Improving Explicit Constructions of r-PD-Sets for $\mathbb{Z}_{p^s}$-Linear Generalized Hadamard Codes

Josep Rifà, *Life Senior Member, IEEE*, Adrián Torres-Martín, and Mercè Villanueva

***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, based on the existence of r-PD-sets, which are subsets of the permutation automorphism group of the code. Some constructions of r-PD-sets of minimum size $r+1$ for $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes of type $(n; t_1, \ldots, t_s)$ are known. In this paper, for these codes, we present new constructions of r-PD-sets of size $r+1$, which are suitable for all parameters $t_1, \ldots, t_s$. These allow us to obtain new r-PD-sets for values of r closer to the theoretical upper bound, improving previous known results.**

***Index Terms*— Permutation decoding, PD-set, generalized Hadamard code, $\mathbb{Z}_{p^s}$-linear code, generalized Gray map.**

I. 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 non-empty 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 $\mathbb{Z}_4$. 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 $m\mathbf{u} = \mathbf{0}$.

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 *equivalent* if there is a vector $\mathbf{a} \in \mathbb{Z}_p^n$ and a permutation of coordinates $\pi \in \mathcal{S}_n$ such that $C_2 = \{\mathbf{a} + \pi(\mathbf{c}) : \mathbf{c} \in C_1\}$. 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 non-zero 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 [14], and also used in [23] and [37]:

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

The *weight* of a vector $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{Z}_{p^s}^n$ is $\mathrm{wt}^*(\mathbf{u}) = \sum_{j=1}^n \mathrm{wt}^*(u_j) \in \mathbb{N}$; 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 [24] and [31], 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 $\mathbb{Z}_2^{2^{s-1}}$ [12], [15], [26]. 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 all the distinct elements from $\mathbb{Z}_p^{s-1}$. Note that the rows of Y_{s-1} form a basis for 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 $(\mathbb{Z}_p^{p^{s-1}}, d_H)$ [23], [37]. 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 $\Phi : \mathbb{Z}_{p^s}^n \longrightarrow \mathbb{Z}_p^{np^{s-1}}$ 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 $|\mathcal{C}| = p^{st_1}p^{(s-1)t_2} \cdots p^{t_s}$. A $\mathbb{Z}_{p^s}$-additive code can also be seen as a submodule of the $\mathbb{Z}_{p^s}$-module $\mathbb{Z}_{p^s}^n$, which is not necessarily *free*, that is, it may not have a basis such that every element in the code is uniquely expressible as a linear combination over $\mathbb{Z}_{p^s}$. The code $\mathcal{C}$ is free if and only if $t_2 = \cdots = t_s = 0$. Nonetheless, even when $\mathcal{C}$ is not free,

Manuscript received 19 March 2024; revised 25 June 2024; accepted 7 August 2024. Date of publication 22 August 2024; date of current version 22 November 2024. This work was supported in part by Spanish Ministerio de Economía, Industria y Competitividad (MINECO) under Grant PID2022-137924NB-I00 (AEI/10.13039/501100011033) and in part by the Catalan Agència de Gestió d'Ajuts Universitaris i de Recerca (AGAUR) under Grant 2021 SGR 00643. An earlier version of this paper was presented in part at the 2023 Rijeka Conference on Combinatorial Objects and Their Applications. *(Corresponding author: Mercè Villanueva.)*

The authors are with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193 Barcelona, Spain (e-mail: merce.villanueva@uab.cat).

Communicated by Y. Miao, Associate Editor for Coding and Decoding.
Digital Object Identifier 10.1109/TIT.2024.3448230

there exists a generator matrix 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 [25]. 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 [16]. Note that a GH code over $\mathbb{Z}_p$ of length N has pN codewords and minimum distance $(p-1)N/p$. Moreover, it is not necessarily linear 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*. The $\mathbb{Z}_4$-linear Hadamard codes of length 2^t have been studied and classified in [27] and [33], and their automorphism groups have been characterized in [28] and [32]. For $s > 2$, $\mathbb{Z}_{2^s}$-linear Hadamard codes were first introduced in [26]. A full classification of $\mathbb{Z}_8$-linear Hadamard codes is provided in [20].For $s > 3$, a partial classification and bounds on the number of non-equivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t can be found in [18] and [19]. More generally, for any $s \geq 2$ and p prime, $\mathbb{Z}_{p^s}$-linear GH codes are studied and partially classified in [5] and [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 that are linear [6]; and for $p = 2$, only the codes of type $(n; 1, 0, \ldots, 0, t_s)$ or $(n; 1, 0, \ldots, 0, 1, t_s)$ are linear [18].

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 $\{1, \ldots, n\} \backslash I$ is called a *redundancy set*.

Permutation decoding is a technique, introduced by Prange [34] and developed by MacWilliams [30] 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 encoding. This can be generalized easily to systematic nonlinear codes over $\mathbb{Z}_p$ [38]. Then, since any $\mathbb{Z}_{p^s}$-linear code is systematic, as shown in [38] 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 a suitable permutation in S, for each received vector. In general, to determine the structure of $\mathrm{PAut}(C)$ can be very complex, making the search for r-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], [13], [22], [39]. 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 generalization of these results for (nonlinear) $\mathbb{Z}_{p^s}$-linear GH codes, with $s \geq 2$ and p prime, is given in [39]. A similar result for Hadamard codes over the field $\mathbb{F}_4$ is presented in [13]. In this paper, we improve the results given in [39] for $\mathbb{Z}_{p^s}$-linear GH codes with $s \geq 2$ and p prime.

The paper is organized as follows. In Section II, we recall the construction of $\mathbb{Z}_{p^s}$-additive GH codes, the description of an information set for the corresponding $\mathbb{Z}_{p^s}$-linear GH codes, some results related to the permutation automorphism group for these codes, a criterion to find r-PD-sets of size $r + 1$ for these codes, and some previous known results given in [39]. In Section III, new explicit constructions of r-PD-sets of size $r + 1$, for values of r closer to a known upper bound, are described. In Section IV, we compare the obtained values of r with the theoretical upper bound and also with the computational results, given in [39]. Finally, in Section V, some conclusions and further research on this topic are included.

II. Preliminaries

Let t_1, t_2, …, t_s be non-negative 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 $\mathbf{z}^T$, $\mathbf{z} \in \{1\} \times \mathbb{Z}_{p^s}^{t_1-1} \times (p\mathbb{Z}_{p^s})^{t_2} \times \cdots \times (p^{s-1}\mathbb{Z}_{p^s})^{t_s}$.

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. 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

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

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 $\mathcal{G}^{t'_1,\ldots,t'_s}$.

In this paper, we assume that the matrices $\mathcal{G}^{t_1,\ldots,t_s}$ are constructed recursively starting from $\mathcal{G}^{1,0,\ldots,0}$ in the following way. First, we obtain $\mathcal{G}^{t_1,0,\ldots,0}$ by adding $t_1 - 1$ rows of order

p^s; then $\mathcal{G}^{t_1,t_2,0,\ldots,0}$ is generated by adding t_2 rows of order p^{s-1}; and so on, until $\mathcal{G}^{t_1,\ldots,t_s}$ is reached by adding t_s rows of order p.

Example 1: For $p=3$ and $s=3$, we have the following matrices over $\mathbb{Z}_{27}$:

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

$$\mathcal{G}^{2,0,0}=\begin{pmatrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&\cdots&1&1\\0&1&2&3&4&5&6&7&8&9&10&11&12&13&14&15&16&\cdots&25&26\end{pmatrix},$$

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

We denote by $\mathcal{H}^{t_1,\ldots,t_s}$ the $\mathbb{Z}_{p^s}$-additive code of type $(n;t_1,\ldots,t_s)$ generated by $\mathcal{G}^{t_1,\ldots,t_s}$, where $t_1,\ldots,t_s$ are non-negative 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 $H^{t_1,\ldots,t_s}=\Phi(\mathcal{H}^{t_1,\ldots,t_s})$ denote the corresponding $\mathbb{Z}_{p^s}$-linear code, which is a GH code of length p^t [6]. Thus, we say that $\mathcal{H}^{t_1,\ldots,t_s}$ is a $\mathbb{Z}_{p^s}$-additive GH code, and $H^{t_1,\ldots,t_s}$ a $\mathbb{Z}_{p^s}$-linear GH code of type $(n;t_1,\ldots,t_s)$.

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

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

where $a_1\in\mathbb{Z}_{p^s}^{t_1-1}$, $A_{1,1}\in\mathrm{GL}(t_1-1,\mathbb{Z}_{p^s})$, $a_i\in\mathbb{Z}_{p^s}^{t_i}$, $A_{i,i}\in\mathrm{GL}(t_i,\mathbb{Z}_{p^s})$, for $i\in\{2,\ldots,s\}$, and $A_{i,j}$ are matrices over $\mathbb{Z}_{p^s}$, for $i,j\in\{1,\ldots,s\}$. The set $\mathcal{L}$ is a subgroup of $\mathrm{GL}(t_1+\cdots+t_s,\mathbb{Z}_{p^s})$ [39]. Let ζ_i be the map from $\mathbb{Z}_{p^s}$ to $\mathbb{Z}_{p^s}$ defined as $\zeta_i(a)=a \pmod{p^i}$, $i\in\{1,\ldots,s-1\}$. 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, for any matrix $\mathcal{M}\in\mathcal{L}$ as in (4), by $\pi(\mathcal{M})=$

$$\begin{pmatrix}1&a_1&pa_2&\cdots&p^{s-1}a_s\\0&A_{1,1}&pA_{1,2}&\cdots&p^{s-1}A_{1,s}\\0&\zeta_{s-1}(A_{2,1})&\zeta_{s-1}(A_{2,2})&\cdots&\zeta_{s-1}(p^{s-2}A_{2,s})\\\vdots&\vdots&\vdots&\ddots&\vdots\\0&\zeta_2(A_{s-1,1})&\zeta_2(A_{s-1,2})&\cdots&\zeta_2(pA_{s-1,s})\\0&\zeta_1(A_{s,1})&\zeta_1(A_{s,2})&\cdots&\zeta_1(A_{s,s})\end{pmatrix},\tag{5}$$

Let $\pi(\mathcal{L})=\{\pi(\mathcal{M}):\mathcal{M}\in\mathcal{L}\}\subseteq\mathrm{GL}(t_1+\cdots+t_s,\mathbb{Z}_{p^s})$. Since $\mathcal{L}$ is a subgroup of $\mathrm{GL}(t_1+\cdots+t_s,\mathbb{Z}_{p^s})$, 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 generalizing the proof of Theorem 2 in [28], it is possible to show that $\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$ is isomorphic to $\pi(\mathcal{L})$ [39].

Now, we give an additive information set for the $\mathbb{Z}_{p^s}$-additive GH code $\mathcal{H}^{t_1,\ldots,t_s}$, and an information set for the corresponding $\mathbb{Z}_{p^s}$-linear GH code $H^{t_1,\ldots,t_s}$. An ordered set $\mathcal{I}=\{i_1,\ldots,i_{t_1+\cdots+t_s}\}\subseteq\{1,\ldots,n\}$ 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 $(n;t_1,\ldots,t_s)$ 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 $k\in\{1,\ldots,s\}$, $|\mathcal{C}_{\{i_1,\ldots,i_{t_1+\cdots+t_k}\}}|=(p^s)^{t_1}(p^{s-1})^{t_2}\cdots(p^{s-k+1})^{t_k}$, then it can be seen that the set $\Phi(\mathcal{I})$, defined as

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

where

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

is an information set for $C=\Phi(\mathcal{C})$ [38]. 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 2: It is easy to see, from the matrix $\mathcal{G}^{1,1,1}$ given in Example 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 $\mathcal{H}^{t_1,\ldots,t_s}$. The following result provides a recursive and simple form to obtain such a set.

Proposition 1 ([39]): Let $\mathcal{I}$ be an additive information set for the $\mathbb{Z}_{p^s}$-additive GH code $\mathcal{H}^{t_1,\ldots,t_s}$ of type $(n;t_1,\ldots,t_s)$. Then $\mathcal{I}\cup\{n+1\}$ is an additive information set for each of the codes $\mathcal{H}^{t_1+1,t_2,\ldots,t_s}$, $\mathcal{H}^{t_1,t_2+1,\ldots,t_s}$, $\ldots$, $\mathcal{H}^{t_1,t_2,\ldots,t_s+1}$, obtained from $\mathcal{H}^{t_1,t_2,\ldots,t_s}$ by applying (3).

Let $\mathcal{I}$ be an additive information set for $\mathcal{H}^{t_1,\ldots,t_s}$ of type $(n;t_1,\ldots,t_s)$. Let $\mathcal{H}_k=\mathcal{H}^{t'_1,t'_2,\ldots,t'_s}$, $k\in\{1,\ldots,s\}$, 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 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 $k\in\{1,\ldots,s\}$. In particular,

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

is an information set for H_k.

We can label the i-th coordinate position of a $\mathbb{Z}_{p^s}$-additive GH code $\mathcal{H}^{t_1,\ldots,t_s}$, with the ith column of its generator matrix $\mathcal{G}^{t_1,\ldots,t_s}$. Note that, by construction, all columns in $\mathcal{G}^{t_1,\ldots,t_s}$ 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 $\mathcal{H}^{t_1,\ldots,t_s}$ 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 i-th position, which is equal to 1. Then, by Proposition 1, we have that the set $\mathcal{I}_{t_1,\ldots,t_s}$ equal to

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

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

Example 3: 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 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 $\mathcal{G}^{2,0,1}$ generating 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 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, in terms of vectors representing these positions, we have

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

Finally, we have that

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

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 $p^{s-1}n$. Now, we define a new map, called also Φ, that sends permutations on a set of n elements to permutations on a set of $p^{s-1}n$ elements. This is a generalization of the map defined in [2] for $\mathbb{Z}_4$. It can be deduced from the context whether Φ refers to the generalized Gray map, from $\mathbb{Z}_{p^s}^n$ to $\mathbb{Z}_p^{np^{s-1}}$, or this new map $\Phi:\mathrm{Sym}(n)\longrightarrow\mathrm{Sym}(p^{s-1}n)$, defined as

$$\Phi(\tau)(i)=p^{s-1}\tau\left(\frac{i+\chi(i)}{p^{s-1}}\right)-\chi(i),\tag{6}$$

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 $\Phi(\mathcal{S})\subseteq\mathrm{PAut}(\Phi(\mathcal{C}))\subseteq\mathrm{Sym}(p^{s-1}n)$. Moreover, the map $\Phi:\mathrm{Sym}(n)\longrightarrow\mathrm{Sym}(p^{s-1}n)$ is a group monomorphism [39].

Recall that we can identify $\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$ with the group $\pi(\mathcal{L})$ [39]. Recall also that we can label the i-th coordinate position of $\mathcal{H}^{t_1,\ldots,t_s}$ with the i-th column w_i of the generator matrix $\mathcal{G}^{t_1,\ldots,t_s}$ constructed via (3), $i\in\{1,\ldots,n\}$. Any matrix $\mathcal{M}\in\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$ sends columns of $\mathcal{G}^{t_1,\ldots,t_s}$ to other columns of $\mathcal{G}^{t_1,\ldots,t_s}$. Therefore, $\mathcal{M}$ can be seen as a permutation of coordinate positions $\tau\in\mathrm{Sym}(n)$, such that for all $i\in\{1,\ldots,n\}$

$$\tau(i)=j\iff w_i\mathcal{M}=w_j,\quad j\in\{1,\ldots,n\}.\tag{7}$$

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

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

Theorem 1 ([39]): Let $\mathcal{H}^{t_1,\ldots,t_s}$ be the $\mathbb{Z}_{p^s}$-additive GH code of type $(n;t_1,\ldots,t_s)$. Let $\mathcal{P}_r=\{\mathcal{M}_i:0\le i\le r\}$ be a set of $r+1$ matrices in $\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$. Then, $\Phi(\mathcal{P}_r)$ is an r-PD-set of size $r+1$ for $H^{t_1,\ldots,t_s}$ with information set $\Phi(\mathcal{I}_{t_1,\ldots,t_s})$ if and only if no two matrices $(\mathcal{M}_i^{-1})^*$ and $(\mathcal{M}_j^{-1})^*$ have a row in common, for $i,j\in\{0,\ldots,r\}$ and $i\neq j$.

Corollary 1 ([39]): Let $\mathcal{P}_r$ be a set of $r+1$ matrices in $\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$. If $\Phi(\mathcal{P}_r)$ is an r-PD-set of size $r+1$ for $H^{t_1,\ldots,t_s}$, then any ordering of elements in $\Phi(\mathcal{P}_r)$ provides nested k-PD-sets for $k\in\{1,\ldots,r\}$.

Corollary 2 ([39]): Let $\mathcal{P}_r$ be a set of $r+1$ matrices in $\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$. If $\Phi(\mathcal{P}_r)$ is an r-PD-set of size $r+1$ for $H^{t_1,\ldots,t_s}$, then $r\le f_p^{t_1,\ldots,t_s}$, where

$$f_p^{t_1,\ldots,t_s}=\left\lfloor\frac{p^{st_1+(s-1)t_2+\cdots+t_s-s}-t_1-t_2-\cdots-t_s}{t_1+t_2+\cdots+t_s}\right\rfloor.\tag{8}$$

By using Theorem 1, in [39], some constructions of r-PD-sets of minimum size $r+1$ for some infinite families of $\mathbb{Z}_{p^s}$-linear GH codes of type $(n;t_1,\ldots,t_s)$ are presented. Specifically, first, an explicit construction of r-PD-sets of size $r+1$ is given for the $\mathbb{Z}_{p^s}$-linear GH codes $H^{t_1,0,\ldots,0}$, with $t_1\ge 2$, for any r up to the upper bound given in (8), that is, for any $r\le f_p^{t_1,0,\ldots,0}$. Then, using a similar idea, it is also given another explicit construction for the $\mathbb{Z}_{p^s}$-linear GH codes $H_i=H^{1,0,\ldots,0,t_i,0,\ldots,0}$, with $t_i\ge 1$ and $i\in\{2,\ldots,s\}$, for any $r\le f_p^{1,0,\ldots,0,t_i,0,\ldots,0}$.

In [39], it is also shown that, given an r-PD-set of size ℓ for a $\mathbb{Z}_{p^s}$-linear GH code $H^{t_1,\ldots,t_s}$, we can easily obtain an r-PD-set of size ℓ for the $\mathbb{Z}_{p^s}$-linear GH code $H^{t_1+i_1,\ldots,t_s+i_s}$, for all $i_1,\ldots,i_s\ge 0$. In particular, this is useful to obtain r-PD-sets for any code $H^{t_1,\ldots,t_s}$, including those of type different to $(n;t_1,0,\ldots,0)$ or $(n;1,0,\ldots,0,t_i,0,\ldots,0)$. Indeed, we can use the explicit construction given in [39, Theorem 5.1] for $H_1=H^{t_1,0,\ldots,0}$, or the one given in [39, Corollary 5.1] for $H_i=H^{1,0,\ldots,0,t_i,0,\ldots,0}$, with $i\in\{2,\ldots,s\}$, and then extend the obtained r-PD-set up to achieve an r-PD-set for $H^{t_1,\ldots,t_s}$ using the recursive construction given in [39, Corollary 6.1]. In order to maximize the value of r, we select the construction that gives its maximum value $r=\tilde{f}_p^{t_1,\ldots,t_s}$, where

$$\begin{aligned}\tilde{f}_p^{t_1,\ldots,t_s}&=\max\{f_p^{t_1,0,\ldots,0},f_p^{1,t_2,0,\ldots,0},\ldots,f_p^{1,0,\ldots,0,t_s}\}\\ &\le f_p^{t_1,\ldots,t_s}.\end{aligned}\tag{9}$$

We also define a parameter, $h_p^{t_1,\ldots,t_s}$, to indicate which construction is selected. If $\tilde{f}_p^{t_1,\ldots,t_s} = f_p^{t_1,0,\ldots,0}$, then $h_p^{t_1,\ldots,t_s} = 1$. Otherwise, $h_p^{t_1,\ldots,t_s} = i \in \{2,\ldots,s\}$, where i is the minimum index such that $\tilde{f}_p^{t_1,\ldots,t_s} = f_p^{1,0,\ldots,0,t_i,0,\ldots,0}$.

III. New r-PD-Sets for Non-Free Codes

In this section, we present new constructions of r-PD-sets of size $r+1$, which are also suitable for any non-free $\mathbb{Z}_{p^s}$-linear GH code $H^{t_1,\ldots,t_s}$, that is, with $t_2+\cdots+t_s>0$. Recall that for free $\mathbb{Z}_{p^s}$-linear GH codes, r-PD-sets of size $r+1$ up to the upper bound were given in [39]. In Section IV, we show that depending on the type of the code, these new constructions allow us to improve the previous results, that is, to obtain r-PD-sets for values of r larger than $\tilde{f}_p^{t_1,\ldots,t_s}$ and closer to the theoretical upper bound $f_p^{t_1,\ldots,t_s}$. In order to present the new constructions (Theorem 2 and Corollary 3), first we need to introduce the elements of a specific Galois ring with a structure that will be useful in the proof of Theorem 2.

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 $\mathbb{Z}_{p^s}[x]$ such that $h(x) \mid (x^n-1)$ in $\mathbb{Z}_{p^s}[x]$ and $\bar{h}(x) = f(x)$. This unique polynomial $h(x)$ 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 [40]. 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 $\mathcal{T} = \{0,1,\alpha,\alpha^2,\ldots,\alpha^{\ell-1}\}$ is called the *Teichmüller set*.

The *p-adic representation* of an element $y \in \mathcal{R}$ is given by

$$y = y_0 + py_1 + p^2y_2 + \cdots + p^{s-1}y_{s-1},$$

where $y_0,\ldots,y_{s-1} \in \mathcal{T}$. Consider the sequence of elements $r_1,\ldots,r_{p^{s(t_1-1)}} \in \mathcal{R}$ lexicographically ordered. That is, $a_0 + pa_1 + \cdots + p^{s-1}a_{s-1} < b_0 + pb_1 + \cdots + p^{s-1}b_{s-1}$ if $a_j < b_j$ for the last j where a_j and b_j differ. From now on, along the paper, we refer to this order as *lexicographical order*.

We structure the ordered elements of $\mathcal{R}$ in s different tables: $A, A_p, \ldots, A_{p^{s-1}}$. First, we divide all elements in blocks of p^{t_1-1} consecutive elements, and then we place each block as a column of a table, denoted by A. Note that any two elements r_i, r_j from the same row of A satisfy that $i-j$ is a multiple of p^{t_1-1}, which implies that $r_i - r_j \in (p) \subset \mathcal{R}$. In order to use Lemma 1 in the construction of the r-PD-sets, we take sequences of t_1 consecutive elements in $\mathcal{R}$. Let d_p and h_p be the quotient and the remainder of the division of p^{t_1-1} by t_1, respectively. The last h_p rows of this table are discarded, resulting in a table of t_1d_p rows and $p^{(s-1)(t_1-1)}$ columns, denoted by A_p. Table A_{p^k}, for $k \in \{2,\ldots,s-1\}$, is constructed by taking as the i-th column the vertical concatenation of consecutive columns in $A_{p^{k-1}}$, from the $(p^{t_1-1}(i-1)+1)$-th column up to the $(p^{t_1-1}i)$-th. This process results in a table A_{p^k} with $t_1d_{p^{k-1}}p^{t_1-1} = t_1d_{p^k}$ rows and $p^{(s-k+1)(t_1-1)}/p^{t_1-1} = p^{(s-k)(t_1-1)}$ columns, where $d_{p^k} = p^{t_1-1}d_{p^{k-1}} = p^{(k-1)(t_1-1)}d_p$. Note that any two elements r_i, r_j from the same row of A_{p^k} satisfy that $i-j$ is a multiple of $p^{k(t_1-1)}$, which implies that $r_i - r_j \in (p^k) \subset \mathcal{R}$.

Example 4: For $t_1=3$, $s=3$, and $p=2$, we have that $|\mathcal{R}| = 8^{t_1-1} = 64$, $d_2=1$, and $d_4 = 2^{t_1-1}d_2 = 4$. Tables A, A_2 and A_4 are of size $2^{t_1-1}\times 4^{t_1-1} = 4\times 16$, $t_1d_2\times 4^{t_1-1} = 3\times 16$, and $t_1d_4\times 2^{t_1-1} = 12\times 4$, respectively. Below appears a representation of Tables A, A_2, and A_4, where instead of the elements $r_i \in \mathcal{R}$, only the corresponding index i is shown:

$$A: \begin{array}{cccc} 1 & 5 & \cdots & 61 \\ 2 & 6 & \cdots & 62 \\ 3 & 7 & \cdots & 63 \\ \hline 4 & 8 & \cdots & 64 \end{array}, \quad A_2: \begin{array}{cccc} 1 & 5 & \cdots & 61 \\ 2 & 6 & \cdots & 62 \\ 3 & 7 & \cdots & 63 \end{array}, \quad A_4: \begin{array}{cccc} 1 & 17 & 33 & 49 \\ 2 & 18 & 34 & 50 \\ 3 & 19 & 35 & 51 \\ \hline 5 & 21 & 37 & 53 \\ \cdots & \cdots & \cdots & \cdots \\ \hline 15 & 31 & 47 & 63 \end{array}.$$

Lemma 1: Let $t_1 \geq 2$. Let $r_{i_1},\ldots,r_{i_{t_1}}$ be a sequence of elements in $\mathcal{R}$. If they are consecutive in the lexicographical order, then $\{r_{i_2}-r_{i_1},\ldots,r_{i_{t_1}}-r_{i_1}\}$ is a set of linearly independent vectors in their additive representation. Moreover, any permutation of the indices $i_1,\ldots,i_{t_1}$ preserves the linear independence of the set of vectors.

Proof: Theorem 5.1 in [39] implies that any matrix

$$\mathcal{N}_i^* = \begin{pmatrix} 1 & r_{t_1i+1} \\ 1 & r_{t_1i+2} \\ \vdots & \vdots \\ 1 & r_{t_1(i+1)} \end{pmatrix}$$

satisfies that $\mathcal{N}_i^{-1} \in \mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$, where

$$\mathcal{N}_i = \begin{pmatrix} 1 & r_{t_1i+1} \\ 0 & r_{t_1i+2}-r_{t_1i+1} \\ \vdots & \vdots \\ 0 & r_{t_1(i+1)}-r_{t_1i+1} \end{pmatrix}.$$

In particular, $\mathcal{N}_i$ is invertible.

Therefore, $\{r_{t_1i+2}-r_{t_1i+1},\ldots,r_{t_1(i+1)}-r_{t_1i+1}\}$ is a set of linearly independent vectors. The same argument applies for any sequence of t_1 consecutive elements in $\mathcal{R}$.

Assume $\{r_{i_2}-r_{i_1},\ldots,r_{i_{t_1}}-r_{i_1}\}$ is a set of linearly independent vectors. Any permutation of the indices $i_2,\ldots,i_{t_1}$ preserves the set of vectors. We just need to consider the transposition of one of these indices with i_1. Without loss of generality, we choose index i_2 and consider the set $\{r_{i_1}-r_{i_2}, r_{i_3}-r_{i_2}\ldots,r_{i_{t_1}}-r_{i_2}\}$. If these are not linearly independent vectors, then

$$\lambda_1(r_{i_1}-r_{i_2}) + \lambda_3(r_{i_3}-r_{i_2}) + \cdots + \lambda_{t_1}(r_{i_{t_1}}-r_{i_2}) = 0$$

for certain $\lambda_1,\lambda_3,\ldots,\lambda_{t_1} \in \mathbb{Z}_{p^s}$, with some of them being non-zero. This equation can be rewritten, as

$$\begin{aligned} -\lambda_1(r_{i_2}-r_{i_1}) + \lambda_3(r_{i_3}-r_{i_1}) + \cdots + \lambda_{t_1}(r_{i_{t_1}}-r_{i_1}) \\ - \lambda_3(r_{i_2}-r_{i_1}) - \cdots - \lambda_{t_1}(r_{i_2}-r_{i_1}) = 0, \end{aligned}$$

and so,

$(-\lambda_1-\lambda_3-\cdots-\lambda_{t_1})(r_{i_2}-r_{i_1})+\lambda_3(r_{i_3}-r_{i_1})+\cdots+\lambda_{t_1}(r_{i_{t_1}}-r_{i_1})=0$, which contradicts the initial assumption about the set $\{r_{i_2}-r_{i_1},\ldots,r_{i_{t_1}}-r_{i_1}\}$ being a set of linearly independent vectors. □

Next theorem gives an explicit construction of r-PD-sets of size $r+1$ for any $\mathbb{Z}_{p^s}$-linear GH code $H^{t_1,\ldots,t_s}$ with $t_1\geq 2$, which allows us to improve previous known results, as shown in Tables II and III.

Theorem 2: Let $H^{t_1,\ldots,t_s}$ be a $\mathbb{Z}_{p^s}$-linear GH code of type $(n;t_1,\ldots,t_s)$ with $t_1\geq 2$ and $t_2+\cdots+t_s>0$. There exist r-PD-sets of size $r+1$ for $H^{t_1,\ldots,t_s}$, with respect to the information set $\Phi(\mathcal{I}_{t_1,\ldots,t_s})$, for every

$$r\leq g_p^{t_1,\ldots,t_s}=p^{(s-1)t_2+(s-2)t_3+\cdots+t_s}\alpha-1, \tag{10}$$

where $\alpha=\tau d_{p^{s-1}}$ is the maximum value multiple of $d_{p^{s-1}}=p^{(s-2)(t_1-1)}d_p$, with $d_p=\lfloor\frac{p^{t_1-1}}{t_1}\rfloor$, such that the following condition is satisfied for each $k\in\{1,\ldots,s-1\}$:

$$\alpha\leq t_1 d_{p^{s-k}}\left\lfloor\frac{p^{(k-1)(t_1-1)}(p^{t_1-1}-\tau)}{t_{s-k+1}+\cdots+t_s}\right\rfloor \tag{11}$$

when $t_{s-k+1}+\cdots+t_s>0$.

Proof: Let $\mathcal{R}=\mathrm{GR}(p^{s(t_1-1)})$ be the Galois ring of degree t_1-1 over $\mathbb{Z}_{p^s}$ and consider the sequence of elements $r_1,\ldots,r_{p^{s(t_1-1)}}$ of $\mathcal{R}$, following the lexicographical order. In order to use the result given by Theorem 1, we need to produce a set of matrices $\{\mathcal{M}_0^*,\ldots,\mathcal{M}_r^*\}$, such that $\mathcal{M}_i^{-1}\in\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$, or equivalently $\mathcal{M}_i\in\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$, for $0\leq i\leq r$, and such that no two different matrices $(\mathcal{M}_i^{-1})^*,(\mathcal{M}_j^{-1})^*$, with $0\leq i,j\leq r$ and $i\neq j$, have a row in common.

Consider the matrix $\mathcal{M}_i^*$, given in (12), where

$$r_{i_1},\ldots,r_{i_{t_1+\cdots+t_s}}\in\mathcal{R}.$$

Then $\mathcal{M}_i$ is defined as in (13), where $\chi_k(a)=p^k a$, for $1\leq k\leq s-1$ and every $a\in\mathbb{Z}_{p^s}$.

$$\mathcal{M}_i^*=\left(\begin{array}{c|c|c|c|c|c}
1 & r_{i_1} & \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0}\\ \hline
\begin{array}{c}1\\ \vdots\\ 1\end{array} & \begin{array}{c}r_{i_2}\\ \vdots\\ r_{i_{t_1}}\end{array} & \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0}\\ \hline
\begin{array}{c}1\\ \vdots\\ 1\end{array} & \begin{array}{c}r_{i_{t_1+1}}\\ \vdots\\ r_{i_{t_1+t_2}}\end{array} & pI_{t_2} & \mathbf{0} & \ldots & \mathbf{0}\\ \hline
\begin{array}{c}1\\ \vdots\\ 1\end{array} & \begin{array}{c}r_{i_{t_1+t_2+1}}\\ \vdots\\ r_{i_{t_1+t_2+t_3}}\end{array} & \mathbf{0} & p^2I_{t_3} & \ldots & \mathbf{0}\\ \hline
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots\\ \hline
\begin{array}{c}1\\ \vdots\\ 1\end{array} & \begin{array}{c}r_{i_{t_1+\cdots+t_{s-1}+1}}\\ \vdots\\ r_{i_{t_1+\cdots+t_{s-1}+t_s}}\end{array} & \mathbf{0} & \mathbf{0} & \ldots & p^{s-1}I_{t_s}
\end{array}\right) \tag{12}$$

$$\mathcal{M}_i=\left(\begin{array}{c|c|c|c|c|c}
1 & r_{i_1} & \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0}\\ \hline
\begin{array}{c}0\\ \vdots\\ 0\end{array} & \begin{array}{c}r_{i_2}-r_{i_1}\\ \vdots\\ r_{i_{t_1}}-r_{i_1}\end{array} & \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0}\\ \hline
\begin{array}{c}0\\ \vdots\\ 0\end{array} & \begin{array}{c}\chi_1^{-1}(r_{i_{t_1+1}}-r_{i_1})\\ \vdots\\ \chi_1^{-1}(r_{i_{t_1+t_2}}-r_{i_1})\end{array} & I_{t_2} & \mathbf{0} & \ldots & \mathbf{0}\\ \hline
\begin{array}{c}0\\ \vdots\\ 0\end{array} & \begin{array}{c}\chi_2^{-1}(r_{i_{t_1+t_2+1}}-r_{i_1})\\ \vdots\\ \chi_2^{-1}(r_{i_{t_1+t_2+t_3}}-r_{i_1})\end{array} & \mathbf{0} & I_{t_3} & \ldots & \mathbf{0}\\ \hline
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots\\ \hline
\begin{array}{c}0\\ \vdots\\ 0\end{array} & \begin{array}{c}\chi_{s-1}^{-1}(r_{i_{t_1+\cdots+t_{s-1}+1}}-r_{i_1})\\ \vdots\\ \chi_{s-1}^{-1}(r_{i_{t_1+\cdots+t_{s-1}+t_s}}-r_{i_1})\end{array} & \mathbf{0} & \mathbf{0} & \ldots & I_{t_s}
\end{array}\right) \tag{13}$$

Thus, the construction of $\mathcal{M}_i$ is only well-defined if $r_{i_{t_1+\cdots+t_k+j}}-r_{i_1}\in(p^k)$ for $1\leq j\leq t_{k+1}$. Moreover, in order to ensure that $\mathcal{M}_i\in\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$, the vectors $r_{i_2}-r_{i_1},\ldots,r_{i_{t_1}}-r_{i_1}$ must be linearly independent. By Lemma 1, this is fulfilled if $r_{i_1},\ldots,r_{i_{t_1}}$ are consecutive, following the lexicographical order. Therefore, the proof is reduced to determine the indices $i_1,\ldots,i_{t_1+\cdots+t_s}\in\{1,\ldots,p^{s(t_1-1)}\}$ for each matrix $\mathcal{M}_i$, $0\leq i\leq r$, such that the following conditions are satisfied:

(i) the elements $r_{i_1},\ldots,r_{i_{t_1}}$ must be consecutive in the lexicographically ordered sequence $r_1,\ldots,r_{p^{s(t_1-1)}}$,
(ii) $r_{i_{t_1+\cdots+t_h+j}}-r_{i_1}\in(p^h)$ for $1\leq j\leq t_{h+1}$, $1\leq h\leq s-1$, and
(iii) all indices $i_1,\ldots,i_{t_1+\cdots+t_s}$ must be distinct.

We begin by constructing the first t_1 rows of matrices $\mathcal{M}_i^*$, for $i\in\{0,\ldots\alpha-1\}$. Since α is a multiple of $d_{p^{s-1}}$, we have $\alpha=\tau d_{p^{s-1}}$. First, we split the table $A_{p^{s-1}}$ in two subtables: $A^{(1)}_{p^{s-1}}$, containing the first τ columns, and $A^{(2)}_{p^{s-1}}$, containing the last $p^{t_1-1}-\tau$ columns. Then, we take the sequence of elements, beginning with the first element in the first column of $A^{(1)}_{p^{s-1}}$ and finishing with the last element in the column τ of $A^{(1)}_{p^{s-1}}$. We have a sequence of $t_1 d_{p^{s-1}}\tau=t_1\alpha$ elements. The first t_1 elements of this sequence are placed in the first t_1 rows of matrix $\mathcal{M}_0^*$, the next t_1 elements are placed in the first t_1 rows of matrix $\mathcal{M}_1^*$, and so on, until matrix $\mathcal{M}_{\alpha-1}^*$. This ensures that condition (i) is satisfied for every $0\leq i\leq\alpha-1$. The elements of $A^{(2)}_{p^{s-1}}$ will be used later to fill the last $t_2+\cdots+t_s$ rows of matrices $\mathcal{M}_i^*$, for $i\in\{0,\ldots\alpha-1\}$.

Since $\alpha=\tau d_{p^{s-1}}=\tau p^{t_1-1}d_{p^{s-2}}=\tau p^{2(t_1-1)}d_{p^{s-3}}=\cdots=p^{(s-2)(t_1-1)}d_p$, the index $i\in\{0,\ldots,\alpha-1\}$ can be decomposed, in a unique way, as

$$i=b_1 d_{p^{s-1}}+b_2 d_{p^{s-2}}+\cdots+b_{s-1}d_p+b_s, \tag{14}$$

where $b_1\in\{0,\ldots,\tau-1\}$, $b_2,\ldots,b_{s-1}\in\{0,\ldots,p^{t_1-1}-1\}$, and $b_s\in\{0,\ldots,d_p-1\}$. Similarly, the index $j\in\{1,\ldots,t_1 d_{p^{s-1}}\}$ corresponding to the j-th row of $A^{(1)}_{p^{s-1}}$ can

be decomposed in a unique way as

$$j = a_1 t_1 d_{p^{s-2}} + a_2 t_1 d_{p^{s-3}} + \ldots + a_{s-2} t_1 d_p + a_{s-1} t_1 + a_s + 1, \tag{15}$$

where $a_1, \ldots, a_{s-2} \in \{0, \ldots, p^{t_1-1}-1\}$, $a_{s-1} \in \{0, \ldots, d_p - 1\}$, and $a_s \in \{0, \ldots, t_1 - 1\}$.

Any of the t_1 elements $r_{i_1}, \ldots, r_{i_{t_1}}$ can act as the first row of $\mathcal{M}_i^*$, $i \in \{0, \ldots, \alpha-1\}$, by applying a permutation of rows, by Lemma 1. We refer to the element selected to be in the first row as the *leader* of $\mathcal{M}_i^*$. The leader plays an important role in each matrix, since it determines which elements $r_{i_j} \in \mathcal{R}$, $j \in \{t_1+1, \ldots, t_1 + \cdots + t_s\}$, satisfy condition (ii). We take as leader of $\mathcal{M}_i^*$, the element in the x-th position, r_{i_x}, where

$$x = \left[(b_1 + b_2\tau + b_3\tau p^{t_1-1} + \ldots + b_s \tau p^{(s-2)(t_1-1)}) \pmod{t_1} \right] + 1 \tag{16}$$

and i is as in (14). Note that the leader r_{i_x} of $\mathcal{M}_i^*$ belongs to the j-th row of $A^{(1)}_{p^{s-1}}$, where $j = \left[i t_1 \pmod{t_1 d_{p^{s-1}}} \right] + x$. Hence,

$$\begin{aligned} j = {} & b_2 t_1 d_{p^{s-2}} + b_3 t_1 d_{p^{s-3}} + \cdots + b_{s-1} t_1 d_p + b_s t_1 + \\ & \left[(b_1 + b_2\tau + b_3\tau p^{t_1-1} + \ldots + b_s \tau p^{(s-2)(t_1-1)}) (\mathrm{mod}\ t_1) \right] + 1. \end{aligned} \tag{17}$$

Consider two matrices $\mathcal{M}_i^*$ and $\mathcal{M}_{i'}^*$, where

$$\begin{aligned} i &= b_1 d_{p^{s-1}} + b_2 d_{p^{s-2}} + \cdots + b_{s-1} d_p + b_s \quad \text{and} \\ i' &= b'_1 d_{p^{s-1}} + b'_2 d_{p^{s-2}} + \cdots + b'_{s-1} d_p + b'_s, \end{aligned}$$

and their respective leaders $r_{i_x}, r_{i'_{x'}}$, where $x = \left[(b_1 + b_2\tau + b_3\tau p^{t_1-1} + \ldots + b_s \tau p^{(s-2)(t_1-1)}) \pmod{t_1} \right] + 1$ and $x' = [(b'_1 + b'_2\tau + b'_3\tau p^{t_1-1} + \ldots + b'_s \tau p^{(s-2)(t_1-1)}) \pmod{t_1}] + 1$. Clearly, by the uniqueness of the decompositions given in (14) and (15), if $b_k \neq b'_k$ for some $k \in \{2, \ldots, s\}$, then r_{i_x} and $r_{i'_{x'}}$ belong to different rows of $A_{p^{s-1}}$. However, if $b_k = b'_k$ for all $k \in \{2, \ldots, s\}$, then r_{i_x} and $r_{i'_{x'}}$ belong to the same row of $A_{p^{s-1}}$ if and only if $b_1 = b'_1 \pmod{t_1}$. Since $b_1 \in \{0, \ldots, \tau - 1\}$, then each row of $A_{p^{s-1}}$ contains at most $\lceil \frac{\tau}{t_1} \rceil$ leaders.

Denote by $S^{(j)}_{p^{s-1}}$, for $j \in \{1, \ldots, t_1 d_{p^{s-1}}\}$, the set containing the elements in the j-th row of $A^{(2)}_{p^{s-1}}$. For each matrix $\mathcal{M}_i^*$, if its leader belongs to the j-th row of $A_{p^{s-1}}$, then a subset of t_s distinct elements of $S^{(j)}_{p^{s-1}}$ is taken to fill the last t_s rows of this matrix. Note that any $s' \in S^{(j)}_{p^{s-1}}$ satisfies that $s' - r' \in (p^{s-1}) \subseteq \mathcal{R}$, where r' is the leader of $\mathcal{M}_i^*$, so the above condition (ii) is satisfied for $h = s - 1$. In order to satisfy condition (iii), the elements of $S^{(j)}_{p^{s-1}}$ can only be selected once. Thus, if more than one matrix have a leader in the same row j of $A_{p^{s-1}}$, then disjoint subsets of t_s elements of $S^{(j)}_{p^{s-1}}$ are selected, one for each matrix. Since each row j of $A_{p^{s-1}}$ may have up to $\lceil \frac{\tau}{t_1} \rceil$ leaders, then we must ensure that

$$\left\lceil \frac{\tau}{t_1} \right\rceil \leq \frac{|S^{(j)}_{p^{s-1}}|}{t_s}.$$

It is easy to see that this is guaranteed by condition (11) for $k = 1$.

Up to this point, we have selected the elements $r_{i_1}, \ldots, r_{i_{t_1}}$ and $r_{i_{t_1+\cdots+t_{s-1}+1}}, \ldots, r_{i_{t_1+\cdots+t_s}}$, for every $i \in \{0, \ldots, \alpha - 1\}$, satisfying conditions (i), (ii), and (iii). In particular, in order to satisfy condition (ii) for $h = s - 1$, we have used Table $A_{p^{s-1}}$, since any two elements r_i, r_j in the same row of $A_{p^{s-1}}$ satisfy $r_i - r_j \in (p^{s-1})$. After this step, the leaders are fixed for every matrix and the elements that have already been selected cannot be selected again in order to satisfy condition (iii).

In the next step, using the structure of the table $A_{p^{s-2}}$, we select the elements $r_{i_{t_1+\cdots+t_{s-2}+1}}, \ldots, r_{i_{t_1+\cdots+t_{s-1}}}$. They are chosen from the same row of $A_{p^{s-2}}$ as r_{i_x}, satisfying condition (ii) for $h = s - 2$. In general, an iterative process takes place, for $k \in \{2, \ldots, s-1\}$, where $r_{i_{t_1+\cdots+t_{s-k}+1}}, \ldots, r_{i_{t_1+\cdots+t_{s-k+1}}}$ are selected from the same row of $A_{p^{s-k}}$ as the leader of the corresponding matrix, so that condition (ii) is satisfied for $h = s - k$. The remaining part of the proof ensures that this is possible, that is, it is seen that there are enough elements to select all r_{i_j}, for $j \in \{1, \ldots, t_1 + \cdots + t_s\}$ and $i \in \{0, \ldots, \alpha - 1\}$, while satisfying these conditions.

Now, recall that the table $A_{p^{s-2}}$ has $t_1 d_{p^{s-2}}$ rows and $p^{2(t_1-1)}$ columns. Every element in the first $\frac{\alpha}{d_{p^{s-2}}} = p^{t_1-1}\tau$ columns of $A_{p^{s-2}}$ has already been selected as one of the elements $r_{i_1}, \ldots, r_{i_{t_1}}$, for some $i \in \{0, \ldots, \alpha - 1\}$. Moreover, some elements in the last $p^{2(t_1-1)} - p^{t_1-1}\tau$ columns of $A_{p^{s-2}}$ may have been selected as one of the elements $r_{i_{t_1+\cdots+t_{s-1}+1}}, \ldots, r_{i_{t_1+\cdots+t_s}}$, but some are still available in order to fill the remaining $t_2 + \cdots + t_{s-1}$ rows in each matrix.

Let $A^{(2)}_{p^{s-2}}$ be the subtable of $A_{p^{s-2}}$ consisting of the last $p^{2(t_1-1)} - p^{t_1-1}\tau$ columns and, for $\ell \in \{1, \ldots, t_1 d_{p^{s-2}}\}$, let $S^{(\ell)}_{p^{s-2}}$ be the set containing the elements in the ℓ-th row of $A^{(2)}_{p^{s-2}}$.

By construction, the ℓ-th row of $A_{p^{s-2}}$ and $A^{(2)}_{p^{s-2}}$ contains all elements from each j_{a_1}-th row of $A_{p^{s-1}}$ and $A^{(2)}_{p^{s-1}}$, respectively, where $j_{a_1} = a_1 t_1 d_{p^{s-2}} + \ell$ and $a_1 \in \{0, \ldots, p^{t_1-1}-1\}$. Thus,

$$S^{(\ell)}_{p^{s-2}} = \bigcup_{0 \leq a_1 \leq p^{t_1-1}-1} S^{(a_1 t_1 d_{p^{s-2}} + \ell)}_{p^{s-1}}.$$

Note that ℓ can be decomposed in a unique way as $\ell = a_2 t_1 d_{p^{s-3}} + \cdots + a_{s-2} t_1 d_p + a_{s-1} t_1 + a_s + 1$, where $a_2, \ldots, a_{s-2} \in \{0, \ldots, p^{t_1-1} - 1\}$, $a_{s-1} \in \{0, \ldots, d_p - 1\}$, and $a_s \in \{0, \ldots, t_1 - 1\}$. Recall that for a matrix $\mathcal{M}_i^*$, where i is as in (14), we selected as leader the element in the x-th position, r_{i_x}, where x is as in (16), which belongs to the j-th row of $A_{p^{s-1}}$, where j is as in (17). At the same time, r_{i_x} also belongs to the ℓ-th row of $A_{p^{s-2}}$, where $\ell = j \pmod{t_1 d_{p^{s-2}}}$. That is,

$$\begin{aligned} \ell = {} & a_2 t_1 d_{p^{s-3}} + \cdots + a_{s-2} t_1 d_p + a_{s-1} t_1 + a_s + 1 = \\ & b_3 t_1 d_{p^{s-3}} + \cdots + b_{s-1} t_1 d_p + b_s t_1 + \\ & \left[(b_1 + b_2\tau + b_3\tau p^{t_1-1} + \ldots + b_s \tau p^{(s-2)(t_1-1)}) \pmod{t_1} \right] + 1. \end{aligned} \tag{18}$$

Consider two matrices $\mathcal{M}_i^*$ and $\mathcal{M}_{i'}^*$, where $i = b_1 d_{p^{s-1}} + b_2 d_{p^{s-2}} + \cdots + b_{s-1} d_p + b_s$ and $i' = b'_1 d_{p^{s-1}} + b'_2 d_{p^{s-2}} + \cdots + b'_{s-1} d_p + b'_s$, and their respective leaders $r_{i_x}, r_{i'_{x'}}$. Clearly,

if $b_k \neq b'_k$ for a $k \in \{3,\ldots,s\}$, then r_{i_x} and $r_{i'_{x'}}$ belong to different rows of $A_{p^{s-1}}$. However, if $b_k = b'_k$ for all $k \in \{3,\ldots,s\}$, then r_{i_x} and $r_{i'_{x'}}$ belong to the same row ℓ of $A_{p^{s-2}}$ if and only if $b_1 + b_2\tau = (b'_1 + b'_2\tau) \pmod{t_1}$. Since $b_1 \in \{0,\ldots,\tau-1\}$ and $b_2 \in \{0,\ldots,p^{t_1-1}-1\}$, then each row of $A_{p^{s-2}}$ contains at most $\lceil \frac{p^{t_1-1}\tau}{t_1} \rceil$ leaders.

For each matrix $\mathcal{M}_i^*$, if its leader is in the ℓ-th row of $A_{p^{s-2}}$, then t_{s-1} distinct elements of $S^{(\ell)}_{p^{s-2}}$ are taken to be the elements $r_{i_{t_1+\cdots+t_{s-2}+1}},\ldots,r_{i_{t_1+\cdots+t_{s-1}}}$. Note that any $s' \in S^{(\ell)}_{p^{s-2}}$ satisfies that $s'-r' \in (p^{s-2}) \subseteq \mathcal{R}$, for any r' in the ℓ-th row of $A_{p^{s-2}}$, so the above condition (ii) is satisfied for $h = s-2$. To ensure condition (iii), the elements of $S^{(\ell)}_{p^{s-2}}$ can only be selected once, so $t_{s-1}+t_s$ different elements from $S^{(\ell)}_{p^{s-2}}$ must be selected for each leader in the ℓ-th row of $A_{p^{s-2}}$. Since each row ℓ of $A_{p^{s-2}}$ may have up to $\lceil \frac{p^{t_1-1}\tau}{t_1} \rceil$ leaders, then we must ensure that

$$\lceil \frac{p^{t_1-1}\tau}{t_1} \rceil \leq \frac{|S^{(\ell)}_{p^{s-2}}|}{t_{s-1}+t_s}.$$

It is easy to see that this is guaranteed by condition (11) for $k=2$.

Similarly, with an increasing ordering in $k \in \{3,\ldots,s-1\}$, we select the elements $r_{i_{t_1+\cdots+t_{s-k}+1}},\ldots,r_{i_{t_1+\cdots+t_{s-k+1}}}$ using the structure provided by $A_{p^{s-k}}$. Let $A^{(2)}_{p^{s-k}}$ be the subtable with the last $p^{(k-1)(t_1-1)}(p^{t_1-1}-\tau)$ columns of $A_{p^{s-k}}$, and let $S^{(\ell)}_{p^{s-k}}$ be the set containing the elements in the ℓ-th row of $A^{(2)}_{p^{s-k}}$. By construction, we have

$$\begin{aligned} S^{(\ell)}_{p^{s-k}} &= \bigcup_{0\leq a_{k-1}\leq p^{t_1-1}-1} S^{(a_{k-1}t_1 d_{p^{s-k}}+\ell)}_{p^{s-k+1}} \\ &\vdots \\ &= \bigcup_{0\leq a_1,\ldots,a_{k-1}\leq p^{t_1-1}-1} S^{(a_1 t_1 d_{p^{s-2}}+\cdots+a_{k-1}t_1 d_{p^{s-k}}+\ell)}_{p^{s-1}}. \end{aligned} \tag{19}$$

Using a similar argument to the one used for $k=2$, we see that each row of $A_{p^{s-k}}$ contains at most $\lceil \frac{p^{(k-1)(t_1-1)}\tau}{t_1} \rceil$ leaders. Moreover, any $s' \in S^{(\ell)}_{p^{s-k}}$ satisfies that $s'-r' \in (p^{s-k}) \subseteq \mathcal{R}$, for any r' in the ℓ-th row of $A_{p^{s-k}}$, so the above condition (ii) is satisfied for $h = s-k$. Since $S^{(\ell)}_{p^{s-k}}$ satisfies all equalities in (19), for each leader in the ℓ-th row of $A_{p^{s-k}}$, we must select $t_{s-k+1}+\cdots+t_s$ different elements in $S^{(\ell)}_{p^{s-k}}$. Therefore, we must ensure that

$$\lceil \frac{p^{(k-1)(t_1-1)}\tau}{t_1} \rceil \leq \frac{|S^{(\ell)}_{p^{s-k}}|}{t_{s-k+1}+\cdots+t_s},$$

which is guaranteed by condition (11).

By using this construction, we obtain a set of matrices $\{\mathcal{M}_0^*,\ldots,\mathcal{M}_{\alpha-1}^*\}$ such that $\mathcal{M}_i^* \in \mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$ for all $i \in \{0,\ldots,\alpha-1\}$. Furthermore, for each matrix $\mathcal{M}_i^*$, we can obtain $p^{(s-1)t_2+\cdots+t_s}$ different matrices, $\mathcal{M}_{i,k}^* \in \mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$, such that all rows from all matrices in $\{\mathcal{M}_{i,k}^* : 0 \leq i \leq \alpha-1, 0 \leq k \leq p^{(s-1)t_2+\cdots+t_s}-1\}$ are different. Define $\mathcal{M}_{i,k}$ as

$$\left(\begin{array}{c|c|c|c|c|c} 1 & r_{i_1} & \mathbf{u}_2^{(k)} & \mathbf{u}_3^{(k)} & \ldots & \mathbf{u}_s^{(k)} \\ \hline 0 & r_{i_2}-r_{i_1} & & & & \\ \vdots & \vdots & \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} \\ 0 & r_{i_{t_1}}-r_{i_1} & & & & \\ \hline 0 & \chi_1^{-1}(r_{i_{t_1+1}}-r_{i_1}) & & & & \\ \vdots & \vdots & I_{t_2} & \mathbf{0} & \ldots & \mathbf{0} \\ 0 & \chi_1^{-1}(r_{i_{t_1+t_2}}-r_{i_1}) & & & & \\ \hline 0 & \chi_2^{-1}(r_{i_{t_1+t_2+1}}-r_{i_1}) & & & & \\ \vdots & \vdots & \mathbf{0} & I_{t_3} & \ldots & \mathbf{0} \\ 0 & \chi_2^{-1}(r_{i_{t_1+t_2+t_3}}-r_{i_1}) & & & & \\ \hline \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \hline 0 & \chi_{s-1}^{-1}(r_{i_{t_1+\cdots+t_{s-1}+1}}-r_{i_1}) & & & & \\ \vdots & \vdots & \mathbf{0} & \mathbf{0} & \ldots & I_{t_s} \\ 0 & \chi_{s-1}^{-1}(r_{i_{t_1+\cdots+t_{s-1}+t_s}}-r_{i_1}) & & & & \end{array}\right), \tag{20}$$

where $\mathbf{u}_j^{(k)}$, $2 \leq j \leq s$, is a vector with t_j coordinates over $p^{j-1}\mathbb{Z}_{p^s}$. Note that there are $p^{(s-j+1)t_j}$ different vectors $\mathbf{u}_j^{(k)}$. Let $\mathcal{P} = \{\mathcal{M}_{i,k}^{-1} : 0 \leq i \leq \alpha-1, 0 \leq k \leq p^{(s-1)t_2+\cdots+t_s}-1\}$. By Theorem 1, $\Phi(\mathcal{P})$ is an r-PD-set of size $r+1$ for $H^{t_1,\ldots,t_s}$, with respect to the information set $\Phi(\mathcal{I}_{t_1,\ldots,t_s})$, for every $r \leq p^{(s-1)t_2+\cdots+t_s}\alpha - 1$. □

Example 5: Using the construction given by the proof of Theorem 2, we can construct a 12287-PD-set of size 12288 for the $\mathbb{Z}_8$-linear Hadamard code $H^{4,2,4}$. In this case, we have $d_2 = 2$, $h_2 = 0$, and $d_4 = 16$. First, tables A_2 and A_4 are constructed. The elements of $\mathcal{R} = \mathrm{GR}(8^3)$, the Galois ring of dimension 3 over $\mathbb{Z}_8$, are distributed in A_2, by columns, so that for any two elements $r_i, r_j \in \mathcal{R}$ in the same row, $r_i - r_j \in (2)$. Thus, table A_2 has $t_1 d_2 = 8$ rows and $4^{t_1-1} = 64$ columns. Since $h_2 = 0$, A_2 contains all the elements of $\mathcal{R}$. The elements of A_2 are also distributed in a table A_4, where each column is formed by the elements in $2^{t_1-1} = 8$ consecutive columns of A_2, so that for any two elements r_i, r_j in the same row, $r_i - r_j \in (4)$. Thus, table A_4 has $t_1 d_4 = 64$ rows and $2^{t_1-1} = 8$ columns. Figure 1 shows table A_4 and the transpose of table A_2, giving only the index i for each element $r_i \in \mathcal{R}$.

The maximum value of α satisfying conditions (21) and (22) is $\alpha = 48$. From the first $\alpha = 48$ blocks of $t_1 = 4$ consecutive elements of $\mathcal{R}$, which are placed in the first $\tau = \alpha/d_4 = 3$ columns of A_4, we construct the first t_1 rows of matrices $\mathcal{M}_0^*,\ldots,\mathcal{M}_{47}^*$. The bordered elements in table A_4 of Figure 1 are selected as the leaders for the corresponding matrices, and the ones with a light gray background are selected to construct the last $t_3 = 4$ rows of these matrices. The elements with a dark gray background in table A_2 of Figure 1 are selected to construct the remaining $t_2 = 2$ rows, 5-th and 6-th rows, of these matrices. By construction, the leaders $1, 66, 131, 12, 73, 138, \ldots$ are distributed cyclically among the t_1 positions of the blocks. Moreover, they are also distributed in a balanced way among the first t_1 rows of A_2. This ensures that there are enough elements of each class in order to fill

the last $t_2+t_3=6$ rows of these matrices. For example, the first matrix $\mathcal{M}_0^*$ is constructed as follows:

$$\mathcal{M}_0^* = \begin{pmatrix} 1 & r_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & r_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & r_3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & r_4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & r_{217} & 2 & 0 & 0 & 0 & 0 & 0 \\ 1 & r_{249} & 0 & 2 & 0 & 0 & 0 & 0 \\ 1 & r_{193} & 0 & 0 & 4 & 0 & 0 & 0 \\ 1 & r_{257} & 0 & 0 & 0 & 4 & 0 & 0 \\ 1 & r_{321} & 0 & 0 & 0 & 0 & 4 & 0 \\ 1 & r_{385} & 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 6 & 2 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 4 & 6 & 0 & 2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 4 & 0 & 0 & 4 & 0 & 0 & 0 \\ 1 & 4 & 4 & 0 & 0 & 0 & 0 & 4 & 0 & 0 \\ 1 & 0 & 4 & 4 & 0 & 0 & 0 & 0 & 4 & 0 \\ 1 & 4 & 4 & 4 & 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}.$$

Then,

$$\mathcal{M}_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Finally, we can obtain $4^2 2^4 = 256$ different matrices $\mathcal{M}_{i,k}^*$, $0 \le k \le 255$, for each one of the matrices $\mathcal{M}_i^*$, $0 \le i \le 47$, which give us a 12287-PD-set of size $48 \cdot 256 = 12288$ for the code $H^{4,2,4}$.

Remark 1: The $s-1$ conditions (11) given by Theorem 2 for $k \in \{1,\ldots,s-1\}$ are independent and must be satisfied in order to obtain a valid value for α. For example, consider the case $p=2$ and $s=3$. From (11) we obtain the following two conditions:

$$\text{for } k=2, \quad \alpha \le t_1 d_2 \left\lfloor \frac{4^{t_1-1} - 2^{t_1-1}\tau}{t_2+t_3} \right\rfloor \text{ when } t_2+t_3>0, \tag{21}$$

$$\text{for } k=1, \quad \alpha \le t_1 d_4 \left\lfloor \frac{2^{t_1-1} - \tau}{t_3} \right\rfloor \text{ when } t_3>0. \tag{22}$$

It is easy to see that condition (21) does not imply condition (22), and vice versa. For instance, for the $\mathbb{Z}_8$-linear Hadamard code $H^{4,2,4}$, which is considered in Example 5, the maximum multiple of $d_4=16$ that satisfies both conditions is $\alpha=48$. Let us denote the right-hand side of both restrictions by $f_1(\alpha;\, t_1,t_2,t_3)$ and $f_2(\alpha;\, t_1,t_2,t_3)$, respectively. Then,

$$f_1(48;\,4,2,4)=48, \quad f_1(64;\,4,2,4)=40<\alpha=64,$$
$$f_2(48;\,4,2,4)=64, \quad f_2(64;\,4,2,4)=64.$$

Note that if $\alpha=64$, which is the next multiple of $d_4=16$, condition (22) is fulfilled, but condition (21) is not satisfied. On the other hand, for the $\mathbb{Z}_8$-linear Hadamard code $H^{4,0,4}$, the maximum feasible value for α is $\alpha=64$. For this value and the next multiple of $d_4=16$, $\alpha=80$, the following restrictions are obtained:

$$f_1(64;\,4,0,2)=128, \quad f_1(80;\,4,0,2)=96,$$
$$f_2(64;\,4,0,2)=128, \quad f_2(80;\,4,0,2)=64<\alpha=80.$$

Thus, if $\alpha=80$, condition (21) is fulfilled, but condition (22) is not satisfied.

Note that Theorem 2 can only be applied when $t_1 \ge 2$. For the $\mathbb{Z}_{p^s}$-linear GH codes $H^{1,t_2,\ldots,t_s} = H^{1,0,\ldots,0,t_j,\ldots,t_s}$, where $j=\min\{i \mid i \in \{2,\ldots,s\}, t_i>0\}$, it is possible to obtain r-PD-sets of size $r+1$ by applying the recursive constructions presented in [39] as follows. Let $j'=\min\{i \mid i \in \{j,\ldots,s\}, t_i>1\}$. First, we use Theorem 2 to obtain an r-PD-set for $H^{t_{j'},\ldots,t_s}$ with $r \le g_p^{t_{j'},\ldots,t_s}$, and then, we use [39, Corollary 6.1] to extend it to an r-PD-set for $H^{1,0,\ldots,0,t_j,\ldots,t_s}$. Next proposition allows us to present a new construction to obtain r-PD-sets of size $r+1$ for the $\mathbb{Z}_{p^s}$-linear GH codes $H^{1,t_2,\ldots,t_s} = H^{1,0,\ldots,0,t_j,\ldots,t_s}$ (see Corollary 3), which gives an r-PD-set with $r \le g_p^{t_j+1,t_{j+1},\ldots,t_s}$. Note that $j \le j'$ and $g_p^{t_j+1,t_{j+1},\ldots,t_s} \ge g_p^{t_{j'},\ldots,t_s}$.

Proposition 2: Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$ be a $\mathbb{Z}_{p^s}$-additive GH code of type $(n;t_1,t_2,\ldots,t_s)$ with $t_1 \ge 2$, and let $\mathcal{H}' = \mathcal{H}^{1,0,\ldots,0,t_1-1,\ldots,t_s}$ be a $\mathbb{Z}_{p^{s'}}$-additive GH code of type $(n';1,0,\ldots,0,t_1-1,t_2,\ldots,t_s)$ with $s'>s$. If there exists a set $\mathcal{S} \subseteq \mathrm{PAut}(\mathcal{H})$ such that $\Phi(\mathcal{S})$ is an r-PD-set of size $r+1$ for $H=\Phi(\mathcal{H})$, then there exists a set $\mathcal{P} \subseteq \mathrm{PAut}(\mathcal{H}')$ such that $\Phi(\mathcal{P})$ is an r-PD-set of size $r+1$ for $H'=\Phi(\mathcal{H}')$.

Proof: Let $\mathcal{S}=\{\mathcal{M}_1^{-1},\ldots,\mathcal{M}_{r+1}^{-1}\} \subseteq \mathrm{PAut}(\mathcal{H})$ such that $\Phi(\mathcal{S})$ is an r-PD-set for $H=\Phi(\mathcal{H})$. Since $\mathcal{M}_i$ is as in (5), we can partition it as

$$\mathcal{M}_i = \begin{pmatrix} 1 & a \\ \mathbf{0} & A \end{pmatrix}.$$

Then, we define the following matrix over $\mathbb{Z}_{p^{s'}}$:

$$\mathcal{N}_i = \begin{pmatrix} 1 & \chi(a) \\ \mathbf{0} & \iota(A) \end{pmatrix},$$

where χ and ι are maps from $\mathbb{Z}_{p^s}$ to $\mathbb{Z}_{p^{s'}}$ defined as $\chi(a)=p^{s'-s}a$ and $\iota(a)=a$, respectively. Clearly, if $\mathcal{M}_i \in \mathrm{PAut}(\mathcal{H})$, then $\mathcal{N}_i \in \mathrm{PAut}(\mathcal{H}')$.

Let $m_{i,j}=(a_j,\bar{m}_{i,j})$ and $n_{i,j}=(a_j,\bar{n}_{i,j})$ be the j-th rows of $\mathcal{M}_i$ and $\mathcal{N}_i$, respectively, where $a_1=1$ and $a_j=0$ if $j>1$. Note that $\bar{n}_{i,1}=p^{s'-s}\bar{m}_{i,1}$ for any $i \in \{1,\ldots,r+1\}$, and $\bar{n}_{i,j}=\bar{m}_{i,j}$ for any $i \in \{1,\ldots,r+1\}$ and $j \in \{2,\ldots,t_1+\cdots+t_s\}$.

Consider also the j-th rows $m_{i,j}^*=(1,\bar{m}_{i,j}^*)$ and $n_{i,j}^*=(1,\bar{n}_{i,j}^*)$ of $\mathcal{M}_i^*$ and $\mathcal{N}_i^*$, respectively. We have

$$m_{i,1}^* = m_{i,1} = (1,\bar{m}_{i,1}),$$
$$m_{i,j}^* = m_{i,1}+m_{i,j} = (1,\bar{m}_{i,1}+\bar{m}_{i,j}) \quad \text{if } j \in \{2,\ldots,t_1\},$$
$$m_{i,j}^* = m_{i,1}+p^{k-1}m_{i,j} = (1,\bar{m}_{i,1}+p^{k-1}\bar{m}_{i,j}) \quad \text{if } j \in \{t_1+\cdots+t_{k-1}+1,\ldots,t_1+\cdots+t_k\}.$$

Similarly,

$$\begin{aligned} n^*_{i,1} &= n_{i,1} = (1, \bar{n}_{i,1}), \\ n^*_{i,j} &= n_{i,1} + p^{s'-s} n_{i,j} = (1, \bar{n}_{i,1} + p^{s'-s}\bar{n}_{i,j}) \\ &\quad \text{if } j \in \{2, \ldots, t_1\}, \\ n^*_{i,j} &= n_{i,1} + p^{s'-s+k-1} n_{i,j} = (1, \bar{n}_{i,1} + p^{s'-s+k-1}\bar{n}_{i,j}) \\ &\quad \text{if } j \in \{t_1 + \cdots + t_{k-1} + 1, \ldots, t_1 + \cdots + t_k\}. \end{aligned}$$

Therefore, $\bar{n}^*_{i,j} = p^{s'-s}\bar{m}^*_{i,j}$ for any $i \in \{1, \ldots, r+1\}$ and $j \in \{1, \ldots, t_1 + \cdots + t_s\}$. By Theorem 1, all rows $m^*_{i,j} = (1, \bar{m}^*_{i,j})$ are different over $\mathbb{Z}_{p^s}$. Thus, all rows $n^*_{i,j} = (1, p^{s'-s}\bar{m}^*_{i,j})$ are different over $\mathbb{Z}_{p^{s'}}$. Using again Theorem 1, we obtain that $\Phi(\mathcal{P}) = \Phi(\{\mathcal{N}_1^{-1}, \ldots, \mathcal{N}_{r+1}^{-1}\})$ is an r-PD-set for $H' = \Phi(\mathcal{H}')$. □

Corollary 3: Let $H^{1,t_2,\ldots,t_s}$ be a $\mathbb{Z}_{p^s}$-linear GH code of type $(n; 1, t_2, \ldots, t_s)$ and let $j \in \{2, \ldots, s\}$ be the minimum index such that $t_j > 0$. If $t_{j+1} + \cdots + t_s > 0$, then there exist r-PD-sets of size $r+1$ for $H^{1,t_2,\ldots,t_s}$, with respect to the information set $\Phi(\mathcal{I}_{1,t_2,\ldots,t_s})$, for every $r \le g_p^{1,t_2,\ldots,t_s} = g_p^{t_j+1,t_{j+1},\ldots,t_s}$, where $g_p^{t_j+1,t_{j+1},\ldots,t_s}$ is defined as in (10).

Proof: By Theorem 2, there exist r-PD-sets of size $r+1$ for $H^{t_j+1,\ldots,t_s}$, with respect to the information set $\Phi(\mathcal{I}_{t_j+1,\ldots,t_s})$, for every $r \le g_p^{t_j+1,\ldots,t_s}$. In fact, in the proof of Theorem 2, we see that these r-PD-sets, say S, can be obtained as $S = \Phi(\mathcal{S})$, where $\mathcal{S} \subseteq \mathrm{PAut}(\mathcal{H}^{t_j+1,\ldots,t_s})$. Therefore, Proposition 2 guarantees the existence of a set $\mathcal{P} \subseteq \mathrm{PAut}(\mathcal{H}^{1,t_2,\ldots,t_s})$ such that $\Phi(\mathcal{P})$ is an r-PD-set of size $r+1$ for $H^{1,t_2,\ldots,t_s}$ with respect to the information set $\Phi(\mathcal{I}_{1,t_2,\ldots,t_s})$. □

Example 6: By Corollary 3, from the r-PD-set of size $r+1$ given in Example 5, we can obtain a 12287-PD-set of size 12288 for the $\mathbb{Z}_{2^s}$-linear Hadamard codes $H^{1,3,2,4}$, $H^{1,0,3,2,4}$, $H^{1,0,0,3,2,4}$, ... with $s = 4, 5, 6, \ldots$, respectively.

Corollary 3 can be seen as a generalization of the construction of r-PD-sets of size $r+1$ for $\mathbb{Z}_{p^s}$-linear GH codes $H_i = H^{1,0,\ldots,0,t_i,0,\ldots,0}$ with $t_i > 0$ for all $i \in \{2, \ldots, s\}$, given by Corollary 5.1 in [39]. The combination of both results implies that we can obtain an r-PD-set of size $r+1$ for any code $H^{1,t_2,\ldots,t_s}$.

IV. Upper Bound Comparative Analysis

Using the construction proposed in Theorem 2 and Corollary 3, r-PD-sets of size $r+1$ with $r \le g_p^{t_1,\ldots,t_s}$ can be obtained for the $\mathbb{Z}_{p^s}$-linear codes $H^{t_1,\ldots,t_s}$ with $t_2 + \cdots + t_s > 0$. By Corollary 2, we have that $g_p^{t_1,\ldots,t_s} \le f_p^{t_1,\ldots,t_s}$. In this section, we find new values of $p, t_1, \ldots, t_s$ for which this theoretical upper bound $f_p^{t_1,\ldots,t_s}$ is tight. Moreover, even when the upper bound is not reached, $g_p^{t_1,\ldots,t_s}$ approaches $f_p^{t_1,\ldots,t_s}$ considerably. Finally, computational results given in [39] are compared with the values of $g_p^{t_1,\ldots,t_s}$.

Table I shows the values of $g_2^{t_1,t_2,t_3}$ and $f_2^{t_1,t_2,t_3}$, where $t_1 \in \{3, 4, 5\}$ and $t_2, t_3 \in \{0, 1, 2, 3, 4\}$. Gray colored cells indicate that the upper bound is reached, that is, $g_2^{t_1,t_2,t_3} = f_2^{t_1,t_2,t_3}$. Note that $g_2^{t_1,0,0}$ is not defined for any $t_1 \ge 1$. We use the symbol $-$ to represent this undefined value. Moreover, note that there are cases where $g_2^{t_1,t_2,t_3}$ is defined but it is equal to -1, which means that the construction given by Theorem 2 is not able to produce an r-PD-set. As an illustration, see Example 5, where we construct an r-PD-set of size $r+1$ for the code $H^{4,2,4}$, with $r = g_2^{4,2,4} = 12287$, which does not reach the upper bound $f_2^{4,2,4} = 13106$, so there could be r-PD-sets of size $r+1$ for $H^{4,2,4}$ such that $g_2^{4,2,4} = 12287 < r \le 13106 = f_2^{4,2,4}$.

The results given in this paper, using Theorem 2 and Corollary 3, allow us to achieve r-PD-sets of size $r+1$ up to $r \le g_p^{t_1,\ldots,t_s}$. These results are usually better than the ones obtained in [39], where the given r-PD-sets are of size

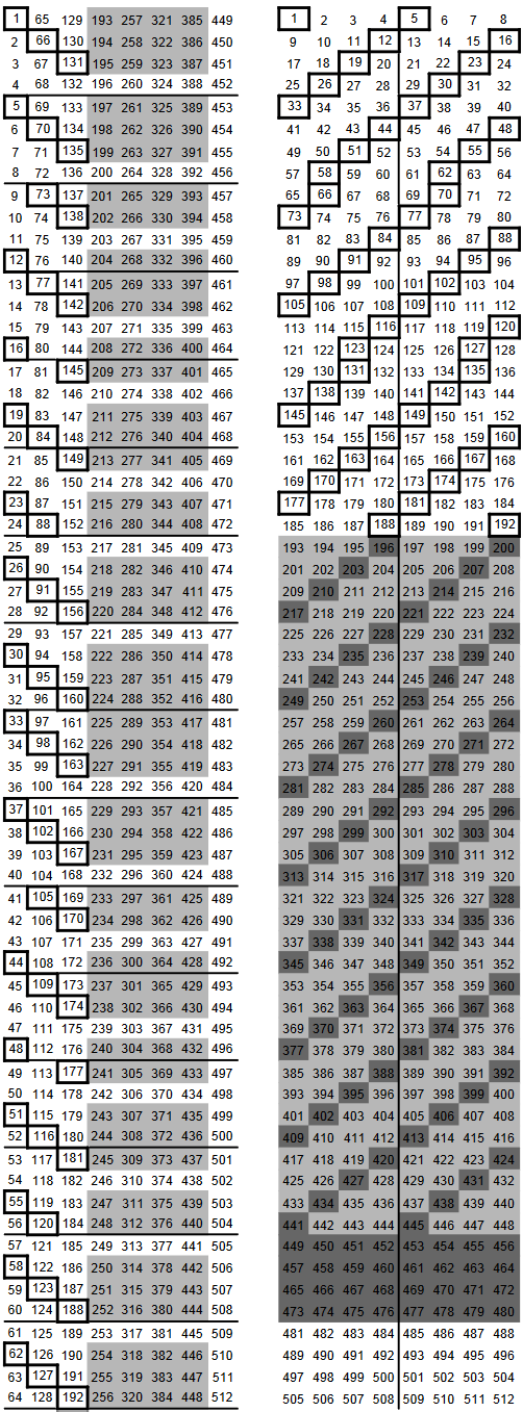

Fig. 1. Table A_4 (left) and the transpose of A_2 (right), used for the construction of an 12287-PD-set of size 12288 for $H^{4,2,4}$ in Example 5.

TABLE I

COLUMNS g_2 AND f_2 CONTAIN THE VALUES OF $g_2^{t_1,t_2,t_3}$ AND $f_2^{t_1,t_2,t_3}$, FOR $t_1 \in \{3,4,5\}$, $t_2, t_3 \in \{0,1,2,3,4\}$, RESPECTIVELY

		$t_3=0$		$t_3=1$		$t_3=2$		$t_3=3$		$t_3=4$	
t_1	t_2	g_2	f_2	g_2	f_2	g_2	f_2	g_2	f_2	g_2	f_2
3	0	–	20	23	31	31	50	31	84	-1	145
3	1	47	63	63	101	63	169	127	291	-1	511
3	2	127	203	127	340	255	584	511	1023	-1	1819
3	3	255	681	511	1169	1023	2047	2047	3639	-1	6552
3	4	1023	2339	2047	4095	4095	7280	-1	13106	-1	23830

		$t_3=0$		$t_3=1$		$t_3=2$		$t_3=3$		$t_3=4$	
t_1	t_2	g_2	f_2	g_2	f_2	g_2	f_2	g_2	f_2	g_2	f_2
4	0	–	127	191	203	255	340	511	584	1023	1023
4	1	383	408	639	681	1023	1169	2047	2047	3071	3639
4	2	1279	1364	2047	2339	4095	4095	6143	7280	12287	13106
4	3	4095	4680	8191	8191	12287	14562	24575	26213	32767	47661
4	4	16383	16383	24575	29126	49151	52427	65535	95324	131071	174761

		$t_3=0$		$t_3=1$		$t_3=2$		$t_3=3$		$t_3=4$	
t_1	t_2	g_2	f_2	g_2	f_2	g_2	f_2	g_2	f_2	g_2	f_2
5	0	–	818	1247	1364	1919	2339	3839	4095	6143	7280
5	1	2495	2729	4223	4680	7679	8191	12287	14562	21503	26213
5	2	8447	9361	15359	16383	24575	29126	43007	52427	86015	95324
5	3	30719	32767	49151	58253	86015	104856	172031	190649	294911	349524
5	4	98303	116507	172031	209714	344063	381299	589823	699049	1179647	1290554

TABLE II

COLUMNS g_2, $\tilde{f}_2$, AND h_2 CONTAIN THE VALUES OF g_2^{3,t_2,t_3}, $\tilde{f}_2^{3,t_2,t_3}$, AND h_2^{3,t_2,t_3}, FOR $t_2, t_3 \in \{0,1,2,3,4\}$, RESPECTIVELY

	$t_3=0$		$t_3=1$		$t_3=2$		$t_3=3$		$t_3=4$	
t_2	g_2	$\tilde{f}_2, h_2$	g_2	$\tilde{f}_2, h_2$	g_2	$\tilde{f}_2, h_2$	g_2	$\tilde{f}_2, h_2$	g_2	$\tilde{f}_2, h_2$
0	–	**20**, 1	**23**	20, 1	**31**	20, 1	**31**	20, 1	-1	**20**, 1
1	**47**	20, 1	**63**	20, 1	**63**	20, 1	**127**	20, 1	-1	**20**, 1
2	**127**	20, 1	**127**	20, 1	**255**	20, 1	**511**	20, 1	-1	**20**, 1
3	**255**	20, 1	**511**	20, 1	**1023**	20, 1	**2047**	20, 1	-1	**20**, 1
4	**1023**	50, 2	**2047**	50, 2	**4095**	50, 2	-1	**50**, 2	-1	**50**, 2

TABLE III

COLUMNS $g_3, \tilde{f}_3$, AND h_3 CONTAIN THE VALUES OF g_3^{2,t_2,t_3}, $\tilde{f}_3^{2,t_2,t_3}$, AND h_3^{2,t_2,t_3}, FOR $t_2, t_3 \in \{0,1,2\}$, RESPECTIVELY

	$t_3=0$		$t_3=1$		$t_3=2$	
t_2	g_3	$\tilde{f}_3, h_3$	g_3	$\tilde{f}_3, h_3$	g_3	$\tilde{f}_3, h_3$
0	–	**12**, 1	**17**	12, 1	**26**	12, 1
1	**53**	12, 1	**80**	12, 1	**80**	12, 1
2	**242**	26, 2	**728**	26, 2	-1	**26**, 2

TABLE IV

VALUES r_c FOR WHICH r_c-PD-SETS FOR $\mathbb{Z}_4$-LINEAR HADAMARD CODES H^{t_1,t_2} WITH $t_1 \in \{3,4,5\}$ AND $t_2 \in \{0,1,2,3,4,5\}$ WERE FOUND IN [39] USING A NON-DETERMINISTIC METHOD. THE CORRESPONDING VALUES OF $g_2^{t_1,t_2}$ AND $f_2^{t_1,t_2}$ ARE ALSO GIVEN

t_1	t_2	r_c	$g_2^{t_1,t_2}$	$f_2^{t_1,t_2}$
3	0	**4**	–	4
	1	**7**	5	7
	2	**11**	7	11
	3	**18**	7	20
	4	**31**	-1	35
	5	**50**	-1	63
4	0	**15**	–	15
	1	**23**	**23**	24
	2	**38**	31	41
	3	62	**63**	72
	4	103	**127**	127
	5	172	**191**	226
5	0	**50**	–	50
	1	76	**77**	84
	2	**124**	119	145
	3	199	**239**	255
	4	321	**383**	454
	5	551	**575**	818

$r+1$ up to $r \leq \tilde{f}_p^{t_1,\ldots,t_s}$. However, there are some isolated cases where $g_p^{t_1,\ldots,t_s} < \tilde{f}_p^{t_1,\ldots,t_s}$, such as when $g_p^{t_1,\ldots,t_s} = -1$. There are some even more isolated cases in which $g_p^{t_1,\ldots,t_s}$ is not defined, such as when $t_2 = \cdots = t_s = 0$ for any t_1. In the latter case, $\tilde{f}_p^{t_1,0,\ldots,0} = f_p^{t_1,0,\ldots,0}$, so the upper bound can be achieved instead by using the explicit construction given in [39, Theorem 5.1].

Table II shows the values of g_2^{3,t_2,t_3}, $\tilde{f}_2^{3,t_2,t_3}$ and h_2^{3,t_2,t_3}, as defined in (9), where $t_2, t_3 \in \{0,1,2,3,4\}$. This table considers the same cases as the first subtable in Table I, where $t_1 = 3$. As mentioned above, $g_2^{3,0,0}$ is not defined, but in this case the code is free, so we can use the explicit construction given in [39, Theorem 5.1], obtaining $\tilde{f}_p^{3,0,0} = f_p^{3,0,0} = 20$. Note that $\tilde{f}_2^{3,4,t_3} = f_2^{1,4,0} = 50$ for any $t_3 \in \{0,1,2,3,4\}$, that is, $h_2^{3,4,t_3} = 2$. However, if $t_2 < 4$, then $\tilde{f}_2^{3,t_2,t_3} = f_2^{3,0,0} = 20$ for any $t_3 \in \{0,1,2,3,4\}$, that is, $h_2^{3,t_2,t_3} = 1$. Similarly, Table III shows the values of g_3^{2,t_2,t_3}, $\tilde{f}_3^{2,t_2,t_3}$ and h_3^{2,t_2,t_3}, as defined in (9), where $t_2, t_3 \in \{0,1,2\}$. In both tables, the maximum value between $g_p^{t_1,t_2,t_3}$ and $\tilde{f}_p^{t_1,t_2,t_3}$ is shown in bold type.

In [39], some computational results showed that r-PD-sets can be obtained with $\tilde{f}_p^{t_1,\ldots,t_s} \leq r \leq f_p^{t_1,\ldots,t_s}$. In fact, some of

those computational results improve the values of $g_p^{t_1,\ldots,t_s}$. For example, a 73-PD-set of size 74 was found computationally for the $\mathbb{Z}_8$-linear code $H^{3,0,3}$. Note that $g_2^{3,0,3} = 31 < 73 < 84 = f_2^{3,0,3}$. Indeed, for all $\mathbb{Z}_8$-linear codes H^{3,t_2,t_3} with $t_2 \in \{0,1,2\}$ and $t_3 \in \{0,1,2,3\}$, the computational results given in [39, Table 2] are better than the values of g_2^{3,t_2,t_3}. On the other hand, for the $\mathbb{Z}_4$-linear codes H^{4,t_2} with $t_2 \in \{3,4,5\}$ and H^{5,t_2} with $t_2 \in \{1,3,4,5\}$, the values of g_p^{4,t_2} and g_p^{5,t_2} are better than the computational results given in [39, Table 1], which are denoted by r_c. Table IV shows the values of r_c and the values of $g_2^{t_1,t_2}$ and $f_2^{t_1,t_2}$ for the $\mathbb{Z}_4$-linear Hadamard codes H^{t_1,t_2} with $t_1 \in \{3,4,5\}$ and $t_2 \in \{0,1,2,3,4,5\}$. The maximum between r_c and $g_2^{t_1,t_2}$ is shown in bold type, and the gray coloured cells indicate the case where the upper bound is reached.

V. Conclusion

In [39], explicit constructions of r-PD-sets of minimum size $r+1$ for $\mathbb{Z}_{p^s}$-linear GH codes $H^{t_1,\ldots,t_s}$, with values of r up to $\tilde{f}_p^{t_1,\ldots,t_s}$, were given. These values of r are usually far from the theoretical upper bound $f_p^{t_1,\ldots,t_s}$. In this paper, new explicit constructions of r-PD-sets of size $r+1$ for these codes, for values of r larger than $\tilde{f}_p^{t_1,\ldots,t_s}$ and closer to the upper bound $f_p^{t_1,\ldots,t_s}$, are given.

For some infinite families of codes, these constructions allow us to construct r-PD-sets with r up to the upper bound, that is, for all $r \leq f_p^{t_1,\ldots,t_s}$. A natural direction of further research on this topic is to achieve the theoretical upper bound for all cases, or to prove that there are cases where it is impossible, resulting in a lower upper bound which depends on the type of the code.

As also mentioned in [39], another topic of further research is the generalization of these results to other families of $\mathbb{Z}_{p^s}$-linear codes [21], [35], [36] or 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 [9], [10], 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], [29], and [37]. The results given in [38] 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], and [7], [8] showing that they are not necessarily equivalent to the $\mathbb{Z}_{p^s}$-linear GH codes considered in this paper.

Finally, we would like to point out that some Magma functions to construct the r-PD-sets of size $r+1$, described in [39] and in the current paper, have been developed by the authors. They have 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 [11]. It has been developed mainly by the authors of this paper and with the collaboration of some undergraduate students. The first version of this new package and a manual describing all functions are available in a GitHub repository (https://github.com/merce-github/ZpAdditiveCodes) and in the CCSG website (https://ccsg.uab.cat).

References

[1] I. Aydogdu and I. Siap, "On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes," *Linear Multilinear Algebra*, vol. 63, no. 10, pp. 2089–2102, 2015.

[2] R. D. Barrolleta and M. Villanueva, "Partial permutation decoding for binary linear and $\mathbb{Z}_4$-linear Hadamard codes," *Des., Codes Cryptogr.*, vol. 86, no. 3, pp. 569–586, Mar. 2018.

[3] R. D. Barrolleta and M. Villanueva, "Partial permutation decoding for several families of linear and $\mathbb{Z}_4$-linear codes," *IEEE Trans. Inf. Theory*, vol. 65, no. 1, pp. 131–141, Jan. 2019.

[4] J. J. Bernal, J. Borges, C. Fernández-Córdoba, and M. Villanueva, "Permutation decoding of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes," *Des. Codes Cryptogr.*, vol. 76, no. 2, pp. 269–277, 2015.

[5] D. K. Bhunia, C. Fernández-Córdoba, C. Vela, and M. Villanueva, "On the equivalence of $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes," *Des. Codes Cryptogr.*, vol. 92, no. 4, pp. 999–1022, 2024.

[6] D. K. Bhunia, C. Fernández-Córdoba, and M. Villanueva, "On the linearity and classification of $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes," *Des. Codes Cryptogr.*, vol. 90, no. 4, pp. 1037–1058, 2022.

[7] D. K. Bhunia, C. Fernández-Córdoba, and M. Villanueva, "On the constructions of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear generalized Hadamard codes," *Finite Fields Their Appl.*, vol. 83, Jan. 2022, Art. no. 102093.

[8] D. K. Bhunia, C. Fernández-Córdoba, and M. Villanueva, "Linearity and classification of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear generalized Hadamard codes," *Finite Fields Their Appl.*, vol. 86, Feb. 2023, Art. no. 102140.

[9] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. Villanueva, "$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: Generator matrices and duality," *Des. Codes Cryptogr.*, vol. 54, no. 2, pp. 167–179, 2010.

[10] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. Villanueva, $\mathbb{Z}_2\mathbb{Z}_4$*-Linear Codes*. Cham, Switzerland: Springer, 2022.

[11] W. Bosma, J. J. Cannon, C. Fieker, and A. Steel. (2022). *Handbook of Magma functions, Version 2.27*. [Online]. Available: https://magma.maths.usyd.edu.au/magma/

[12] C. Carlet, "$\mathbb{Z}_{2^k}$-linear codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1543–1547, Jan. 1998.

[13] B. J. Chathely and R. P. Deore, "Construction of binary Hadamard codes and their s-PD sets," *Cryptogr. Commun.*, vol. 13, no. 3, pp. 425–438, May 2021.

[14] I. Constantinescu and W. Heise, "A metric for codes over residue class rings," *Problemy Peredachi Informatsii*, vol. 33, no. 3, pp. 22–28, 1997.

[15] S. T. Dougherty and C. Fernández-Córdoba, "Codes over $\mathbb{Z}_{2^k}$, Gray map and self-dual codes," *Adv. Math. Commun.*, vol. 5, no. 4, pp. 571–588, 2011.

[16] S. T. Dougherty, J. Rifà, and M. Villanueva, "Ranks and kernels of codes from generalized Hadamard matrices," *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 687–694, Feb. 2016.

[17] C. Fernández-Córdoba, A. Torres-Martín, and M. Villanueva, *Linear Codes Over the Integer Residue Ring $\mathbb{Z}_{p^s}$. A MAGMA Package, Version 1.0*. Bellaterra, Spain: Universitat Autònoma de Barcelona, 2023. [Online]. Available: https://ccsg.uab.cat

[18] C. Fernández-Córdoba, C. Vela, and M. Villanueva, "On $\mathbb{Z}_{2^s}$-linear Hadamard codes: Kernel and partial classification," *Des. Codes Cryptogr.*, vol. 87, nos. 2–3, pp. 417–435, 2019.

[19] C. Fernández-Córdoba, C. Vela, and M. Villanueva, "Equivalences among $\mathbb{Z}_{2^s}$-linear Hadamard codes," *Discrete Math.*, vol. 343, no. 3, 2020, Art. no. 111721.

[20] C. Fernández-Córdoba, C. Vela, and M. Villanueva, "On $\mathbb{Z}_8$-linear Hadamard codes: Rank and classification," *IEEE Trans. Inf. Theory*, vol. 66, no. 2, pp. 970–982, Feb. 2020.

[21] C. Fernández-Córdoba, C. Vela, and M. Villanueva, "Nonlinearity and kernel of $\mathbb{Z}_{2^s}$-linear simplex and MacDonald codes," *IEEE Trans. Inf. Theory*, vol. 68, no. 11, pp. 7174–7183, Nov. 2022.

[22] W. Fish, J. D. Key, and E. Mwambene, "Partial permutation decoding for simplex codes," *Adv. Math. Commun.*, vol. 6, no. 4, pp. 505–516, 2012.
[23] M. Greferath and S. E. Schmidt, "Gray isometries for finite chain rings and a nonlinear ternary (36, 3^{12}, 15) code," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2522–2524, Nov. 1999.
[24] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Sole, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 301–319, Mar. 1994.
[25] D. Jungnickel, "On difference matrices, resolvable transversal designs and generalized Hadamard matrices," *Mathematische Zeitschrift*, vol. 167, no. 1, pp. 49–60, Feb. 1979.
[26] D. S. Krotov, "On $\mathbb{Z}_{2^k}$-dual binary codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 4, pp. 1532–1537, Jan. 2007.
[27] D. S. Krotov, "$\mathbb{Z}_4$-linear Hadamard and extended perfect codes," *Electron. Notes Discrete Math.*, vol. 6, pp. 107–112, Apr. 2001.
[28] D. S. Krotov and M. Villanueva, "Classification of the $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes and their automorphism groups," *IEEE Trans. Inf. Theory*, vol. 61, no. 2, pp. 887–894, Feb. 2015.
[29] X. Li, M. Shi, S. Wang, H. Lu, and Y. Zheng, "Rank and pairs of rank and dimension of kernel of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear codes," *IEEE Trans. Inf. Theory*, vol. 70, no. 5, pp. 3202–3212, May 2024.
[30] J. Macwilliams, "Permutation decoding of systematic codes," *Bell Syst. Tech. J.*, vol. 43, no. 1, pp. 485–505, Jan. 1964.
[31] A. A. Nechaev, "Kerdock code in a cyclic form," *Discrete Math. Appl.*, vol. 1, no. 4, pp. 365–384, 1991.
[32] J. Pernas, J. Pujol, and M. Villanueva, "Characterization of the automorphism group of quaternary linear Hadamard codes," *Des., Codes Cryptogr.*, vol. 70, nos. 1–2, pp. 105–115, Jan. 2014.
[33] K. T. Phelps, J. Rifà, and M. Villanueva, "On the additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes: Rank and kernel," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 316–319, Sep. 2006.
[34] E. Prange, "The use of information sets in decoding cyclic codes," *IEEE Trans. Inf. Theory*, vol. IT-8, no. 5, pp. 5–9, Sep. 1962.
[35] M. Shi, T. Honold, P. Solé, Y. Qiu, R. Wu, and Z. Sepasdar, "The geometry of two-weight codes over $\mathbb{Z}_{p^m}$," *IEEE Trans. Inf. Theory*, vol. 67, no. 12, pp. 7769–7781, Dec. 2021.
[36] M. Shi, Z. Sepasdar, A. Alahmadi, and P. Solé, "On two-weight $\mathbb{Z}_{2^k}$-codes," *Des. Codes Cryptogr.*, vol. 86, pp. 1201–1209, Jun. 2018.
[37] M. Shi, R. Wu, and D. S. Krotov, "On $\mathbb{Z}_p\mathbb{Z}_{p^k}$-additive codes and their duality," *IEEE Trans. Inf. Theory*, vol. 65, no. 6, pp. 3841–3847, Jan. 2019.
[38] A. Torres-Martín and M. Villanueva, "Systematic encoding and permutation decoding for $\mathbb{Z}_{p^s}$-linear codes," *IEEE Trans. Inf. Theory*, vol. 68, no. 7, pp. 4435–4443, Jul. 2022.
[39] A. Torres-Martín and M. Villanueva, "Partial permutation decoding and PD-sets for $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes," *Finite Fields Their Appl.*, vol. 93, Jan. 2024, Art. no. 102316.
[40] Z.-X. Wan, *Lectures on Finite Fields and Galois Rings*. Singapore: World Scientific, 2003.

Josep Rifà (Life Senior Member, IEEE) was born in Manlleu, Catalonia, Spain, in July 1951. He received the degree in sciences (mathematical section) from the University of Barcelona in 1973 and the Ph.D. degree in sciences (computer sciences section) from the Autonomous University of Barcelona (UAB) in 1987. In 1974, he was an Assistant Professor with the Mathematics Department, Barcelona University. In 1987, he joined UAB and since 1992, he has been a Full Professor with UAB. He was the Former Head of the Information and Communications Engineering Department, UAB. Currently, he is a Professor Emeritus with UAB. He has worked on several projects for Spanish CICYT and other organizations on subjects related to digital communications, error-correcting codes, and encryption of digital information. His research interests include information theory, coding theory, and cryptography. He was the Former Vice-Chairperson of the Spanish Chapter of Information Theory of IEEE.

Adrián Torres-Martín was born in Sabadell, Catalonia, in December 1996. He received the dual B.Sc. degree in mathematics and in physics from Universitat Autònoma de Barcelona in 2019 and the M.Sc. degree in fundamental principles of data science from Universitat de Barcelona in 2021. He is currently pursuing the Ph.D. degree with the Computer Science Program. In 2021, he joined the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, as a Research Support Technician. His research interests include subjects related to algebra, coding theory, machine learning, and artificial intelligence.

Mercè Villanueva was born in Roses, Catalonia, in January 1972. She received the B.Sc. degree in mathematics, the M.Sc. degree in computer science, and the Ph.D. degree in science (computer science section) from Universitat Autònoma de Barcelona in 1994, 1996, and 2001, respectively. In 1994, she joined the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, as an Assistant Professor. She was promoted to an Associate Professor in 2002 and became a Full Professor in 2023. Her research interests include subjects related to combinatorics, algebra, coding theory, and graph theory.