \in \mathrm{GL}(t_1 - 1, \mathbb{Z}_{p^s})$. By using the additive representation, $y_{y_1 i+1} \in \mathbb{Z}_{p^s}^{t_1-1}$, for any $i \in \{0, \ldots, r\}$. Then, we need to prove that the vectors $y_{t_1 i+2} - y_{t_1 i+1}, \ldots, y_{t_1(i+1)} - y_{t_1 i+1}$ are linearly independent over $\mathbb{Z}_{p^s}$, for any $i \in \{0, \ldots, r\}$. Taking into account that $\alpha^\ell = 1$ and $t_1 \leq p^{t_1-1}$ for $t_1 \geq 2$, the set of vectors $\{y_{t_1 i+2} - y_{t_1 i+1}, \ldots, y_{t_1(i+1)} - y_{t_1 i+1}\}$ is equal to one of the following three sets:

$$\begin{aligned} L_1 &= \{1, \ldots, \alpha^{t_1-2}\}, \\ L_2 &= \{\alpha^{k+1} - \alpha^k, \ldots, \alpha^{k+t_1-1} - \alpha^k\}, \\ L_3 &= \{\alpha^{k+1} - \alpha^k, \ldots, \alpha^{\ell-1} - \alpha^k, -\alpha^k + pb, \alpha^\ell - \alpha^k + pb, \ldots, \alpha^{k+t_1-2} - \alpha^k + pb\}, \end{aligned}$$

for some $k \in \{0, \ldots, \ell - 1\}$ and some $b \in \mathcal{R}$. Clearly, L_1 is a set of linearly independent vectors over $\mathbb{Z}_{p^s}$.

For the second set L_2, suppose that $\sum_{i=1}^{t_1-1} \lambda_i(\alpha^{k+i} - \alpha^k) = 0$ for certain $\lambda_i \in \mathbb{Z}_{p^s}$, with some of them being non-zero. Note that, since α is a unit in $\mathcal{R}$, then $\sum_i \lambda_i(\alpha^i - 1) = 0$. Let m be the smallest integer in $\{0, \ldots, s-1\}$ for which there exists an $i \in \{1, \ldots, t_1 - 1\}$

such that $\lambda_i \in p^m\mathbb{Z}_{p^s}$ and $\lambda_i \notin p^{m+1}\mathbb{Z}_{p^s}$. For example, if all $\lambda_i \in p\mathbb{Z}_{p^s}$ and there is a certain $\lambda_i \notin p^2\mathbb{Z}_{p^s}$, then $m = 1$. Therefore, we can define $\lambda_i = p^m\lambda'_i$ for all i, and we obtain $p^m \sum_i \lambda'_i(\alpha^i - 1) = 0$, hence $\sum_i \lambda'_i(\alpha^i - 1) = p^{s-m}\lambda$ for a certain $\lambda \in \mathcal{R}$. Thus, by taking modulo p, we obtain $\sum_i \bar{\lambda}'_i(\bar{\alpha}^i - 1) = 0$ over $\mathbb{Z}_p$, with at least one $\bar{\lambda}'_i \neq 0$. Clearly, $\bar{\alpha}$ is a unit in $\mathbb{Z}_p[x]/(\bar{h}(x))$. Therefore, by applying Lemma 5.1 on the vectors $\bar{\alpha}^i - 1$ for $i \in \{1, \ldots, t_1 - 1\}$, we obtain a contradiction.

For the third set L_3, we follow a similar argument. Suppose that

$$-\lambda_{t_1-1}(\alpha^k - pb) + \sum_{i=1}^{\ell-k-1} \lambda_i(\alpha^{k+i} - \alpha^k) + \sum_{i=\ell-k}^{t_1-2} \lambda_i(\alpha^{k+i} - \alpha^k + pb) = 0$$

for certain $\lambda_i \in \mathbb{Z}_{p^s}$, with some of them being non-zero. With the same definition of m as in the previous case, we obtain $-p^m\lambda'_{t_1-1}(\alpha^k - pb) + p^m \sum_{i=1}^{\ell-k-1} \lambda'_i(\alpha^{k+i} - \alpha^k) + p^m \sum_{i=\ell-k}^{t_1-2} \lambda'_i(\alpha^{k+i} - \alpha^k + pb) = 0$, where $\lambda_i = p^m\lambda'_i$. Thus, $-\lambda'_{t_1-1}(\alpha^k - pb) + \sum_{i=1}^{\ell-k-1} \lambda'_i(\alpha^{k+i} - \alpha^k) + \sum_{i=\ell-k}^{t_1-2} \lambda'_i(\alpha^{k+i} - \alpha^k + pb) = p^{s-m}\lambda$ for some $\lambda \in \mathcal{R}$. Taking modulo p, $-\bar{\lambda}'_{t_1-1}\bar{\alpha}^k + \sum_i \bar{\lambda}'_i(\bar{\alpha}^{k+i} - \bar{\alpha}^k) = 0$ over $\mathbb{Z}_p$, with at least one $\bar{\lambda}'_i \neq 0$. Since $\bar{\alpha}$ is a unit, we obtain $-\bar{\lambda}'_{t_1-1} + \sum_i \bar{\lambda}'_i(\bar{\alpha}^i - 1) = 0$. We obtain a contradiction since the vectors $-1, \bar{\alpha} - 1, \ldots, \bar{\alpha}^{t_1-2} - 1$ are linearly independent over $\mathbb{Z}_p$. □

Example 5.1. Let $\mathcal{H}^{3,0,0}$ be the $\mathbb{Z}_{27}$-additive GH code of type $(3^6; 3, 0, 0)$. Let $\mathcal{R} = \mathrm{GR}(27^2)$ be the Galois ring over $\mathbb{Z}_{27}$, isomorphic to $\mathbb{Z}_{27}[x]/(h(x))$, where $h(x) = x^2 + 22x + 26$. This polynomial can be obtained as the Hensel lift of $f(x) = \bar{h}(x) = x^2 + x + 2$ over $\mathbb{Z}_3$. Note that $h(x)$ is a monic basic primitive polynomial dividing $x^8 - 1$ in $\mathbb{Z}_{27}[x]$. Let α be a root of $h(x)$ of order 8. Then, $T = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^7\}$ and we can order the elements of $\mathcal{R}$ as follows:

$$\begin{aligned}
\mathcal{R} = \{&0 + 3\cdot 0 + 9\cdot 0, 1 + 3\cdot 0 + 9\cdot 0, \alpha + 3\cdot 0 + 9\cdot 0, \ldots, \alpha^7 + 3\cdot 0 + 9\cdot 0,\\
&0 + 3\cdot 1 + 9\cdot 0, 1 + 3\cdot 1 + 9\cdot 0, \alpha + 3\cdot 1 + 9\cdot 0, \ldots, \alpha^7 + 3\cdot 1 + 9\cdot 0,\\
&\ldots\\
&0 + 3\cdot \alpha^7 + 9\cdot \alpha^7, 1 + 3\cdot \alpha^7 + 9\cdot \alpha^7, \alpha + 3\cdot \alpha^7 + 9\cdot \alpha^7, \ldots,\\
&\quad \alpha^7 + 3\cdot \alpha^7 + 9\cdot \alpha^7\}\\
= \{&0, 1, \alpha, \ldots, 22 + \alpha,\\
&3, 4, 3 + \alpha, \ldots, 25 + \alpha,\\
&\ldots\\
&21 + 12\alpha, 22 + 12\alpha, 21 + 13\alpha, \ldots, 16 + 13\alpha\}.
\end{aligned}$$

By Theorem 5.1, we can find r-PD-sets of size $r + 1$ for all $2 \leq r \leq f_3^{3,0,0} = 242$, by using the elements of $\mathcal{R}$. Indeed, we can construct up to 243 matrices taking all the elements of $\mathcal{R}$ in groups of 3 in order to reach the upper bound. Here, we just show a smaller example by constructing an 11-PD-set formed by 12 matrices.

Consider the following 12 matrices, constructed by dividing the first 36 ordered elements of $\mathcal{R}$ in groups of 3:

$$\mathcal{N}_0^* = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \mathcal{N}_1^* = \begin{pmatrix} 1 & 1 & 5 \\ 1 & 5 & 26 \\ 1 & 26 & 0 \end{pmatrix}, \quad \mathcal{N}_2^* = \begin{pmatrix} 1 & 0 & 26 \\ 1 & 26 & 22 \\ 1 & 22 & 1 \end{pmatrix},$$
$$\mathcal{N}_3^* = \begin{pmatrix} 1 & 3 & 0 \\ 1 & 4 & 0 \\ 1 & 3 & 1 \end{pmatrix}, \quad \mathcal{N}_4^* = \begin{pmatrix} 1 & 4 & 5 \\ 1 & 8 & 26 \\ 1 & 2 & 0 \end{pmatrix}, \quad \mathcal{N}_5^* = \begin{pmatrix} 1 & 3 & 26 \\ 1 & 2 & 22 \\ 1 & 25 & 1 \end{pmatrix},$$
$$\mathcal{N}_6^* = \begin{pmatrix} 1 & 0 & 3 \\ 1 & 1 & 3 \\ 1 & 0 & 4 \end{pmatrix}, \quad \mathcal{N}_7^* = \begin{pmatrix} 1 & 1 & 8 \\ 1 & 5 & 2 \\ 1 & 26 & 3 \end{pmatrix}, \quad \mathcal{N}_8^* = \begin{pmatrix} 1 & 0 & 2 \\ 1 & 26 & 25 \\ 1 & 22 & 4 \end{pmatrix},$$
$$\mathcal{N}_9^* = \begin{pmatrix} 1 & 3 & 15 \\ 1 & 4 & 15 \\ 1 & 3 & 16 \end{pmatrix}, \quad \mathcal{N}_{10}^* = \begin{pmatrix} 1 & 4 & 20 \\ 1 & 8 & 14 \\ 1 & 2 & 15 \end{pmatrix}, \quad \mathcal{N}_{11}^* = \begin{pmatrix} 1 & 3 & 14 \\ 1 & 2 & 10 \\ 1 & 25 & 16 \end{pmatrix}.$$

Note that there are no repeated rows in the whole set of matrices. Let $\mathcal{P}_{11} = \{\mathcal{N}_0^{-1}, \ldots, \mathcal{N}_{11}^{-1}\}$, where

$$\mathcal{N}_0^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathcal{N}_1^{-1} = \begin{pmatrix} 1 & 1 & 16 \\ 0 & 1 & 15 \\ 0 & 5 & 10 \end{pmatrix}, \quad \mathcal{N}_2^{-1} = \begin{pmatrix} 1 & 1 & 16 \\ 0 & 22 & 17 \\ 0 & 1 & 16 \end{pmatrix},$$
$$\mathcal{N}_3^{-1} = \begin{pmatrix} 1 & 24 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathcal{N}_4^{-1} = \begin{pmatrix} 1 & 25 & 25 \\ 0 & 1 & 15 \\ 0 & 5 & 10 \end{pmatrix}, \quad \mathcal{N}_5^{-1} = \begin{pmatrix} 1 & 16 & 19 \\ 0 & 22 & 17 \\ 0 & 1 & 16 \end{pmatrix},$$
$$\mathcal{N}_6^{-1} = \begin{pmatrix} 1 & 0 & 24 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathcal{N}_7^{-1} = \begin{pmatrix} 1 & 13 & 13 \\ 0 & 1 & 15 \\ 0 & 5 & 10 \end{pmatrix}, \quad \mathcal{N}_8^{-1} = \begin{pmatrix} 1 & 25 & 22 \\ 0 & 22 & 17 \\ 0 & 1 & 16 \end{pmatrix},$$
$$\mathcal{N}_9^{-1} = \begin{pmatrix} 1 & 24 & 12 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathcal{N}_{10}^{-1} = \begin{pmatrix} 1 & 4 & 10 \\ 0 & 1 & 15 \\ 0 & 5 & 10 \end{pmatrix}, \quad \mathcal{N}_{11}^{-1} = \begin{pmatrix} 1 & 1 & 22 \\ 0 & 22 & 17 \\ 0 & 1 & 16 \end{pmatrix}.$$

The matrices of $\mathcal{P}_{11}$ can also be represented as permutations of coordinate positions as shown in (9). Let $\tau_i \in \mathrm{Sym}(729)$ be the one corresponding to $\mathcal{N}_i^{-1}$, $i \in \{0, \ldots, 11\}$. Recall that $\Phi(\mathcal{N}_i^{-1}) = \Phi(\tau_i)$ as defined in (8). Then, by Theorem 5.1, $\Phi(\mathcal{P}_{11}) = \{\Phi(\mathcal{N}_i^{-1}) : i \in \{0, \ldots, 11\}\} \subseteq \mathrm{Sym}(6561)$ is an 11-PD-set of size 12 for the $\mathbb{Z}_{27}$-linear GH code $H^{3,0,0} = \Phi(\mathcal{H}^{3,0,0})$ with information set $\Phi(\mathcal{I}_{3,0,0}) = \{1, 2, 4, 10, 11, 13, 244, 245, 247\}$, given in Example 4.2.

Remark 5.1. By Corollary 4.2, $f_p^{t_1,0,\dots,0}$ is the maximum number of errors that can be corrected using r-PD-sets of size $r+1$ of the form $\Phi(\mathcal{P}_r)$, where $\mathcal{P}_r \subseteq \mathrm{PAut}(\mathcal{H}^{t_1,0,\dots,0})$. However, higher values of r could be achieved by considering elements in $\mathrm{PAut}(H^{t_1,0,\dots,0})$ that are not the Φ image of elements in $\mathrm{PAut}(\mathcal{H}^{t_1,0,\dots,0})$.

Following a similar reasoning to the one used in Theorem 5.1, we can also obtain r-PD-sets of size $r+1$ for the $\mathbb{Z}_{p^s}$-linear GH codes $H_i = H^{1,t_2,\dots,t_s}$, $i \in \{2,\dots,s\}$, of type $(n;1,t_2,\dots,t_s)$, where $t_j = 0$ for all $j \neq i$, $t_i \geq 1$, and $r \leq f_p^{1,t_2,\dots,t_s}$. Let $\mathcal{R}_i = \mathrm{GR}(p^{(s-i+1)t_i})$ be the Galois extension of dimension t_i over $\mathbb{Z}_{p^{s-i+1}}$, isomorphic to $\mathbb{Z}_{p^{s-i+1}}[x]/(h(x))$, with $h(x)$ being a monic basic primitive polynomial of degree t_i dividing $x^{p^{t_i}-1}-1$ in $\mathbb{Z}_{p^{s-i+1}}[x]$. Let $\alpha \in \mathcal{R}_i$ be a root of $h(x)$ of order $\ell = p^{t_i}-1$ and $T = \{0,1,\alpha,\alpha^2,\dots,\alpha^{\ell-1}\}$. The p-adic representation of an element $y \in \mathcal{R}_i$ is $y = a_1 + pa_2 + p^2a_3 + \cdots + p^{s-i}a_{s-i+1}$, where $a_k \in T$ for $k \in \{1,\dots,s-i+1\}$. Using this representation, we define the ordered set $\{y_1,\dots,y_{p^{(s-i+1)t_i}}\}$ with all the elements in $\mathcal{R}_i$. Consider the set of matrices $\{\mathcal{M}_0^*,\dots,\mathcal{M}_r^*\}$ of size $(t_i+1)\times(t_i+1)$ over $\mathbb{Z}_{p^s}$, where

$$\mathcal{M}_j^* = \begin{pmatrix} 1 & p^{i-1}y_{(t_i+1)j+1} \\ 1 & p^{i-1}y_{(t_i+1)j+2} \\ \vdots & \vdots \\ 1 & p^{i-1}y_{(t_i+1)(j+1)} \end{pmatrix},$$

for $j \in \{0,\dots,r\}$. Note that

$$r \leq f_p^{1,t_2,\dots,t_s} = \left\lfloor \frac{p^{(s-i+1)t_i}-1-t_i}{1+t_i} \right\rfloor$$

by Corollary 4.2. The elements $y \in \mathcal{R}_i$ are given as vectors over $\mathbb{Z}_{p^{s-i+1}}$ by using the additive representation. Then, we consider the inclusion of vectors y over $\mathbb{Z}_{p^{s-i+1}}$ to vectors over $\mathbb{Z}_{p^s}$ as $p^{i-1}y$.

Let $(1,p^{i-1}m_{j,k}^*)$ be the kth row of the matrix $\mathcal{M}_j^*$, for any $j \in \{0,\dots,r\}$. In the context of the $\mathbb{Z}_{p^s}$-linear GH code H_i, we define $\mathcal{M}_j$ as the matrix that has $(1,p^{i-1}m_{j,1}^*)$ as the first row and $(0,m_{j,k}^* - m_{j,1}^*)$ as the kth row, for $k \in \{2,\dots,t_i+1\}$. Note that this is consistent with Definition 4.1. Indeed, in the proof of Corollary 5.1, we see that $\mathcal{M}_0,\dots,\mathcal{M}_r \subseteq \mathrm{PAut}(\mathcal{H}_i)$, where $\mathcal{H}_i$ is the $\mathbb{Z}_{p^s}$-additive code such that $\Phi(\mathcal{H}_i) = H_i$.

Corollary 5.1. *Let $\mathcal{P}_r = \{\mathcal{M}_0^{-1},\dots,\mathcal{M}_r^{-1}\}$. Then, $\Phi(\mathcal{P}_r)$ is an r-PD-set of size $r+1$ for the $\mathbb{Z}_{p^s}$-linear GH code $H_i = H^{1,t_2,\dots,t_s}$, where $t_i \geq 1$, $i \in \{2,\dots,s\}$, and $t_j = 0$ for all $j \in \{2,\dots,s\}$ such that $j \neq i$, with information set $\Phi(\mathcal{I}_{1,t_2,\dots,t_s})$, for all $2 \leq r \leq f_p^{1,t_2,\dots,t_s}$.*

Proof. Since $\mathbb{Z}_{p^{s-i+1}}$ is isomorphic to $p^{i-1}\mathbb{Z}_{p^s}$, the matrices $\mathcal{M}_0^*,\dots,\mathcal{M}_r^*$ do not share a row in common. Then, the matrix $\mathcal{M}_j$ is in the form

$$\mathcal{M}_j = \begin{pmatrix} 1 & p^{i-1}y_{(t_i+1)j+1} \\ 0 & y_{(t_i+1)j+2} - y_{(t_i+1)j+1} \\ \vdots & \vdots \\ 0 & y_{(t_i+1)(j+1)} - y_{(t_i+1)j+1} \end{pmatrix}, \tag{12}$$

for any $j \in \{0, \ldots, r\}$. As shown in (5), the elements in $\mathrm{PAut}(\mathcal{H}^{1,0,\ldots,0,t_i,0,\ldots,0})$ have the form

$$\begin{pmatrix} 1 & p^{i-1}a_i \\ 0 & \zeta_{s-i+1}(A_{i,i}) \end{pmatrix}, \tag{13}$$

where $a_i \in \mathbb{Z}_{p^s}^{t_i}$ and $A_{i,i} \in \mathrm{GL}(t_i, \mathbb{Z}_{p^s})$. Note that $\zeta_{s-i+1}(A_{i,i})$ can be seen as an element of $\mathrm{GL}(t_i, \mathbb{Z}_{p^{s-i+1}})$ and, in fact, it can be any element in $\mathrm{GL}(t_i, \mathbb{Z}_{p^{s-i+1}})$.

Following the same argument as in the proof of Theorem 5.1, over the Galois ring $\mathcal{R}_i = \mathrm{GR}(p^{(s-i+1)t_i})$ instead of $\mathrm{GR}(p^{s(t_1-1)})$, it can be proven that the vectors $y_{(t_i+1)j+2} - y_{(t_i+1)j+1}, \ldots, y_{(t_i+1)(j+1)} - y_{(t_i+1)j+1}$ are linearly independent over $\mathbb{Z}_{p^{s-i+1}}$. □

Example 5.2. Let $\mathcal{H}^{1,3,0}$ be the $\mathbb{Z}_8$-additive Hadamard code of type $(2^6; 1, 3, 0)$. Let $\mathcal{R}_2 = \mathrm{GR}(4^3)$ be the Galois ring over $\mathbb{Z}_4$, isomorphic to $\mathbb{Z}_4[x]/(h(x))$, where $h(x) = x^3 + 2x^2 + x + 3$. This polynomial can be obtained as the Hensel lift of $f(x) = \bar{h}(x) = x^3 + x + 1$ over $\mathbb{Z}_2$. Note that $h(x)$ is a monic basic primitive polynomial dividing $x^7 - 1$ in $\mathbb{Z}_4[x]$. Let α be a root of $h(x)$ of order 7. Then, $T = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^6\}$ and we can order the 64 elements of $\mathcal{R}_2$ as follows:

$$\begin{aligned} \mathcal{R}_2 = \{&0 + 2 \cdot 0, 1 + 2 \cdot 0, \alpha + 2 \cdot 0, \ldots, \alpha^6 + 2 \cdot 0, \\ &0 + 2 \cdot 1, 1 + 2 \cdot 1, \alpha + 2 \cdot 1, \ldots, \alpha^6 + 2 \cdot 1, \\ &\ldots, \\ &0 + 2 \cdot \alpha^6, 1 + 2 \cdot \alpha^6, \alpha + 2 \cdot \alpha^6, \ldots, \alpha^6 + 2 \cdot \alpha^6\} \\ = \{&0, 1, \alpha, \ldots, 1 + 2\alpha + \alpha^2, \\ &2, 3, 2 + \alpha, \ldots, 3 + 2\alpha + \alpha^2, \\ &\ldots \\ &2 + 2\alpha^2, 3 + 2\alpha^2, 2 + \alpha + 2\alpha^2, \ldots, 3 + 2\alpha + 3\alpha^2\}. \end{aligned}$$

By Corollary 5.1, we can find r-PD-sets of size $r+1$ for all $2 \leq r \leq f_2^{1,3,0} = 15$, by using the elements of $\mathcal{R}_2$. Indeed, we can construct up to 16 matrices taking all the elements of $\mathcal{R}_2$, multiplied by 2, in groups of 4 in order to reach the upper bound. Here, we just show a smaller example by constructing an 8-PD-set formed by 9 matrices.

Consider the following 9 matrices over $\mathbb{Z}_8$, constructed by taking the first 36 ordered elements of $\mathcal{R}_2$ in groups of 4 and multiplying them by 2 as elements of $\mathbb{Z}_8^3$:

$$\mathcal{M}_0^* = \begin{pmatrix} 1&0&0&0\\ 1&2&0&0\\ 1&0&2&0\\ 1&0&0&2 \end{pmatrix}, \quad \mathcal{M}_1^* = \begin{pmatrix} 1&2&6&4\\ 1&4&6&6\\ 1&6&6&2\\ 1&2&4&2 \end{pmatrix}, \quad \mathcal{M}_2^* = \begin{pmatrix} 1&4&0&0\\ 1&6&0&0\\ 1&4&2&0\\ 1&4&0&2 \end{pmatrix},$$

$$\mathcal{M}_3^* = \begin{pmatrix} 1&6&6&4\\ 1&0&6&6\\ 1&2&6&2\\ 1&6&4&2 \end{pmatrix}, \quad \mathcal{M}_4^* = \begin{pmatrix} 1&0&4&0\\ 1&2&4&0\\ 1&0&6&0\\ 1&0&4&2 \end{pmatrix}, \quad \mathcal{M}_5^* = \begin{pmatrix} 1&2&2&4\\ 1&4&2&6\\ 1&6&2&2\\ 1&2&0&2 \end{pmatrix},$$

$$\mathcal{M}_6^* = \begin{pmatrix} 1&0&0&4\\ 1&2&0&4\\ 1&0&2&4\\ 1&0&0&6 \end{pmatrix}, \quad \mathcal{M}_7^* = \begin{pmatrix} 1&2&6&0\\ 1&4&6&2\\ 1&6&6&6\\ 1&2&4&6 \end{pmatrix}, \quad \mathcal{M}_8^* = \begin{pmatrix} 1&4&4&0\\ 1&6&4&0\\ 1&4&6&0\\ 1&4&4&2 \end{pmatrix}.$$

Note that there are no repeated rows in the whole set of matrices. Let $\mathcal{P}_8 = \{\mathcal{M}_0^{-1}, \ldots, \mathcal{M}_8^{-1}\}$, where

$$\mathcal{M}_0^{-1} = \begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix}, \quad \mathcal{M}_1^{-1} = \begin{pmatrix} 1&6&4&6\\ 0&3&3&0\\ 0&2&3&3\\ 0&2&1&0 \end{pmatrix}, \quad \mathcal{M}_2^{-1} = \begin{pmatrix} 1&4&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix},$$

$$\mathcal{M}_3^{-1} = \begin{pmatrix} 1&2&0&6\\ 0&3&3&0\\ 0&2&3&3\\ 0&2&1&0 \end{pmatrix}, \quad \mathcal{M}_4^{-1} = \begin{pmatrix} 1&0&4&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix}, \quad \mathcal{M}_5^{-1} = \begin{pmatrix} 1&6&0&2\\ 0&3&3&0\\ 0&2&3&3\\ 0&2&1&0 \end{pmatrix},$$

$$\mathcal{M}_6^{-1} = \begin{pmatrix} 1&0&0&4\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix}, \quad \mathcal{M}_7^{-1} = \begin{pmatrix} 1&6&0&6\\ 0&3&3&0\\ 0&2&3&3\\ 0&2&1&0 \end{pmatrix}, \quad \mathcal{M}_8^{-1} = \begin{pmatrix} 1&4&4&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix}.$$

The matrices of $\mathcal{P}_8$ can also be represented as permutations of coordinate positions as shown in (9). Let $\tau_i \in \mathrm{Sym}(64)$ be the one corresponding to $\mathcal{M}_i^{-1}$, $i \in \{0, \ldots, 8\}$. For example, matrix $\mathcal{M}_1^{-1}$ is equivalent to the permutation

$$\begin{aligned}\tau_1 = {} & (1,60,19,56,37,46)(2,55,42,23,34,63)(3,50,49,54,47,16)\\ & (4,61,12,21,44,29)(5,38,41,28,27,32)(6,33,52,59,24,45)\\ & (7,48,11,26,17,62)(8,43,18,57,30,15)(9,20,51,64,13,14)\\ & (10,31)(22,39,40,35,58,25)(36,53).\end{aligned}$$

Recall that $\Phi(\mathcal{M}_j^{-1}) = \Phi(\tau_j)$ as defined in (8). Then, by Corollary 5.1, $\Phi(\mathcal{P}_8) = \{\Phi(\mathcal{M}_j^{-1}) : j \in \{0, \ldots, 8\}\} \subseteq \mathrm{Sym}(256)$ is an 8-PD-set of size 9 for the $\mathbb{Z}_8$-linear Hadamard code $H^{1,3,0} = \Phi(\mathcal{H}^{1,3,0})$ with information set $\Phi(\mathcal{I}_{1,3,0}) = \{1, 2, 3, 5, 7, 17, 19, 65, 67\}$.

6. Recursive constructions of r-PD-sets

In this section, given an r-PD-set of size ℓ for a $\mathbb{Z}_{p^s}$-linear GH code $H^{t_1,\dots,t_s}$, we show that one can easily obtain an r-PD-set of size ℓ for the $\mathbb{Z}_{p^s}$-linear GH code $H^{t_1+i_1,\dots,t_s+i_s}$, for all $i_1,\dots,i_s \geq 0$. In particular, this is useful to obtain r-PD-sets for any code $H^{t_1,\dots,t_s}$, including those of type different to $(n;t_1,0,\dots,0)$ and $(n;1,0,\dots,0,t_i,0,\dots,0)$, $i \in \{2,\dots,s\}$, which have been already considered in Section 5.

We present two different constructions that produce a similar result. One uses the matrix representation of the elements in $\mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$ and the other one uses the permutation representation. These constructions are a generalization of the ones given in [2] for $\mathbb{Z}_4$-linear Hadamard codes.

6.1. Matrix representation

In this first construction, we consider the elements of $\mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$ as matrices in the subgroup $\pi(\mathcal{L})$ of $\mathrm{GL}(t_1+\cdots+t_s,\mathbb{Z}_{p^s})$, described in Section 3. Consider a matrix $\mathcal{M} \in \mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$ in the form given in (5) and s positive integers $\kappa_1,\dots,\kappa_s$. Then, we define the matrix $\mathcal{M}(\kappa_1,\dots,\kappa_s)$ as

$$\begin{pmatrix} 1 & a'_1 & pa'_2 & \cdots & p^{s-2}a'_{s-1} & p^{s-1}a'_s \\ \mathbf{0} & A'_{1,1} & pA'_{1,2} & \cdots & p^{s-2}A'_{1,s-1} & p^{s-1}A'_{1,s} \\ \mathbf{0} & \zeta_{s-1}(A'_{2,1}) & \zeta_{s-1}(A'_{2,2}) & \cdots & \zeta_{s-1}(p^{s-3}A'_{2,s-1}) & \zeta_{s-1}(p^{s-2}A'_{2,s}) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \zeta_2(A'_{s-1,1}) & \zeta_2(A'_{s-1,2}) & \cdots & \zeta_2(A'_{s-1,s-1}) & \zeta_2(pA'_{s-1,s}) \\ \mathbf{0} & \zeta_1(A'_{s,1}) & \zeta_1(A'_{s,2}) & \cdots & \zeta_1(A'_{s,s-1}) & \zeta_1(A'_{s,s}) \end{pmatrix},$$

where $a'_1 = (a_1,\mathbf{0}) \in \mathbb{Z}_{p^s}^{t_1-1+\kappa_1}$, $a'_j = (a_j,\mathbf{0}) \in \mathbb{Z}_{p^s}^{t_j+\kappa_j}$ for $j \in \{2,\dots,s\}$, $A'_{1,1} = \begin{pmatrix} A_{1,1} & \mathbf{0} \\ \mathbf{0} & \mathrm{Id}_{\kappa_1} \end{pmatrix} \in \mathrm{GL}(t_1-1+\kappa_1)$, $A'_{i,i} = \begin{pmatrix} A_{i,i} & \mathbf{0} \\ \mathbf{0} & \mathrm{Id}_{\kappa_i} \end{pmatrix} \in \mathrm{GL}(t_i+\kappa_i,\mathbb{Z}_{p^s})$ for $i \in \{2,\dots,s\}$, and $A'_{i,j} = \begin{pmatrix} A_{i,j} & \mathbf{0} \end{pmatrix}$, $A'_{j,i} = \begin{pmatrix} A_{j,i} \\ \mathbf{0} \end{pmatrix}$ are matrices over $\mathbb{Z}_{p^s}$ for $i,j \in \{1,\dots,s\}$ with $i<j$, respectively. Note that $\mathcal{M}(\kappa_1,\dots,\kappa_s) \in \mathrm{GL}(t_1+\cdots+t_s+\kappa_1+\cdots+\kappa_s,\mathbb{Z}_{p^s})$.

Proposition 6.1. *Let $\mathcal{P}_r = \{\mathcal{M}_0,\dots,\mathcal{M}_r\} \subseteq \mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$ such that $\Phi(\mathcal{P}_r)$ is an r-PD-set of size $r+1$ for $H^{t_1,\dots,t_s}$ with information set $\Phi(\mathcal{I}_{t_1,\dots,t_s})$. Then, $\mathcal{Q}_r = \{(\mathcal{M}_i^{-1}(\kappa_1,\dots,\kappa_s))^{-1} : i \in \{0,\dots,r\}\} \subseteq \mathrm{PAut}(\mathcal{H}^{t_1+\kappa_1,\dots,t_s+\kappa_s})$ and $\Phi(\mathcal{Q}_r)$ is an r-PD-set of size $r+1$ for $H^{t_1+\kappa_1,\dots,t_s+\kappa_s}$ with information set $\Phi(\mathcal{I}_{t_1+\kappa_1,\dots,t_s+\kappa_s})$, for any $\kappa_1,\dots,\kappa_s \geq 0$.*

Proof. Since $\mathcal{M}_i^{-1} \in \mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$, $\mathcal{M}_i^{-1}(\kappa_1,\dots,\kappa_s) \in \mathrm{PAut}(\mathcal{H}^{t_1+\kappa_1,\dots,t_s+\kappa_s})$, so $\mathcal{Q}_r \subseteq \mathrm{PAut}(\mathcal{H}^{t_1+\kappa_1,\dots,t_s+\kappa_s})$. Moreover, if $\Phi(\mathcal{P}_r)$ is an r-PD-set for $\mathcal{H}^{t_1,\dots,t_s}$, by Theorem 4.1,

the matrices $(\mathcal{M}_i^{-1})^*$ for $i \in \{0, \ldots, r\}$ share no row in common. Clearly, the extended matrices $(\mathcal{M}_i^{-1}(\kappa_1, \ldots, \kappa_s))^*$ do not share any row either. □

6.2. Permutation representation

In the second construction, the elements of $\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$ are considered as permutations in $\mathrm{Sym}(n)$, where $n = p^{s(t_1-1)+(s-1)t_2+\cdots+t_s}$. Let $\sigma \in \mathrm{Sym}(n)$ and let q be a positive integer, then we define $q\sigma \in \mathrm{Sym}(qn)$ as the permutation that acts as σ in each of the following sets of coordinate positions: $\{1, \ldots, n\}$, $\{n+1, \ldots, 2n\}$, $\{2n+1, \ldots, 3n\}$, $\ldots$, $\{(q-1)n+1, \ldots, qn\}$.

Proposition 6.2. *Let S be an r-PD-set of size ℓ for $H^{t_1,\ldots,t_s}$ of length n with information set I. Then, $pS = \{p\sigma : \sigma \in S\}$ is an r-PD-set of size ℓ for $H^{t_1,\ldots,t_{s-1},t_s+1}$, with respect to any information set $I' = I \cup \{j+n\}$ with $j \in I$.*

Proof. Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$, $H = \Phi(\mathcal{H})$, $\mathcal{H}^{(s)} = \mathcal{H}^{t_1,\ldots,t_{s-1},t_s+1}$ and $H^{(s)} = \Phi(\mathcal{H}^{(s)})$. Using the recursive construction given in (3), we obtain

$$\begin{aligned} H^{(s)} &= \{\Phi((h,h,h,\ldots,h) + \lambda(\mathbf{0}, \mathbf{p}^{s-1}, 2\mathbf{p}^{s-1}, \ldots, (p-1)\mathbf{p}^{s-1})) : h \in \mathcal{H}, \lambda \in \mathbb{Z}_p\} \\ &= \{(\Phi(h), \Phi(h+\lambda\mathbf{p}^{s-1}), \Phi(h+\lambda 2\mathbf{p}^{s-1}), \ldots, \Phi(h+\lambda(p-1)\mathbf{p}^{s-1})) : \\ &\qquad h \in \mathcal{H}, \lambda \in \mathbb{Z}_p\}, \end{aligned}$$

where $\mathbf{0}$ and $\mathbf{p}^{s-1}$ are the vectors with 0 and p^{s-1} in all components, respectively. We have that $\Phi(h + \lambda\mu\mathbf{p}^{s-1}) = \Phi(h) + \lambda\mu\Phi(\mathbf{p}^{s-1}) = \Phi(h) + \lambda\mu\mathbf{1}$ for any $\lambda, \mu \in \mathbb{Z}_p$ [5]. Therefore,

$$H^{(s)} = \{(h', h'+\lambda\mathbf{1}, h'+\lambda\mathbf{2}, \ldots, h'+\lambda(\mathbf{p}-\mathbf{1})) : h' \in H, \lambda \in \mathbb{Z}_p\}.$$

If $\sigma \in \mathrm{PAut}(H)$, then $\sigma(x) = y \in H$ for any $x \in H$. Consider an element $\mathbf{x} = (x, x+\lambda\mathbf{1}, \ldots, x+\lambda(\mathbf{p}-\mathbf{1})) \in H^{(s)}$. Then,

$$\begin{aligned} (p\sigma)(x, x+\lambda\mathbf{1}, \ldots, x+\lambda(\mathbf{p}-\mathbf{1})) &= (\sigma(x), \sigma(x)+\sigma(\lambda\mathbf{1}), \ldots, \sigma(x)+\sigma(\lambda(\mathbf{p}-\mathbf{1}))) \\ &= (y, y+\lambda\mathbf{1}, \ldots, y+\lambda(\mathbf{p}-\mathbf{1})) \in H^{(s)}, \end{aligned}$$

which means that $p\sigma \in \mathrm{PAut}(H^{(s)})$.

Let $I \subseteq \{1, \ldots, n\}$ be an information set for H. Define $I' = I \cup \{j+n\}$, for any $j \in I$. We have that $\mathbf{x}|_{I'} = (x|_I, x_j + \lambda)$, for any $\mathbf{x} = (x, x+\lambda\mathbf{1}, \ldots, x+\lambda(\mathbf{p}-\mathbf{1})) \in H^{(s)}$, where $x \in H$ and $\lambda \in \mathbb{Z}_p$. Since there are $p^{st_1+(s-1)t_2+\cdots+t_s}$ different possible values of $x|_I$ and p possible values of λ, we obtain $p^{st_1+(s-1)t_2+\cdots+2t_{s-1}+t_s+1}$ different elements $\mathbf{x}|_{I'}$, which means that I' is an information set for $H^{(s)}$.

Consider an error vector $e = (e^1, \ldots, e^p) \in \mathbb{Z}_p^{pn}$ of weight $\mathrm{wt}_H(e) \leq r$, where $e^k = (e_1^k, \ldots, e_n^k) \in \mathbb{Z}_p^n$ for $k \in \{1, \ldots, p\}$. In order for pS to be an r-PD-set for $H^{(s)}$ with

respect to I', there must be an element $p\sigma \in pS$ such that $\mathrm{wt}_H((p\sigma)(e)|_{I'}) = 0$. Note that $p\sigma(e) = (\sigma(e^1), \ldots, \sigma(e^p))$. Consider the vector $\hat{e} = (\hat{e}_1, \ldots, \hat{e}_n) \in \mathbb{Z}_p^n$ such that $\hat{e}_i = 1$ if $e_i^1 > 0$ or $e_i^2 > 0$, and $\hat{e}_i = 0$ otherwise, $i \in \{1, \ldots, n\}$. Since $\mathrm{wt}_H(\hat{e}) \leq r$, there exists $\sigma \in S$ such that $\mathrm{wt}_H(\sigma(\hat{e})|_I) = 0$. Therefore, $\mathrm{wt}_H(\sigma(e^1)|_I) = 0$ and $\mathrm{wt}_H(\sigma(e^2)|_I) = 0$, hence $\mathrm{wt}_H((p\sigma(e))|_{I\cup\{j+n : j\in I\}}) = 0$. Since $I' \subseteq I \cup \{j+n : j \in I\}$, we obtain that pS is an r-PD-set for $H^{(s)}$ with information set I'. □

Note that Proposition 6.2 uses directly permutations from $\mathrm{PAut}(H^{t_1,\ldots,t_s})$, without assuming that they come from elements in $\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$. This means that one can also use r-PD-sets for an r that may exceed the upper bound given by Corollary 4.2. This is not the case in the following proposition, since if S is an r-PD-set for $H^{t_1,\ldots,t_s}$, then it is not always true that $p^{s-i+1}S$ is an r-PD-set for $H^{(i)}$ for $i \in \{1, \ldots, s-1\}$, where $H^{(i)} = \Phi(\mathcal{H}^{(i)})$ and $\mathcal{H}^{(i)} = \mathcal{H}^{t_1,\ldots,t_{i-1},t_i+1,t_{i+1},\ldots,t_s}$. This is because if $\sigma \in \mathrm{PAut}(H^{t_1,\ldots,t_s})$, it is generally not true that $p^{s-i+1}\sigma \in \mathrm{PAut}(H^{(i)})$. Instead, we have to assume that the r-PD-sets come from sets in $\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$ and extend each permutation $\sigma \in \mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$ as $p^{s-i+1}\sigma \in \mathrm{PAut}(\mathcal{H}^{(i)})$ before applying the map Φ to obtain permutations in $\mathrm{PAut}(H^{(i)})$.

Proposition 6.3. *Let $\mathcal{S} \subseteq \mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$ such that $\Phi(\mathcal{S})$ is an r-PD-set of size ℓ for $H^{t_1,\ldots,t_s}$ with information set $I = \Phi(\mathcal{I})$, where $\mathcal{I}$ is an additive information set for $\mathcal{H}^{t_1,\ldots,t_s}$. Then, for any $i \in \{1, \ldots, s\}$, $\Phi(p^{s-i+1}\mathcal{S})$ is an r-PD-set of size ℓ for $H^{t'_1,\ldots,t'_s}$, with $t'_i = t_i + 1$ and $t'_j = t_j$ for any $j \neq i$, with respect to any information set $I' = \Phi(\mathcal{I} \cup \{j+n\})$ with $j \in I$, where n is the length of $\mathcal{H}^{t_1,\ldots,t_s}$.*

Proof. We follow a similar argument to the one given in Proposition 6.2, with the difference that $\mathcal{S}$ is a subset of $\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$ and not of $\mathrm{PAut}(H^{t_1,\ldots,t_s})$. Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$, $H = \Phi(\mathcal{H})$, $\mathcal{H}^{(i)} = \mathcal{H}^{t'_1,\ldots,t'_s}$ and $H^{(i)} = \Phi(\mathcal{H}^{(i)})$. Taking into account that $\mathcal{H}^{(i)}$ is constructed using (3),

$$H^{(i)} = \{(\Phi(h), \Phi(h + \lambda\mathbf{p}^{i-1}), \Phi(h + \lambda 2\mathbf{p}^{i-1}), \ldots, \Phi(h + \lambda(p^{s-i+1} - 1)\mathbf{p}^{i-1})) : h \in \mathcal{H}, \lambda \in \mathbb{Z}_{p^{s-i+1}}\}.$$

If $\tau \in \mathrm{PAut}(\mathcal{H})$, then

$$\begin{aligned}(p^{s-i+1}\tau)(\mathbf{h}) &= (\sigma(h), \sigma(h) + \sigma(\lambda\mathbf{p}^{\mathbf{i-1}}), \ldots, \sigma(x) + \sigma(\lambda(p^{s-i+1} - 1)\mathbf{p}^{\mathbf{i-1}})) \\ &= (\sigma(h), \sigma(h) + \lambda\mathbf{p}^{\mathbf{i-1}}, \ldots, \sigma(h) + \lambda(p^{s-i+1} - 1)\mathbf{p}^{\mathbf{i-1}}) \in \mathcal{H}^{(i)},\end{aligned}$$

for any $\mathbf{h} = (h, h+\lambda\mathbf{p}^{\mathbf{i-1}}, \ldots, h+\lambda(p^{s-i+1}-1)\mathbf{p}^{\mathbf{i-1}}) \in \mathcal{H}^{(i)}$, with $h \in \mathcal{H}$ and $\lambda \in \mathbb{Z}_{p^{s-i+1}}$. Therefore, $(p^{s-i+1}\tau) \in \mathrm{PAut}(\mathcal{H}^{(i)})$ and $\Phi(p^{s-i+1}\tau) \in \mathrm{PAut}(H^{(i)})$.

By Proposition 4.1, the set $\mathcal{I} \cup \{n+1\}$ is an additive information set for $\mathcal{H}^{(i)}$. In fact, in the proof we also show that any set $\mathcal{I} \cup \{x\}$, for $x \in \{n+1, \ldots, 2n\}$ is also an information set. In particular $\mathcal{I}' = \mathcal{I} \cup \{j+n\}$, for any $j \in \mathcal{I}$, is an information set

for $\mathcal{H}^{(i)}$ and $I' = \Phi(\mathcal{I}')$ is an information set for $H^{(i)}$. Note that I' has $s-i+1$ more coordinates than I.

Finally, consider an error vector $e = (e^1, \dots, e^{p^{s-i+1}})$ of weight $\mathrm{wt}_H(e) \leq r$, where $e^k = (e_1^k, \dots, e_n^k) \in \mathbb{Z}_p^n$ for $k \in \{1, \dots, p^{s-i+1}\}$. Define the vector $\hat{e} = (\hat{e}_1, \dots, \hat{e}_n) \in \mathbb{Z}_p^n$ that satisfies $\hat{e}_m = 1$ if $e_m^1 \neq 0$ or $e_m^2 \neq 0$, and $\hat{e}_m = 0$ otherwise, $m \in \{1, \dots, n\}$. Since $\mathrm{wt}_H(\hat{e}) \leq r$, there exists $\tau \in \mathcal{S}$ such that $\mathrm{wt}_H(\Phi(\tau)(\hat{e})|_I) = 0$. Thus, $\mathrm{wt}_H(\Phi(\tau)(e^1)|_I) = 0$ and $\mathrm{wt}_H(\Phi(\tau)(e^2)|_I) = 0$. Note that $\Phi(p^{s-i+1}\tau)(e) = (\Phi(\tau)(e^1), \dots, \Phi(\tau)(e^{p^{s-i+1}}))$. Therefore,

$$\mathrm{wt}_H(\Phi(p^{s-i+1}\tau)(e)|_{I \cup \{j+p^{s-1}n : j \in I\}}) = \mathrm{wt}_H(\Phi(\tau)(e^1)|_I) + \mathrm{wt}_H(\Phi(\tau)(e^2)|_I) = 0.$$

Since $I' \subseteq I \cup \{j + p^{s-1}n : j \in I\}$, this implies that $\Phi(p^{s-i+1}\mathcal{S})$ is an r-PD-set for $H^{(i)}$ with information set I'. □

Remark 6.1. By the definition of $p^{s-i+1}\tau$ and Φ, we have that $\Phi(p^{s-i+1}\tau) = p^{s-i+1}\Phi(\tau)$, for any $\tau \in \mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$ and $i \in \{1, \dots, s\}$. By the proof of Proposition 6.3, $p^{s-i+1}\tau \in \mathrm{PAut}(\mathcal{H}^{(i)})$, so $p^{s-i+1}\Phi(\tau) \in \mathrm{PAut}(H^{(i)})$, where $\mathcal{H}^{(i)}, H^{(i)}$ are defined as in this proof.

Example 6.1. Consider the $\mathbb{Z}_{27}$-linear GH code $H^{3,0,0}$ as in Example 5.1. We have that $\Phi(\mathcal{P}_{11})$ is an 11-PD-set of size 12, where $\mathcal{P}_{11}$ can be identified by the set of permutations $\{\mathrm{id}, \tau_1, \dots, \tau_{11}\} \subseteq \mathrm{Sym}(729)$. Then, by Proposition 6.2 or Proposition 6.3, we know that the following subset of Sym(19683):

$$\{3\Phi(\mathrm{id}), 3\Phi(\tau_1), \dots, 3\Phi(\tau_{11})\}$$

is an 11-PD-set for the $\mathbb{Z}_{27}$-linear GH code $H^{3,0,1}$, with information set $\Phi(\mathcal{I}_{3,0,1}) = \Phi(\mathcal{I}_{3,0,0}) \cup \Phi^{(3)}(\{730\}) = \{1, 2, 4, 10, 11, 13, 244, 245, 247, 6562\}$. Similarly, by Proposition 6.3 and Remark 6.1, we know that the following subset of Sym(59049):

$$\{9\Phi(\mathrm{id}), 9\Phi(\tau_1), \dots, 9\Phi(\tau_{11})\}$$

is an 11-PD-set for the $\mathbb{Z}_{27}$-linear GH code $H^{3,1,0}$, with information set $\Phi(\mathcal{I}_{3,1,0}) = \Phi(\mathcal{I}_{3,0,0}) \cup \Phi^{(2)}(\{730\}) = \{1, 2, 4, 10, 11, 13, 244, 245, 247, 6562, 6565\}$. In general, we can construct r-PD-sets for $H^{3,0,1}$ and $H^{3,1,0}$ for any $r \leq f_3^{3,0,0} = 242$.

We could also use Proposition 6.3 in order to obtain an 11-PD-set for the $\mathbb{Z}_{27}$-linear GH code $H^{4,0,0}$, or in general an r-PD-set for any $r \leq f_3^{3,0,0} = 242$. However, in this case, we can construct an r-PD-set directly, from the explicit construction presented in Section 5, for any $r \leq f_3^{4,0,0} = 4919$.

Corollary 6.1. *Let $\mathcal{S} \subseteq \mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$ such that $\Phi(\mathcal{S})$ is an r-PD-set of size ℓ for $H^{t_1,\dots,t_s}$ with information set I. Then, $\Phi(p^{si_1+(s-1)i_2+\cdots+i_s}\mathcal{S})$ is an r-PD-set of size ℓ for $H^{t_1+i_1,t_2+i_2,\dots,t_s+i_s}$, with the information set obtained by applying recursively Proposition 4.1, for any $i_1, i_2, \dots, i_s \geq 0$.*

Corollary 6.2. *If* $\mathcal{P}_r = \{\mathcal{N}_0^{-1}, \ldots, \mathcal{N}_r^{-1}\}$, *as defined in Section 5 for the* $\mathbb{Z}_{p^s}$*-linear GH code* $H^{t_1,0,\ldots,0}$, *then* $\Phi(p^{(s-1)t_2+\cdots+t_s}\mathcal{P}_r)$ *is an* r*-PD-set of size* $r+1$ *for the* $\mathbb{Z}_{p^s}$*-linear GH code* $H^{t_1,\ldots,t_s}$, *for all* $t_2, \ldots, t_s \geq 0$, $t_1 \geq 2$ *and* $2 \leq r \leq f_p^{t_1,0,\ldots,0}$. *Similarly, if* $\mathcal{P}_r = \{\mathcal{M}_0^{-1}, \ldots, \mathcal{M}_r^{-1}\}$, *as defined in Section 5 for the* $\mathbb{Z}_{p^s}$*-linear GH code* $H^{1,0,\ldots,0,t_i,0,\ldots,0}$. *Then,* $\Phi(p^a\mathcal{P}_r)$, *where* $a = s(t_1-1)+\cdots+(s-i+2)t_{i-1}+(s-i)t_{i+1}+\cdots+t_s$, *is an* r*-PD-set of size* $r+1$ *for the* $\mathbb{Z}_{p^s}$*-linear GH code* $H^{t_1,\ldots,t_s}$, *for all* $t_2, \ldots, t_s \geq 0$, $t_1, t_i \geq 1$ *and* $2 \leq r \leq f_p^{1,0,\ldots,0,t_i,0,\ldots,0}$.

Depending on the type of the $\mathbb{Z}_{p^s}$-linear GH code, the largest r allowed by Corollary 6.2 may be either $f_p^{t_1,0,\ldots,0}$ or one of $f_p^{1,0,\ldots,0,t_i,0,\ldots,0}$, for $i \in \{2, \ldots, s\}$. Let us define

$$\tilde{f}_p^{t_1,\ldots,t_s} = \max\{f_p^{t_1,0,\ldots,0}, f_p^{1,t_2,0,\ldots,0}, \ldots, f_p^{1,0,\ldots,0,t_s}\} \leq f_p^{t_1,\ldots,t_s}.$$

If $\tilde{f}_p^{t_1,\ldots,t_s} = f_p^{t_1,0,\ldots,0}$, we achieve the largest r by using the explicit construction to obtain $\mathcal{P}_r$ for $H^{t_1,0\ldots,0}$ and then extending the r-PD-set as $\Phi(p^{(s-1)t_2+\cdots+t_s}\mathcal{P}_r)$. However, if $\tilde{f}_p^{t_1,\ldots,t_s} = f_p^{1,0,\ldots,0,t_i,0,\ldots,0}$, we achieve the largest r by using the explicit construction to obtain $\mathcal{P}_r$ for $H^{1,0,\ldots,0,t_i,0,\ldots,0}$ and then extending the PD-set as $\Phi(p^{s(t_1-1)+\cdots+(s-i+2)t_{i-1}+(s-i)t_{i+1}+\cdots+t_s}\mathcal{P}_r)$.

Example 6.2. Consider the $\mathbb{Z}_8$-linear Hadamard codes $H^{3,3,7}$, $H^{3,4,7}$ and $H^{3,3,8}$. By Corollary 4.2, we have $f_2^{3,0,0} = 20$, $f_2^{1,3,0} = 15$, $f_2^{1,0,7} = 15$, $f_2^{1,4,0} = 50$, $f_2^{1,0,8} = 27$. Therefore, for example,

- for $H^{3,3,7}$, since $\tilde{f}_2^{3,3,7} = \max\{f_2^{3,0,0}, f_2^{1,3,0}, f_2^{1,0,7}\} = f_2^{3,0,0} = 20$, it is better to start by using the explicit construction for $H^{3,0,0}$.
- for $H^{3,4,7}$, since $\tilde{f}_2^{3,4,7} = f_2^{1,4,0} = 50$, it is better to start with the explicit construction for $H^{1,4,0}$.
- for $H^{3,3,8}$, since $\tilde{f}_2^{3,3,8} = f_2^{1,0,8} = 27$, it is better to start with the explicit construction for $H^{1,0,8}$.

7. Computational results

The explicit constructions presented in Section 5 give r-PD-sets of size $r+1$ with an r that reaches up to the upper bound given by Corollary 4.2. However, these constructions are only defined for some specific $\mathbb{Z}_{p^s}$-linear GH codes: $H^{t_1,0,\ldots,0}$ and $H^{1,0,\ldots,0,t_i,0,\ldots,0}$, with $t_1 \geq 2$ and $t_i \geq 1$, respectively. The recursive constructions presented in Section 6 allow to obtain r-PD-sets for all $\mathbb{Z}_{p^s}$-linear GH codes $H^{t_1,\ldots,t_s}$, but they may not achieve the upper bound. Indeed, for the codes where the explicit constructions can not be applied, $r \leq \tilde{f}_p^{t_1,\ldots,t_s} < f_p^{t_1,\ldots,t_s}$, so other strategies are necessary in order to achieve a value of r closer to the theoretical upper bound $f_p^{t_1,\ldots,t_s}$.

In this section, we present some computational results, obtained by using the computer algebra system Magma [9]. These results show that we can increase the value of r for $\mathbb{Z}_{p^s}$-linear GH codes $H^{t_1,\ldots,t_s}$, by looking for r-PD-sets randomly. We follow a similar method

Table 1
Maximum value r for which r-PD-sets were found for some codes H^{t_1,t_2}, with $p = 2$, using a non-deterministic method. Comparison with previous results, r_{old}, given in [2] and the upper bound $f_2^{t_1,t_2}$.

t_1	t_2	r_{old}	r	$f_2^{t_1,t_2}$
3	0	4	**4**	4
	1	6	**7**	7
	2	10	**11**	11
	3	16	**18**	20
	4	26	**31**	35
	5	42	**50**	63
4	0	15	**15**	15
	1	23	**23**	24
	2	36	**38**	41
	3	56	**62**	72
	4	91	**103**	127
	5	150	**172**	226
5	0	50	**50**	50
	1	72	**76**	84
	2	116	**124**	145
	3	187	**199**	255
	4	312	**321**	454
	5	518	**551**	818

as the one used in [2]. That is, we generate sets $\mathcal{P}_r = \{\mathcal{M}_0, \ldots, \mathcal{M}_r\}$ of $r+1$ random matrices in $\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$ such that all rows from the matrices of $\{\mathcal{M}_0^*, \ldots, \mathcal{M}_r^*\}$ are different. The sets are constructed incrementally, starting from different initial matrices $\mathcal{M}_0$ until the target value of r is achieved. Initially, the target value of r is defined as the upper bound $f_p^{t_1,\ldots,t_s}$. If the method has generated $k < r$ matrices $\mathcal{M}_0^*, \ldots, \mathcal{M}_k^*$, and fails to generate $\mathcal{M}_{k+1}^*$ in a defined time constraint, then it starts again from another initial matrix $\mathcal{M}_0^*$. If the target value r is not attained after a certain number of different initial matrices, then r is decreased by one and the process starts again. If, by decreasing r, it reaches the value of $\tilde{f}_p^{t_1,\ldots,t_s}$, then the r-PD-set given by Corollary 6.2 is returned.

Table 1 shows the maximum values of r obtained for $\mathbb{Z}_4$-linear Hadamard codes H^{t_1,t_2}, with $3 \le t_1 \le 5$ and $0 \le t_2 \le 5$. They are compared with the values given in [2] and the upper bound $f_2^{t_1,t_2}$. The results from [2] were obtained by using a method that is currently implemented in the Magma function `PDSetHadamardCodeZ4(t1, t2: AlgMethod:= "Nondeterministic")` included in the official distribution [9]. We have corrected an error found in the implementation of this function and made some improvements, which has allow us to achieve larger values of r in this case. Then, we have generalized these functions to deal with $\mathbb{Z}_{p^s}$-linear GH codes. Table 2 shows the maximum values of r obtained for $\mathbb{Z}_8$-linear Hadamard codes H^{t_1,t_2,t_3}, with $t_1 = 3$, $0 \le t_2 \le 2$ and $0 \le t_3 \le 3$. The upper bounds $\tilde{f}_2^{3,t_2,t_3}$ and f_2^{3,t_2,t_3} are also shown in order to see the improvement with respect to the recursive construction, which is bounded by $\tilde{f}_2^{3,t_2,t_3}$, and with respect to the theoretical maximum, given by f_2^{3,t_2,t_3}.

Table 2
Maximum value r for which r-PD-sets were found for some codes H^{3,t_2,t_3}, with $p = 2$, using a non-deterministic method. Comparison with the upper bound of the recursive constructions $\tilde{f}_2^{3,t_2,t_3}$ and the upper bound f_2^{3,t_2,t_3}.

t_2	t_3	$\tilde{f}_2^{3,t_2,t_3}$	r	f_2^{3,t_2,t_3}
0	0	20	**20**	20
	1	20	**30**	31
	2	20	**46**	50
	3	20	**73**	84
1	0	20	**61**	63
	1	20	**94**	101
	2	20	**149**	169
	3	20	**242**	291
2	0	20	**189**	203
	1	20	**299**	340
	2	20	**476**	584
	3	20	**773**	1023

The Magma function developed to construct r-PD-sets of size $r+1$ for $\mathbb{Z}_{p^s}$-linear GH codes has been included in a new Magma package to deal with linear codes over $\mathbb{Z}_{p^s}$ [17]. This package also allows the construction of $\mathbb{Z}_{p^s}$-linear GH codes, and includes functions related to generalized Gray maps, information sets, the process of encoding and decoding using permutation decoding, among others. This package generalizes some of the functions for codes over $\mathbb{Z}_4$, which are already included in the standard Magma distribution [9]. It has been developed mainly by the authors of this paper and the collaboration of some undergraduate students. The first version of this new package and a manual describing all functions will be released this year, and it will be available in a GitHub repository and in the CCSG web site (http://ccsg.uab.cat)

8. Conclusions

In this paper, we determine the permutation automorphism group of $\mathbb{Z}_{p^s}$-additive GH codes, $\mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$, and give a representation of the elements as matrices of the general linear group over $\mathbb{Z}_{p^s}$ of dimension $t_1+\cdots+t_s$. Then, explicit constructions of r-PD-sets of size $r+1$ for $\mathbb{Z}_{p^s}$-linear GH codes of types $(n; t_1, 0, \dots, 0)$ and $(n; 1, 0, \dots, 0, t_i, 0, \dots, 0)$, with $t_1 \geq 2$ and $t_i \geq 1$, respectively, are given. For these cases, the value of r is upper-bounded by $f_p^{t_1,0,\dots,0}$ or $f_p^{1,0,\dots,0,t_i,0,\dots,0}$ depending on the type. In general, for $\mathbb{Z}_{p^s}$-linear GH codes of any type $(n; t_1, \dots, t_s)$, we also present some constructions of r-PD-sets of size $r+1$, but only up to $r \leq \tilde{f}_p^{t_1,\dots,t_s} \leq f_p^{t_1,\dots,t_s}$.

The computational results given in Section 7 confirm that r-PD-sets of size $r+1$, with values of r closer to the theoretical upper bound $f_p^{t_1,\dots,t_s}$, may exist for $\mathbb{Z}_{p^s}$-linear GH codes of any type. Therefore, a natural further research on this topic would be to find explicit constructions for codes $H^{t_1,\dots,t_s}$, with $\tilde{f}_p^{t_1,\dots,t_s} \leq r \leq f_p^{t_1,\dots,t_s}$.

Another direction which extends this line of research would be the generalization of these results to $\mathbb{Z}_p\mathbb{Z}_{p^2}\cdots\mathbb{Z}_{p^s}$*-linear GH codes*, which are GH codes and can be obtained from the generalized Gray map image of subgroups over mixed alphabets $\mathbb{Z}_p^{\alpha_1}\times\mathbb{Z}_{p^2}^{\alpha_2}\times\cdots\times\mathbb{Z}_{p^s}^{\alpha_s}$. In particular, $\mathbb{Z}_2\mathbb{Z}_4$-linear codes have been studied extensively, see for example [7,8], and the permutation decoding method given in [4] is also defined for these codes, since they are systematic. More generally, $\mathbb{Z}_p\mathbb{Z}_{p^2}\cdots\mathbb{Z}_{p^s}$-linear codes have been studied for example in [1,31]. The results given in [32] can be extended to $\mathbb{Z}_p\mathbb{Z}_{p^2}\cdots\mathbb{Z}_{p^s}$-linear codes, in order to obtain a systematic encoding for $\mathbb{Z}_p\mathbb{Z}_{p^2}\cdots\mathbb{Z}_{p^s}$-linear codes, which allow us to use the permutation decoding method for these codes. This gives a motivation to construct r-PD-sets for $\mathbb{Z}_p\mathbb{Z}_{p^2}\cdots\mathbb{Z}_{p^s}$-linear GH codes, which have been recently studied in [5,6] showing that they are not necessarily equivalent to the $\mathbb{Z}_{p^s}$-linear GH codes considered in this paper.

For any $\mathbb{Z}_{p^s}$-additive GH code $\mathcal{H}^{t_1,\ldots,t_s}$, we have obtained $\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$, which is a subgroup of the monomial automorphism group, $\mathrm{MAut}(\mathcal{H}^{t_1,\ldots,t_s})$. We also have that $\Phi(\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s}))\subseteq\mathrm{PAut}(H^{t_1,\ldots,t_s})$. The study of these groups, $\mathrm{MAut}(\mathcal{H}^{t_1,\ldots,t_s})$ and $\mathrm{PAut}(H^{t_1,\ldots,t_s})$, also remain as an open problem for $p\geq 3$ or $s\geq 3$. For $\mathbb{Z}_4$-linear Hadamard codes, these groups are studied in [25]. The description of $\mathrm{PAut}(H^{t_1,\ldots,t_s})$ may allow us to find r-PD-sets of size $r+1$ for $r>f_p^{t_1,\ldots,t_s}$ or r-PD-sets of larger size, up to the error-correcting capability, improving the results obtained in this paper.

Data availability

No data was used for the research described in the article.

References

[1] I. Aydogdu, I. Siap, On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes, Linear Multilinear Algebra 63 (10) (2015) 2089–2102.
[2] R.D. Barrolleta, M. Villanueva, Partial permutation decoding for binary linear and $\mathbb{Z}_4$-linear Hadamard codes, Des. Codes Cryptogr. 86 (3) (2018) 569–586.
[3] R.D. Barrolleta, M. Villanueva, Partial permutation decoding for several families of linear and $\mathbb{Z}_4$-linear codes, IEEE Trans. Inf. Theory 65 (1) (2019) 131–141.
[4] J.J. Bernal, J. Borges, C. Fernández-Córdoba, M. Villanueva, Permutation decoding of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, Des. Codes Cryptogr. 76 (2) (2015) 269–277.
[5] D.K. Bhunia, C. Fernández-Córdoba, M. Villanueva, On the linearity and classification of $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes, Des. Codes Cryptogr. 90 (4) (2022) 1037–1058.
[6] D.K. Bhunia, C. Fernández-Córdoba, C. Vela, M. Villanueva, On the equivalence of $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes, Des. Codes Cryptogr. (2023), to appear, arXiv:2203.15407.
[7] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, M. Villanueva, $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality, Des. Codes Cryptogr. 54 (2) (2010) 167–179.
[8] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, M. Villanueva, $\mathbb{Z}_2\mathbb{Z}_4$-Linear Codes, Springer Cham, Switzerland, 2022.
[9] W. Bosma, J.J. Cannon, C. Fieker, A. Steel, Handbook of Magma Functions, Version 2.27, 2022, 6145 pages, http://magma.maths.usyd.edu.au/magma/.
[10] C. Carlet, $\mathbb{Z}_{2^k}$-linear codes, IEEE Trans. Inf. Theory 44 (4) (1998) 1543–1547.
[11] B.J. Chathely, R.P. Deore, Construction of binary Hadamard codes and their s-PD sets, Cryptogr. Commun. 13 (2021) 425–438.
[12] I. Constantinescu, W. Heise, A metric for codes over residue class rings, Probl. Pereda. Inf. 33 (3) (1997) 22–28.

[13] S.T. Dougherty, C. Fernández-Córdoba, Codes over $\mathbb{Z}_{2^k}$, Gray map and self-dual codes, Adv. Math. Commun. 5 (4) (2011) 571–588.
[14] S.T. Dougherty, J. Rifà, M. Villanueva, Ranks and kernels of codes from generalized Hadamard matrices, IEEE Trans. Inf. Theory 62 (2) (2016) 687–694.
[15] C. Fernández-Córdoba, C. Vela, M. Villanueva, On $\mathbb{Z}_{2^s}$-linear Hadamard codes: kernel and partial classification, Des. Codes Cryptogr. 87 (2–3) (2019) 417–435.
[16] C. Fernández-Córdoba, C. Vela, M. Villanueva, On $\mathbb{Z}_8$-linear Hadamard codes: rank and classification, IEEE Trans. Inf. Theory 66 (2) (2018) 970–982.
[17] C. Fernández-Córdoba, A. Torres-Martín, M. Villanueva, Linear Codes over the Integer Residue Ring $\mathbb{Z}_{p^s}$. A MAGMA Package, version 1.0, Universitat Autònoma de Barcelona, 2023, http://ccsg.uab.cat.
[18] W. Fish, J.D. Key, E. Mwambeme, Partial permutation decoding for simplex codes, Adv. Math. Commun. 6 (4) (2012) 505–516.
[19] M. Greferath, S.E. Schmidt, Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code, IEEE Trans. Inf. Theory 45 (7) (1999) 2522–2524.
[20] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inf. Theory 40 (2) (1994) 301–319.
[21] J. Han, General linear group over a ring of integers of modulo k, Kyungpook Math. J. 46 (2006) 255–260.
[22] D. Jungnickel, On difference matrices, resolvable transversal designs and generalized Hadamard matrices, Math. Z. 167 (1) (1979) 49–60.
[23] D.S. Krotov, On $\mathbb{Z}_{2^k}$-dual binary codes, IEEE Trans. Inf. Theory 53 (4) (2007) 1532–1537.
[24] D.S. Krotov, $\mathbb{Z}_4$-linear Hadamard and extended perfect codes, Electron. Notes Discrete Math. 6 (2001) 107–112.
[25] D.S. Krotov, M. Villanueva, Classification of the $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes and their automorphism groups, IEEE Trans. Inf. Theory 61 (2) (2015) 887–894.
[26] F.J. MacWilliams, Permutation decoding of systematic codes, Bell Syst. Tech. J. 43 (1964) 485–505.
[27] A.A. Nechaev, The Kerdock code in a cyclic form, Discrete Math. Appl. 1 (1991) 365–384.
[28] J. Pernas, J. Pujol, M. Villanueva, Characterization of the automorphism group of quaternary linear Hadamard codes, Des. Codes Cryptogr. 70 (1–2) (2014) 105–115.
[29] K.T. Phelps, J. Rifà, M. Villanueva, On the additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes: rank and kernel, IEEE Trans. Inf. Theory 52 (1) (2006) 316–319.
[30] E. Prange, The use of information sets in decoding cyclic codes, IRE Trans. Inf. Theory 8 (5) (1962) 5–9.
[31] M. Shi, R. Wu, D.S. Krotov, On $\mathbb{Z}_p\mathbb{Z}_{p^k}$-additive codes and their duality, IEEE Trans. Inf. Theory 65 (6) (2019) 3841–3847.
[32] A. Torres-Martín, M. Villanueva, Systematic encoding and permutation decoding for $\mathbb{Z}_{p^s}$-linear codes, IEEE Trans. Inf. Theory 68 (7) (2022) 4435–4443.
[33] A. Torres-Martín, M. Villanueva, Partial permutation decoding for $\mathbb{Z}_8$-linear Hadamard codes, in: Proc. of 2022 IEEE Information Theory Workshop (ITW), 1-2 November 2022 - Virtual, 2022.
[34] Z.-X. Wan, Lectures on Finite Fields and Galois Rings, World Scientific, Singapore, 2003.