

This is the **accepted version** of the journal article:

Dougherty, Steven T.; Rifà i Coma, Josep; Villanueva, M. «Rank and kernel of additive generalised Hadamard codes». IEEE Transactions on Information Theory, Vol. 67, Issue 11 (November 2021), p. 7210-7220. DOI 10.1109/TIT.2021.3100433

This version is available at <https://ddd.uab.cat/record/249135>

under the terms of the  ^{IN}
COPYRIGHT license

Rank and Kernel of Additive Generalised Hadamard Codes

Steven T. Dougherty, Josep Rifà, *Senior Member, IEEE*, and Mercè Villanueva

Abstract—A subset of a vector space \mathbb{F}_q^n is additive if it is a linear space over the field \mathbb{F}_p , where $q = p^e$, p prime, and $e > 1$. Bounds on the rank and dimension of the kernel of additive generalised Hadamard (additive GH) codes are established. For specific ranks and dimensions of the kernel within these bounds, additive GH codes are constructed. Moreover, for the case $e = 2$, it is shown that the given bounds are tight and it is possible to construct an additive GH code for all allowable ranks and dimensions of the kernel between these bounds. Finally, we also prove that these codes are self-orthogonal with respect to the trace Hermitian inner product, and generate pure quantum codes.

Index Terms—Additive code, generalised Hadamard code, generalised Hadamard matrix, kernel, nonlinear code, rank.

I. INTRODUCTION

LET $\mathbb{F}_q = \text{GF}(q)$ denote the finite field with q elements, where $q = p^e$, p prime. Let \mathbb{F}_q^n be the vector space of dimension n over \mathbb{F}_q . The *Hamming distance* between vectors $\mathbf{w}, \mathbf{v} \in \mathbb{F}_q^n$, denoted by $d(\mathbf{w}, \mathbf{v})$, is the number of coordinates in which \mathbf{w} and \mathbf{v} differ. A *code* C over \mathbb{F}_q of length n is a nonempty subset of \mathbb{F}_q^n . The elements of C are called *codewords*. The *minimum distance* of a code is the smallest Hamming distance between any pair of distinct codewords. A code C over \mathbb{F}_q is called *linear* if it is a linear space over \mathbb{F}_q and, it is called *additive* if it is linear over the prime field \mathbb{F}_p . An additive code C over \mathbb{F}_q has a dimension k' as a linear space over \mathbb{F}_p and we can write $|C| = p^{k'} = q^k$, where $k' = ke$. The dimension of an additive code C over \mathbb{F}_q is defined as the number k , which is not necessarily an integer number.

Two codes $C_1, C_2 \subset \mathbb{F}_q^n$ are said to be *permutation equivalent* if there exists a permutation σ of the n coordinates such that $C_2 = \{\sigma(c_1, c_2, \dots, c_n) = (c_{\sigma^{-1}(1)}, \dots, c_{\sigma^{-1}(n)}) : (c_1, c_2, \dots, c_n) \in C_1\}$. Without loss of generality, we shall assume, unless stated otherwise, that the all-zero vector, denoted by $\mathbf{0}$, is in C .

Two structural parameters of (nonlinear) codes are the dimension of the linear span and the kernel. The *linear span* of a code C over \mathbb{F}_q , denoted by $\mathcal{R}(C)$, is the subspace over \mathbb{F}_q spanned by C , that is $\mathcal{R}(C) = \langle C \rangle$. The dimension of $\mathcal{R}(C)$

is called the *rank* of C and is denoted by $\text{rank}(C)$. If $q = p^e$, p prime, we can also define $\mathcal{R}_p(C)$ and $\text{rank}_p(C)$ as the additive code spanned by C and its dimension, respectively. The *kernel* of a code C over \mathbb{F}_q , denoted by $\mathcal{K}(C)$, is defined as $\mathcal{K}(C) = \{\mathbf{x} \in \mathbb{F}_q^n : \alpha\mathbf{x} + C = C \text{ for all } \alpha \in \mathbb{F}_q\}$. If $q = p^e$, p prime, we can also define the *p-kernel* of C as $\mathcal{K}_p(C) = \{\mathbf{x} \in \mathbb{F}_q^n : \mathbf{x} + C = C\}$. Since we assume that $\mathbf{0} \in C$, then $\mathcal{K}(C)$ is a linear subcode of C and $\mathcal{K}_p(C)$ is an additive subcode. We denote the dimension of the kernel (resp., *p-kernel*) of C by $\ker(C)$ (resp., $\ker_p(C)$). These concepts were first defined in [17] for codes over \mathbb{F}_q , generalising the binary case described previously in [2], [16]. In [17], it was proved that any code C over \mathbb{F}_q can be written as the union of cosets of $\mathcal{K}(C)$ (resp., $\mathcal{K}_p(C)$), and $\mathcal{K}(C)$ (resp., $\mathcal{K}_p(C)$) is the largest such linear code over \mathbb{F}_q (resp., \mathbb{F}_p) for which this is true. Moreover, it is clear that $\mathcal{K}(C) \subseteq \mathcal{K}_p(C)$.

A *generalised Hadamard* (GH) matrix $H(q, \lambda) = (h_{ij})$ of order $n = q\lambda$ over \mathbb{F}_q is a $q\lambda \times q\lambda$ matrix with entries from \mathbb{F}_q with the property that for every i, j , $1 \leq i < j \leq q\lambda$, each of the multisets $\{h_{is} - h_{js} : 1 \leq s \leq q\lambda\}$ contains every element of \mathbb{F}_q exactly λ times. It is known that since $(\mathbb{F}_q, +)$ is an abelian group then $H(q, \lambda)^T$ is also a GH matrix, where $H(q, \lambda)^T$ denotes the transpose of $H(q, \lambda)$ [11]. An ordinary Hadamard matrix of order 4μ corresponds to a GH matrix $H(2, \lambda)$ over \mathbb{F}_2 , where $\lambda = 2\mu$.

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{F}_q 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 and we obtain an equivalent GH matrix which is called *normalized*. From a normalized GH matrix H , we denote by F_H the code over \mathbb{F}_q consisting of the rows of H , and C_H the one defined as $C_H = \bigcup_{\alpha \in \mathbb{F}_q} (F_H + \alpha\mathbf{1})$, where $F_H + \alpha\mathbf{1} = \{\mathbf{h} + \alpha\mathbf{1} : \mathbf{h} \in F_H\}$ and $\mathbf{1}$ denotes the all-one vector. The code C_H over \mathbb{F}_q is called *generalised Hadamard* (GH) *code*. Note that F_H and C_H are generally nonlinear codes over \mathbb{F}_q .

To check whether two normalized GH matrices are equivalent is known to be an NP-hard problem [15]. However, we can use the invariants related to the linear span and kernel of the corresponding GH codes in order to help in their classification, since if two GH codes have different ranks or dimensions of the kernel, the normalized GH matrices are nonequivalent. Given a normalized GH matrix H , to establish the rank and dimension of the kernel of the corresponding code F_H is the

Steven T. Dougherty is with the Department of Mathematics, University of Scranton, Scranton PA 18510, USA

Josep Rifà and Mercè Villanueva are with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193 Cerdanyola del Vallès, Spain.

The material in this paper was presented in part at the 2020 IEEE International Symposium on Information Theory in Los Angeles, California, USA, 2020 [9].

Copyright (c) 2021 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

same as to establish these values for the code C_H , since

$$\begin{aligned} \text{rank}(C_H) &= \text{rank}(F_H) + 1 \quad \text{and} \\ \ker(C_H) &= \ker(F_H) + 1 \end{aligned} \quad (1)$$

by [8, Lemma 1]. In this paper, we focus on the codes C_H , although everything could be rewritten in terms of the codes F_H . It is important to emphasise that this is true as long as the GH matrix H is normalized.

The rank and dimension of the kernel for ordinary Hadamard codes over \mathbb{F}_2 have already been studied. Specifically, lower and upper bounds for these two parameters were established, and the construction of an Hadamard code for all allowable ranks and dimensions of the kernel between these bounds was given [18], [19]. The values of the rank and dimension of the kernel for $\mathbb{Z}_2\mathbb{Z}_4$ -linear Hadamard codes were given in [20], and these invariants for \mathbb{Z}_{2^s} -linear Hadamard codes have been studied in [6], [7]. The $\mathbb{Z}_2\mathbb{Z}_4$ -linear Hadamard codes (resp. \mathbb{Z}_{2^s} -linear Hadamard codes) are the Hadamard codes over \mathbb{F}_2 obtained as the Gray map image of $\mathbb{Z}_2\mathbb{Z}_4$ -additive codes (resp. \mathbb{Z}_{2^s} -additive codes), which are subgroups of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ (resp. $\mathbb{Z}_{2^s}^\beta$).

Some of the results on the rank and dimension of the kernel for Hadamard codes over \mathbb{F}_2 have been generalised to GH codes over \mathbb{F}_q with $q \neq 2$ [8]. Specifically, some lower and upper bounds for the dimension of the kernel, and for the rank once the dimension of the kernel is fixed, were given. Moreover constructions of GH codes having different values for these invariants within these bounds, were presented. In this paper, we continue studying the rank and dimension of the kernel for GH codes over \mathbb{F}_q . However, now we focus on a specific family of GH codes, namely the *additive GH codes*, that is, additive codes over \mathbb{F}_q obtained from GH matrices $H(q, \lambda)$. In the specific case $q = p^2$ we use the additive GH codes over \mathbb{F}_q to generate pure quantum codes. It is worth mentioning that the invariants rank and dimension of the kernel, used in this paper for additive GH codes, could be extended to classify more general additive or quantum codes.

The paper is organized as follows. In Section II, lower and upper bounds on the dimension of the kernel, and the rank once the dimension of the kernel is fixed, are given. In Sections III and IV, several constructions of additive GH codes over \mathbb{F}_q with $q = p^e$, p prime and $e > 1$, are shown. In Section V, by using these constructions, we establish for which allowable pairs (r, k) , where r is the rank and k the dimension of the kernel, there exists an additive GH code having these invariants. Finally, in Section VI, we see that the additive GH codes over \mathbb{F}_{p^2} can be used to generate pure quantum codes since they are self-orthogonal with respect to the trace Hermitian inner product.

II. BOUNDS ON THE RANK AND DIMENSION OF THE KERNEL

In this section, we state new results on the rank and dimension of the kernel for additive generalised Hadamard codes. Note that a GH matrix $H(p, \lambda)$ over \mathbb{F}_p , p prime, generates an additive GH code C_H of length $n = \lambda p = p^t$ if and only if $\text{rank}(C_H) = \text{rank}_p(C_H) = \ker_p(C_H) = \ker(C_H) = 1 + t$.

Therefore, we focus on additive GH codes over \mathbb{F}_q with $q = p^e$, $e > 1$.

Proposition II.1. [8, Proposition 9] *Let $H(q, \lambda)$ be a GH matrix over \mathbb{F}_q , where $q = p^e$, p prime, and $e \geq 1$. Let $n = q\lambda = p^t s$ such that $\gcd(p, s) = 1$. Then $1 \leq \ker(C_H) \leq \ker_p(C_H) \leq 1 + t/e$.*

Lemma II.2. [8, Lemma 16] *Let C_H be a GH code of length $n = q^h s$ over \mathbb{F}_q , where $s \neq 1$ and s is not a multiple of q . Then $\ker(C_H) \leq h$.*

Lemma II.3. *Let $H(q, \lambda)$ be a GH matrix over \mathbb{F}_q such that C_H is additive. Let $n = q\lambda = p^t s$ such that $\gcd(p, s) = 1$, where $q = p^e$, p prime, and $e \geq 1$. For any $v \in C_H$, $v \in \mathcal{K}(C_H)$ if and only if $\mu v \in C_H$ for all $\mu \in \mathbb{F}_q$.*

Proof. Assume that $\mu v \in C_H$ for all $\mu \in \mathbb{F}_q$. Since C_H is additive, for any $w \in C_H$ we have that $\mu v + w \in C_H$. Hence, the statement follows. \square

Proposition II.4. *Let $H(q, \lambda)$ be a GH matrix over \mathbb{F}_q , where $q = p^e$, p prime, and $e > 1$. Let $n = q\lambda = p^t s$ such that $\gcd(p, s) = 1$. Then*

- (i) *If C_H is an additive code, then $s = 1$.*
- (ii) *The code C_H is an additive code if and only if*

$$\text{rank}_p(C_H) = \ker_p(C_H) = 1 + t/e.$$

- (iii) *If C_H is an additive code and $\ker(C_H) = k$, then*

$$\frac{e + t - k}{e - 1} \leq \text{rank}(C_H) \leq 1 + t - (e - 1)(k - 1).$$

- (iv) *If C_H is an additive code, then $\text{rank}(C_H) = \ker(C_H) = 1 + t/e$ when C_H is linear over \mathbb{F}_q (t is a multiple of e), or otherwise*

$$1 \leq \ker(C_H) \leq \lfloor t/e \rfloor.$$

Proof. Since the number of codewords is $|C_H| = qn = p^{e+t}s$, if C_H is additive, then we have that $s = 1$ and $\text{rank}_p(C_H) = \ker_p(C_H) = 1 + t/e$. This proves items (i) and (ii).

Let C_H be an additive code with $\ker(C_H) = k$. The kernel $\mathcal{K}(C_H)$ is the largest linear subspace over \mathbb{F}_q in C_H such that C_H can be partitioned into cosets of $\mathcal{K}(C_H)$. Specifically, there are $|C_H|/q^k = q^{1+t/e}/q^k = q^{1+t/e-k} = p^{e+t-ek}$ cosets. Since C_H and $\mathcal{K}(C_H)$ are linear over \mathbb{F}_p , the above cosets (that is, the elements of the quotient $C_H/\mathcal{K}(C_H)$) have a linear structure over \mathbb{F}_p . Therefore, there are $e + t - ek$ independent vectors over \mathbb{F}_p generating these cosets, which means that the number of independent vectors over \mathbb{F}_q generating these cosets is upper bounded by $e + t - ek$. Hence $\text{rank}(C_H) \leq k + (e + t - ek) = 1 + t - (e - 1)(k - 1)$. From Lemma II.3, for any $v \notin \mathcal{K}(C_H)$, the intersection of the linear space over \mathbb{F}_q generated by v and C_H is, at most, of dimension $e - 1$ over \mathbb{F}_p . Therefore, for the lower bound, we have that $\frac{e+t-ek}{e-1} + k = \frac{e+t-k}{e-1} \leq \text{rank}(C_H)$ and item (iii) follows.

For item (iv), when C_H is linear over \mathbb{F}_q , we have that $C_H = \mathcal{K}(C_H)$. Since $|C_H| = p^{e+t} = q^{1+t/e}$, t is a multiple of e and $\text{rank}(C_H) = k = 1 + t/e$. Otherwise, $1 \leq k < 1 + t/e$ by Proposition II.1 and item (ii). In this case, if t is a multiple of e , clearly $k \leq \lfloor t/e \rfloor$. Finally, if t is not a multiple of e , by

Lemma II.2, since $n = q^{\lfloor t/e \rfloor} p^{s'}$, where $1 < p^{s'} < q$, we have that $k \leq \lfloor t/e \rfloor$. \square

Corollary II.5. *Let $H(q, \lambda)$ be a GH matrix over \mathbb{F}_q , where $q = p^2$ and p prime. If C_H is an additive code of length $n = q\lambda = p^t$, then*

- (i) $\text{rank}(C_H) + \ker(C_H) = 2 + t$.
- (ii) If $2 \nmid t$, then $\text{rank}(C_H) - \ker(C_H) \geq 3$.
- (iii) If $2 \mid t$ and C_H is nonlinear over \mathbb{F}_q , then $\text{rank}(C_H) - \ker(C_H) \geq 2$.

Proof. The first item is straightforward from item (iii) in Proposition II.4.

For the second item, if $2 = e \nmid t$, then $t = 2h + 1$. From item (iv) in Proposition II.4, $\ker(C_H) \leq h$ and so $\text{rank}(C_H) - \ker(C_H) \geq \text{rank}(C_H) - h = 2 + t - \ker(C_H) - h \geq 2 + t - 2h = 3$. For the third item, we can follow a similar argument, but considering that $t = 2h$. \square

Example II.6. For $q = p^3$, the second column in Table I gives all possible values for the dimension of the kernel of additive GH codes over \mathbb{F}_{p^3} of length $n = p^t$ with $2 \leq t \leq 12$. For each one of these values, the third column shows the possible values for the rank, given by Proposition II.4. \triangle

TABLE I
PARAMETERS $\ker(C_H)$ AND $\text{rank}(C_H)$ FOR ALL ADDITIVE GH CODES C_H OVER \mathbb{F}_{p^3} OF LENGTH $n = p^t$ WITH $3 \leq t \leq 12$.

t	$\ker(C_H)$	$\text{rank}(C_H)$	$\ker_p(C_H) = \text{rank}_p(C_H)$
3	2	2	2
	1	3,4	2
4	1	3,4,5	7/3
5	1	4,5,6	8/3
6	3	3	3
	2	4,5	3
	1	4,5,6,7	3
7	2	4,5,6	10/3
	1	5,6,7,8	10/3
8	2	5,6,7	11/3
	1	5,6,7,8,9	11/3
9	4	4	4
	3	5,6	4
	2	5,6,7,8	4
	1	6,7,8,9,10	4
10	3	5,6,7	13/3
	2	6,7,8,9	13/3
	1	6,7,8,9,10,11	13/3
11	3	6,7,8	14/3
	2	6,7,8,9,10	14/3
	1	7,8,9,10,11,12	14/3
12	5	5	5
	4	6,7	5
	3	6,7,8,9	5
	2	7,8,9,10,11	5
	1	7,8,9,10,11,12,13	5

III. KRONECKER AND SWITCHING CONSTRUCTIONS

In this section, we show that by using the Kronecker sum construction from additive GH codes, we also obtain additive GH codes. Moreover, we present a switching construction that allows for the production of additive GH codes. For all

these constructions, we establish the values of the rank and dimension of the kernel for the obtained codes.

A standard method to construct GH matrices from other GH matrices is given by the *Kronecker sum construction* [14], [23]. That is, if $H(q, \lambda) = (h_{ij})$ is any $q\lambda \times q\lambda$ GH matrix over \mathbb{F}_q , and $B_1, B_2, \dots, B_{q\lambda}$ are any $q\mu \times q\mu$ GH matrices over \mathbb{F}_q , then the matrix in Table II gives a $q^2\lambda\mu \times q^2\lambda\mu$ GH matrix over \mathbb{F}_q , denoted by $H \oplus [B_1, B_2, \dots, B_n]$, where $n = q\lambda$. If $B_1 = B_2 = \dots = B_n = B$, then we write $H \oplus [B_1, B_2, \dots, B_n] = H \oplus B$.

TABLE II
KRONECKER SUM CONSTRUCTION

$$H \oplus B = \begin{pmatrix} h_{11} + B_1 & h_{12} + B_1 & \cdots & h_{1n} + B_1 \\ h_{21} + B_2 & h_{22} + B_2 & \cdots & h_{2n} + B_2 \\ \vdots & \vdots & \ddots & \vdots \\ h_{n1} + B_n & h_{n2} + B_n & \cdots & h_{nn} + B_n \end{pmatrix}$$

Let S_q be the normalized GH matrix $H(q, 1)$ given by the multiplicative table of \mathbb{F}_q . As for ordinary Hadamard matrices over \mathbb{F}_2 , starting from a GH matrix $S^1 = S_q$, we can recursively define S^h as a GH matrix $H(q, q^{h-1})$, constructed as $S^h = S_q \oplus [S^{h-1}, S^{h-1}, \dots, S^{h-1}] = S_q \oplus S^{h-1}$ for $h > 1$, which is called a *Sylvester GH matrix*. Note that the corresponding GH code C_{S^h} is linear over \mathbb{F}_q , so $\text{rank}(C_{S^h}) = \ker(C_{S^h}) = 1 + h$, by Equation (1) or item (iv) of Proposition II.4.

Now, we recall some known results on the rank and dimension of the kernel for GH codes constructed by using the Kronecker sum construction. In these cases, starting with additive GH codes, we obtain additive GH codes.

Lemma III.1. *Let H_1 and H_2 be two GH matrices over \mathbb{F}_q and $H = H_1 \oplus H_2$. Then $\text{rank}(C_H) = \text{rank}(C_{H_1}) + \text{rank}(C_{H_2}) - 1$ and $\ker(C_H) = \ker(C_{H_1}) + \ker(C_{H_2}) - 1$. Moreover, if C_{H_1} and C_{H_2} are additive, then C_H is also additive and $\text{rank}_p(C_H) = \text{rank}_p(C_{H_1}) + \text{rank}_p(C_{H_2}) - 1$.*

Proof. Straightforward from the proof of Lemma 3 in [8]. \square

Corollary III.2. *Let B be a GH matrix over \mathbb{F}_q and $H = S_q \oplus B$. Then $\text{rank}(C_H) = \text{rank}(C_B) + 1$ and $\ker(C_H) = \ker(C_B) + 1$. Moreover, if C_B is additive, then C_H is also additive and $\text{rank}_p(C_H) = \text{rank}_p(C_B) + 1$.*

Proof. Straightforward from the proof of Corollary 4 in [8]. \square

Several switching constructions have been used to construct perfect codes in [21], [22] ordinary Hadamard codes over \mathbb{F}_2 in [18], [19], and generalised Hadamard codes over \mathbb{F}_q in [8]. In this paper, we present different constructions, based on this technique, in order to obtain additive GH codes with different ranks and dimensions of the kernel. The first switching construction, given by Proposition III.3, allows us to construct additive GH codes over \mathbb{F}_{p^e} of length $n = p^{2e}$ with kernel of dimension 2 and rank 4.

Proposition III.3 (Switching Construction I). *For $q = p^e$, p prime, and any $e > 1$, there exists a GH matrix $H(p^e, p^e)$ such*

that C_H is an additive code over \mathbb{F}_{p^e} of length $n = p^{2e} = q^2$ with $\ker(C_H) = 2$ and $\text{rank}(C_H) = 4$.

Proof. Let $\mathbf{0}, \mathbf{1}, \omega^{(1)}, \dots, \omega^{(q-2)}$ be the elements $0, 1, \omega, \dots, \omega^{q-2}$ repeated q times, respectively, where ω is a primitive element in \mathbb{F}_q . Let $S^2 = S_q \oplus S_q$ be the Sylvester GH matrix $H(q, q)$. We can assume without loss of generality that S^2 is generated over \mathbb{F}_q by the row vectors \mathbf{v}_1 and \mathbf{v}_2 of length $n = q^2$, where

$$\mathbf{v}_1 = (0, 1, \omega^1, \dots, \omega^{q-2}, \dots, 0, 1, \omega^1, \dots, \omega^{q-2}), \text{ and}$$

$$\mathbf{v}_2 = (\mathbf{0}, \mathbf{1}, \omega^{(1)}, \dots, \omega^{(q-2)}).$$

Let K be the linear subcode of S^2 generated by the row vector \mathbf{v}_2 . The rows of S^2 can be partitioned into q cosets of K , that is, $S^2 = \cup_{\beta \in \mathbb{F}_q} (K + \beta \mathbf{v}_1)$. Let $\beta_e \in \mathbb{F}_p$ be the last coordinate of the element $\beta \in \mathbb{F}_q$ represented as a vector from \mathbb{F}_p^e . Then we construct the matrix

$$H = (S^2 \setminus \bigcup_{\substack{\beta \in \mathbb{F}_q, \\ \beta_e \neq 0}} (K + \beta \mathbf{v}_1)) \cup \bigcup_{\substack{\beta \in \mathbb{F}_q, \\ \beta_e = 0}} (K + \beta \mathbf{v}_1 + \beta_e \mathbf{g}) = \bigcup_{\beta \in \mathbb{F}_q} K_\beta,$$

where $\mathbf{g} = (0, \dots, 0, 0, 1, \omega^1, \dots, \omega^{q-2})$ and $K_\beta = K + \beta \mathbf{v}_1 + \beta_e \mathbf{g}$.

It is easy to see that H is a GH matrix and C_H is an additive code. Indeed, note that $K_\beta + K_\gamma = K_{\beta+\gamma}$ for all $\beta, \gamma \in \mathbb{F}_q$. Moreover, clearly, $\text{rank}(F_H) = 2 + 1 = 3$ and $K \subseteq \mathcal{K}(F_H)$. It is also easy to prove that $K = \mathcal{K}(F_H)$. Therefore, $\ker(F_H) = 1$. By Equation (1), $\ker(C_H) = 2$ and $\text{rank}(C_H) = 4$. \square

Example III.4. We construct a GH matrix $H(2^2, 2^2)$ such that C_H is an additive code over \mathbb{F}_{2^2} of length $n = 2^4$ with $\ker(C_H) = 2$ and $\text{rank}(C_H) = 4$. We start with the GH matrix $S^2 = S_4 \oplus S_4$, which is linear over \mathbb{F}_{2^2} and is generated by $\mathbf{v}_1 = (0, 1, \omega, \omega^2, 0, 1, \omega, \omega^2, 0, 1, \omega, \omega^2)$ and $\mathbf{v}_2 = (0, 0, 0, 0, 1, 1, 1, 1, \omega, \omega, \omega, \omega^2, \omega^2, \omega^2, \omega^2)$, where ω is a primitive element in \mathbb{F}_{2^2} and $\omega^2 = \omega + 1$. Let $K = \langle \mathbf{v}_2 \rangle$. Then, $S^2 = K \cup (K + \mathbf{v}_1) \cup (K + \omega \mathbf{v}_1) \cup (K + \omega^2 \mathbf{v}_1)$. By the proof of Proposition III.3, we change the last eight rows of S^2 , and we obtain the GH matrix $H(2^2, 2^2) = K \cup (K + \mathbf{v}_1) \cup (K + \omega \mathbf{v}_1 + \mathbf{g}) \cup (K + \omega^2 \mathbf{v}_1 + \mathbf{g})$, where $\mathbf{g} = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, \omega, \omega^2)$, that is, the matrix given in Table III. \triangle

The switching construction given by Proposition III.3 can be generalised to the case $H(p^e, p^{(h-1)e})$ with $h > 1$, that is, when t is a multiple of e . A first generalisation is shown in Proposition III.5, and a second one in Proposition III.6.

Proposition III.5 (Switching Construction II). *For $q = p^e$, p prime, and any $e > 1$, $h > 1$, there exists a GH matrix $H(p^e, p^{(h-1)e})$ such that C_H is an additive code over \mathbb{F}_{p^e} of length $n = p^{he} = q^h$ with $\ker(C_H) = h$ and $\text{rank}(C_H) = r$ for all $r \in \{h+2, \dots, h+e\}$.*

Proof. Let S^h be the Sylvester GH matrix $H(q, q^{h-1})$. We can assume without loss of generality that S^h is generated by the vectors $\mathbf{v}_1, \dots, \mathbf{v}_h$ of length $n = q^h$, where

$$\mathbf{v}_i = (\mathbf{0}_i, \mathbf{1}_i, \omega_i^{(1)}, \dots, \omega_i^{(q-2)}, \dots, \mathbf{0}_i, \mathbf{1}_i, \omega_i^{(1)}, \dots, \omega_i^{(q-2)}),$$

$\mathbf{0}_i, \mathbf{1}_i, \omega_i^{(1)}, \dots, \omega_i^{(q-2)}$ are the elements $0, 1, \omega, \dots, \omega^{q-2}$ repeated q^{i-1} times, respectively, and ω is a primitive element in \mathbb{F}_q , for all $i \in \{1, \dots, h\}$. All vectors $\mathbf{v}_1, \dots, \mathbf{v}_h$ have length q^h and are linearly independent over \mathbb{F}_q . The corresponding GH code C_{S^h} is linear over \mathbb{F}_q , so $\text{rank}(C_{S^h}) = \ker(C_{S^h}) = 1 + h$.

Let K be the linear subcode of S^h generated by the vectors $\mathbf{v}_2, \dots, \mathbf{v}_h$. Note that all $n = q^h$ coordinates are naturally divided into q^{h-1} groups of size q , which will be referred to as blocks, such that the columns of K in a block coincide. Moreover, the rows of S^h can be partitioned into q cosets of K , that is, $S^h = \cup_{\beta \in \mathbb{F}_q} (K + \beta \mathbf{v}_1)$.

Now, consider the vectors $\mathbf{g}_1, \dots, \mathbf{g}_{e-1} \in \mathbb{F}_q^n$, where \mathbf{g}_j has exactly the values $0, 1, \omega, \dots, \omega^{q-2}$ in the coordinate positions $(jq+1), \dots, (j+1)q$, respectively, and zeros elsewhere, for all $j \in \{1, \dots, e-1\}$. Note that, for each $j \in \{1, \dots, e-1\}$, these q coordinate positions correspond to a block. Moreover, there are always enough blocks since $e \leq q \leq q^{h-1} = p^{e(h-1)}$. Let $\beta \in \mathbb{F}_q$ be $\beta = (\beta_0, \dots, \beta_{e-1})$ represented as a vector in \mathbb{F}_p^e . Then, we construct the matrix

$$H^{(s)} = \bigcup_{\beta \in \mathbb{F}_q} K_\beta, \quad (2)$$

where $s \in \{1, \dots, e-1\}$ and $K_\beta = K + \beta \mathbf{v}_1 + \sum_{j=1}^s \beta_j \mathbf{g}_j$.

Next, we prove that the corresponding code $C_{H^{(s)}}$ is an additive GH code for all $s \in \{1, \dots, e-1\}$. First of all, the length of $H^{(s)}$ is q^h and the number of rows is also q^h . The code $C_{H^{(s)}}$ is additive over \mathbb{F}_q , since $K_{\beta+\gamma} = K_\beta + K_\gamma$ for any $\beta, \gamma \in \mathbb{F}_q$. Finally, it can be seen easily that $H^{(s)}$ is a GH matrix by computing the differences between any two different rows. \square

By Lemma II.3, it is straightforward to show that $\mathcal{K}(H^{(s)}) = K$, so we have that $\ker(C_{H^{(s)}}) = h - 1 + 1 = h$ by Equation (1). It is easy to see that all linearly independent vectors $\mathbf{v}_1, \dots, \mathbf{v}_h$ from S^h are in $\langle C_{H^{(s)}} \rangle$. Moreover, the linearly independent vectors $\mathbf{g}_1, \dots, \mathbf{g}_s$ are also in $\langle C_{H^{(s)}} \rangle$. Hence, by Equation (1), $\text{rank}(C_{H^{(s)}}) = h + s + 1$, which covers all values in the range of $h+2$ to $h+e$. \square

We can make a slight modification in the proof of Proposition III.5 allowing the construction of GH matrices $H(p^e, p^{(h-1)e})$ with $h > 1$, where the dimension of the kernel k of the corresponding codes ranges from 2 to h and for each one of these values the rank takes any value from $2h-k+2$ to $h+1+(h-k+1)(e-1)$. Note that this switching construction includes the previous two switching constructions I and II given by Proposition III.3 and Proposition III.5, respectively.

Proposition III.6 (Switching Construction III). *For $q = p^e$, p prime, and any $e > 1$, $h > 1$, there exists a GH matrix $H(p^e, p^{(h-1)e})$ such that C_H is an additive code over \mathbb{F}_{p^e} of length $n = p^{he} = q^h$ with $\ker(C_H) = k$ and $\text{rank}(C_H) = r$, for all $k \in \{2, \dots, h\}$ and*

$$r \in \{2h - k + 2, \dots, 1 + t - (e-1)(k-1)\}.$$

Proof. We consider the vectors $\mathbf{v}_1, \dots, \mathbf{v}_h$ of length $n = q^h$ defined in the proof of Proposition III.5. Let K be the linear subcode of S^h generated by the vectors $\mathbf{v}_3, \dots, \mathbf{v}_h$. In this case, the rows of S^h can be partitioned into q^2 cosets of

TABLE III
THE GH MATRIX $H(2^2, 2^2)$ CONSTRUCTED IN EXAMPLE III.4

$$\left(\begin{array}{cccccccccccccccc}
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \omega & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 & \omega^2 \\
 0 & 0 & 0 & 0 & \omega & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 & \omega^2 & 1 & 1 & 1 & 1 \\
 0 & 0 & 0 & 0 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & 1 & 1 & 1 & 1 & \omega & \omega & \omega & \omega \\
 0 & 1 & \omega & \omega^2 & 0 & 1 & \omega & \omega^2 & 0 & 1 & \omega & \omega^2 & 0 & 1 & \omega & \omega^2 \\
 0 & 1 & \omega & \omega^2 & 1 & 0 & \omega^2 & \omega & \omega & \omega^2 & 0 & 1 & \omega^2 & \omega & 1 & 0 \\
 0 & 1 & \omega & \omega^2 & \omega & \omega^2 & 0 & 1 & \omega^2 & \omega & 1 & 0 & 1 & 0 & \omega^2 & \omega \\
 0 & 1 & \omega & \omega^2 & \omega^2 & \omega & 1 & 0 & 1 & 0 & \omega^2 & \omega & \omega & \omega^2 & 0 & 1 \\
 0 & \omega & \omega^2 & 1 & 0 & \omega & \omega^2 & 1 & 0 & \omega & \omega^2 & 1 & 0 & \omega^2 & 1 & \omega \\
 0 & \omega & \omega^2 & 1 & 1 & \omega^2 & \omega & 0 & \omega & 0 & 1 & \omega^2 & \omega^2 & 0 & \omega & 1 \\
 0 & \omega & \omega^2 & 1 & \omega & 0 & 1 & \omega^2 & \omega^2 & 1 & 0 & \omega & 1 & \omega & 0 & \omega^2 \\
 0 & \omega & \omega^2 & 1 & \omega^2 & 1 & 0 & \omega & 1 & \omega^2 & \omega & 0 & \omega & 1 & \omega^2 & 0 \\
 0 & \omega^2 & 1 & \omega & 0 & \omega^2 & 1 & \omega & 0 & \omega^2 & 1 & \omega & 0 & \omega & \omega^2 & 1 \\
 0 & \omega^2 & 1 & \omega & 1 & \omega & 0 & \omega^2 & \omega & 1 & \omega^2 & 0 & \omega^2 & 1 & 0 & \omega \\
 0 & \omega^2 & 1 & \omega & \omega & 1 & \omega^2 & 0 & \omega^2 & 0 & \omega & 1 & 1 & \omega^2 & \omega & 0 \\
 0 & \omega^2 & 1 & \omega & \omega^2 & 0 & \omega & 1 & 1 & \omega & 0 & \omega^2 & \omega & 1 & \omega^2 & \omega
 \end{array} \right) \left\{ \begin{array}{l} K \\ K + \mathbf{v}_1 \\ K + \omega \mathbf{v}_1 + \mathbf{g} \\ K + \omega^2 \mathbf{v}_1 + \mathbf{g} \end{array} \right.$$

K , that is, $S^h = \cup_{\beta, \gamma \in \mathbb{F}_q} (K + \beta \mathbf{v}_1 + \gamma \mathbf{v}_2)$. Let $\beta, \gamma \in \mathbb{F}_q$ be $\beta = (\beta_0, \dots, \beta_{e-1})$ and $\gamma = (\gamma_0, \dots, \gamma_{e-1})$, respectively, represented as vectors in \mathbb{F}_p^e . Then, we construct the matrix

$$H^{(s_1, s_2)} = \bigcup_{\beta, \gamma \in \mathbb{F}_q} K_{\beta, \gamma}, \quad (3)$$

where $s_1, s_2 \in \{1, \dots, e-1\}$, $K_{\beta, \gamma} = K + \beta \mathbf{v}_1 + \sum_{j=1}^{s_1} \beta_j \mathbf{g}_j^{(1)} + \gamma \mathbf{v}_2 + \sum_{j=1}^{s_2} \gamma_j \mathbf{g}_j^{(2)}$. We take the vector $\mathbf{g}_j^{(1)} = \mathbf{g}_j$ defined as in the proof of Proposition III.5 for $j \in \{1, \dots, e-1\}$. The vector $\mathbf{g}_j^{(2)}$ has exactly the values $\mathbf{0}_2, \mathbf{1}_2, \omega_2^{(1)}, \dots, \omega_2^{(q-2)}$ in the coordinate positions $(jq^2+1), \dots, (j+1)q^2$, respectively, and zeros elsewhere, for all $j \in \{1, \dots, e-1\}$.

We can repeat again and again the above construction taking in the z -th round vectors $\mathbf{g}_j^{(z)}$ with exactly the values $\mathbf{0}_z, \mathbf{1}_z, \omega_z^{(1)}, \dots, \omega_z^{(q-2)}$ in the coordinate positions $(jq^z+1), \dots, (j+1)q^z$, respectively, and zeros elsewhere, for all $j \in \{1, \dots, e-1\}$. Again, there are always enough coordinates since $e \leq q = p^e$. We can follow this process until we consider the linear subcode $K = \langle \mathbf{v}_h \rangle$, and we obtain the matrix $H^{(s_1, s_2, \dots, s_{h-1})}$.

Next, we prove that the matrix $H = H^{(s_1, s_2, \dots, s_{h-k+1})}$ is a GH matrix, and the corresponding code is additive. First of all, the length and the number of rows of H is q^h . The corresponding code C_H is an additive code over \mathbb{F}_q as in the proof of Proposition III.5. Finally, it can be easily seen that H is a GH matrix by computing the differences between any two different rows.

Again, by Lemma II.3, it is easy to see that $\mathcal{K}(H) = K$, so we have that $\ker(C_H) = h - (h - k + 2) + 1 = k - 1 + 1 = k$ by Equation (1). For the $\text{rank}(C_H)$, it is easy to see that all linearly independent vectors in C_{S^h} are also in $\langle C_H \rangle$. Apart from that vectors, we also find in $\langle C_H \rangle$ the linearly independent vectors $\mathbf{g}_1^{(1)}, \dots, \mathbf{g}_{s_1}^{(1)}, \dots, \mathbf{g}_1^{(h-k+1)}, \dots, \mathbf{g}_{s_{h-k+1}}^{(h-k+1)}$. Hence, $\text{rank}(C_H) = h + 1 + s_1 + \dots + s_{h-k+1}$, which covers all values in the range from $h + 1 + (h - k + 1) = 2h - k + 2$ to $h + 1 + (h - k + 1)(e - 1) = 1 + t - (e - 1)(k - 1)$. \square

IV. NEW CONSTRUCTIONS WITH KERNEL OF DIMENSION 1

In this section, two new constructions of additive GH codes having a kernel of dimension 1, one with maximum rank and another one with minimum rank, are presented. In Section V, these constructions together with the Kronecker and switching constructions presented in Section III will be used to construct additive GH codes having different ranks and dimensions of the kernel.

First, we introduce a new construction of GH matrices which allows us to guarantee that the obtained code C_H of length $n = p^t$ is additive over \mathbb{F}_{p^e} , has kernel of minimum dimension 1 and maximum rank $t + 1$.

Proposition IV.1. *For $q = p^e$, p prime, and any $t > e > 1$, there exists a GH matrix $H(p^e, p^{t-e})$ such that C_H is an additive code over \mathbb{F}_{p^e} of length $n = p^t$ with $\ker(C_H) = 1$ and $\text{rank}(C_H) = t + 1$.*

Proof. Let $S_{p^t} = H(p^t, 1)$ be the GH matrix, given by the multiplicative table of \mathbb{F}_{p^t} , that is, the matrix

$$H(p^t, 1) = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & \omega & \dots & \omega^{p^t-3} & \omega^{p^t-2} \\ 0 & \omega & \omega^2 & \dots & \omega^{p^t-2} & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \omega^{p^t-2} & 1 & \dots & \omega^{p^t-4} & \omega^{p^t-3} \end{pmatrix}, \quad (4)$$

where ω is a primitive element in \mathbb{F}_{p^t} . Let $b_0 + b_1x + \dots + b_{t-1}x^{t-1} - x^t \in \mathbb{F}_p[x]$ be the primitive polynomial of ω and note that $b_0 \neq 0$. In this case, C_H is a linear code over \mathbb{F}_{p^t} and an additive code. By Proposition II.4, we have that $\text{rank}_p(C_H) = \ker_p(C_H) = \text{rank}(C_H) = \ker(C_H) = 2$.

Now, for any $e, 1 < e < t$, we consider the projection map from \mathbb{F}_{p^t} to \mathbb{F}_{p^e} given by

$$\mathbf{v} = (v_1, \dots, v_e, v_{e+1}, \dots, v_t) \in \mathbb{F}_{p^t} \longrightarrow \bar{\mathbf{v}} = (v_1, \dots, v_e) \in \mathbb{F}_{p^e}.$$

Note that we can consider that the projection of $\omega \in \mathbb{F}_{p^t}$ gives a primitive element $\bar{\omega} = \alpha \in \mathbb{F}_{p^e}$. Let H_e be the matrix obtained from H after changing each entry \mathbf{v} by $\bar{\mathbf{v}}$. Since in any row of H there are all the elements in \mathbb{F}_{p^t} , it is easy

to see that in any row of H_e there will be all the elements in \mathbb{F}_{p^e} , but each one repeated p^{t-e} times. The same happens taking the difference of any two different rows in H . Hence, $H_e(p^e, p^{t-e})$ is a GH matrix. Since C_H is an additive code it is easy to see, by construction, that C_{H_e} is also an additive code.

Let $H_e^{(r)}$ be the matrix H_e after removing the first row and column. Take any row $\mathbf{v} = (\bar{\gamma}_1, \bar{\gamma}_2, \dots, \bar{\gamma}_{p^t-1})$ of $H_e^{(r)}$, where $\bar{\gamma}_i \in \mathbb{F}_{p^e}$ for all $i \in \{1, 2, \dots, p^t-1\}$. The case when entry $\bar{\gamma}_i$ is zero corresponds to $\gamma_i \in \mathbb{F}_{p^t}$ of the form $\gamma_i = \underbrace{(0, 0, \dots, 0)}_e, \lambda_{e+1}, \dots, \lambda_t)$, or equivalently, $\gamma_i = \lambda_{e+1}\omega^e + \dots + \lambda_t\omega^{t-1}$, where $\lambda_i \in \mathbb{F}_p$ for all $i \in \{e+1, e+2, \dots, t\}$. Now, we compute $\omega\gamma_i = \lambda_{e+1}\omega^{e+1} + \dots + \lambda_t\omega^{t-1} + \lambda_t\omega^t$ and from $\omega^t = b_0 + b_1\omega + \dots + b_{t-1}\omega^{t-1}$ we have $\overline{\omega\gamma_i} = \lambda_t(b_0 + b_1\alpha + \dots + b_{e-1}\alpha^{e-1})$. Hence, taking two consecutive entries in \mathbf{v} , for instance $\bar{\gamma}_i, \bar{\gamma}_{i+1} = \overline{\omega\gamma_i}$, such that $\bar{\gamma}_i = 0$ and $\bar{\gamma}_{i+1} \neq 0$ we have that $\bar{\gamma}_{i+1} = \lambda_t(b_0 + b_1\alpha + \dots + b_{e-1}\alpha^{e-1})$, for some nonzero $\lambda_t \in \mathbb{F}_p$. Therefore, multiplying any row of $H_e^{(r)}$ by α^j , for any $\alpha^j \notin \mathbb{F}_p$, we do not obtain a row of $H_e^{(r)}$. Indeed, if $\alpha^j\mathbf{v}$ were a row in $H_e^{(r)}$, then $\alpha^j\bar{\gamma}_i, \alpha^j\bar{\gamma}_{i+1}$ would be two consecutive entries in the row, where $\alpha^j\bar{\gamma}_i = 0$ and $\alpha^j\bar{\gamma}_{i+1} \neq 0$, so $\alpha^j\bar{\gamma}_{i+1} = \lambda'_t(b_0 + b_1\alpha + \dots + b_{e-1}\alpha^{e-1})$ for some nonzero $\lambda'_t \in \mathbb{F}_p$, and so we have $(\lambda'_t - \alpha^j\lambda_t)(b_0 + b_1\alpha + \dots + b_{e-1}\alpha^{e-1}) = 0$. Since α is a primitive element in \mathbb{F}_{p^e} , we obtain $\lambda'_t - \alpha^j\lambda_t = 0$ which contradicts our assumption $\alpha^j \notin \mathbb{F}_p$. Hence, from Lemma II.3 we obtain that the dimension of the kernel $\ker(F_{H_e})$ is zero (or equivalently, $\ker(C_{H_e}) = 1$).

For the rank, we can improve the lower bound given in Proposition II.4. From the previous paragraph, for any $v \in C_H \setminus \mathcal{K}(C_H)$, the intersection of the linear space over \mathbb{F}_{p^e} generated by v and C_H is of dimension 1 over \mathbb{F}_p . Hence, the number of independent vectors over F_{p^e} generating the p^{e+t-ek} cosets of $\mathcal{K}(C_H)$ over C_H is lower bounded by $e+t-ek = t$ and so $t+k = t+1 \leq \text{rank}(C_H)$. Finally, from item (iv) of Proposition II.4 we obtain the statement. \square

Example IV.2. We construct a GH matrix $H(2^2, 2)$ such that C_H is an additive code over \mathbb{F}_{2^2} of length $n = 2^3$ with $\ker(C_H) = 1$ and $\text{rank}(C_H) = 4$. We begin with the GH matrix $H(2^3, 1)$ given by the multiplicative table of \mathbb{F}_{2^3} , that is,

$$H(2^3, 1) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 \\ 0 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & 1 \\ 0 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & 1 & \omega \\ 0 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & 1 & \omega & \omega^2 \\ 0 & \omega^4 & \omega^5 & \omega^6 & 1 & \omega & \omega^2 & \omega^3 \\ 0 & \omega^5 & \omega^6 & 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 0 & \omega^6 & 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 \end{pmatrix}, \quad (5)$$

where ω is a primitive element in \mathbb{F}_{2^3} and $\omega^3 = \omega + 1$. Next, we write each entry of (5) by using coordinates over \mathbb{F}_2 and projecting them over \mathbb{F}_{2^2} . Note that $\bar{0} = (0, 0, 0) = (0, 0) = 0$, $\bar{1} = (1, 0, 0) = (1, 0) = 1$, $\bar{\omega} = (0, 1, 0) = (0, 1) = \alpha$, $\bar{\omega}^2 = (0, 0, 1) = (0, 0) = 0$, $\bar{\omega}^3 = (1, 1, 0) = (1, 1) = \alpha^2$, $\bar{\omega}^4 = (0, 1, 1) = (0, 1) = \alpha$, $\bar{\omega}^5 = (1, 1, 1) = (1, 1) = \alpha^2$, $\bar{\omega}^6 = (1, 0, 1) = (1, 0) = 1$, where α is a primitive element in

\mathbb{F}_{2^2} and $\alpha^2 = \alpha + 1$. Finally, by the proof of Proposition IV.1, we obtain the following GH matrix $H(2^2, 2)$:

$$H(2^2, 2) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & \alpha & 0 & \alpha^2 & \alpha & \alpha^2 & 1 \\ 0 & \alpha & 0 & \alpha^2 & \alpha & \alpha^2 & 1 & 1 \\ 0 & 0 & \alpha^2 & \alpha & \alpha^2 & 1 & 1 & \alpha \\ 0 & \alpha^2 & \alpha & \alpha^2 & 1 & 1 & \alpha & 0 \\ 0 & \alpha & \alpha^2 & 1 & 1 & \alpha & 0 & \alpha^2 \\ 0 & \alpha^2 & 1 & 1 & \alpha & 0 & \alpha^2 & \alpha \\ 0 & 1 & 1 & \alpha & 0 & \alpha^2 & \alpha & \alpha^2 \end{pmatrix}. \quad (6)$$

\triangle

By Proposition II.4, for $q = p^2$ (that is, for $e = 2$), we have that the rank of an additive GH code C_H of length $n = p^2$ (that is, with $t = e = 2$) has to be 3 if the dimension of the kernel is 1. The next result shows that there exists a code C_H with these parameters for any p prime and $p \neq 2$. Therefore, in this case, we have that the given lower bound for the rank, once the dimension of the kernel is fixed, coincides with the upper bound.

Note that, for $q = 4$, it is well known that there is only one GH matrix $H(4, 1)$, up to equivalence, which gives the linear code C_H of length $n = 4$ over \mathbb{F}_4 , having rank and dimension of the kernel equal to 2.

Proposition IV.3. For $t = e = 2$ and p an odd prime, there exists a GH matrix $H(p^2, 1)$ such that C_H is an additive code over \mathbb{F}_{p^2} of length $n = p^2$ with $\ker(C_H) = 1$ and $\text{rank}(C_H) = 3$.

Proof. First, we construct a GH matrix $H(p^2, 1)$ and then we prove that it fulfils the conditions of the statement. Let $\mathbf{v}_1 = (0, \omega^0, \omega^1, \dots, \omega^{p^2-2})$, where ω is a primitive element in \mathbb{F}_{p^2} . Hence, \mathbf{v}_1 has a zero in the first position and ω^{i-1} in the $(i+1)$ th position, for $i \in \{1, 2, \dots, p^2-1\}$. Now, we define \mathbf{v}_2 as the vector having a zero in the first position and ω^{ip} in the $(i+1)$ th position. We construct the matrix $H(p^2, 1)$ having as rows all linear combinations over \mathbb{F}_p of \mathbf{v}_1 and \mathbf{v}_2 . We permute the rows in order to have the all-zero row as the first one. Note that $H(p^2, 1)$ is a matrix of order p^2 over \mathbb{F}_{p^2} , which has all zeros in the first row and column.

The vector \mathbf{v}_1 has no two positions with the same value. The same is true for \mathbf{v}_2 (indeed, the coordinates of \mathbf{v}_2 correspond to the image of the Frobenius automorphism $x \rightarrow x^p$). The elements of \mathbb{F}_{p^2} which are in \mathbb{F}_p are of the form $\omega^{\lambda(p+1)}$, for $\lambda \in \{0, 1, \dots, p-1\}$. Hence, the $(i+1)$ th position of any row in $H(p^2, 1)$ is of the form $\omega^{\lambda(p+1)\omega^{i-1}} + \omega^{\gamma(p+1)\omega^{ip}}$, for $i \in \{1, 2, \dots, p^2-1\}$ and $\lambda, \gamma \in \{0, 1, \dots, p-1\}$. The coordinates of any row of $H(p^2, 1)$ are all different, otherwise we would have two indexes i, j such that

$$\omega^{\lambda(p+1)\omega^{i-1}} + \omega^{\gamma(p+1)\omega^{ip}} = \omega^{\lambda'(p+1)\omega^{j-1}} + \omega^{\gamma'(p+1)\omega^{jp}}$$

or, equivalently, $\omega^{\lambda(p+1)-1}(\omega^i - \omega^j) = \omega^{\gamma(p+1)}(\omega^{jp} - \omega^{ip})$. Note that $(\omega^{jp} - \omega^{ip}) = (-1)^p(\omega^i - \omega^j)^p$. Therefore, simplifying, there would exist $\delta \in \{0, 1, \dots, p-1\}$ such that $\omega^{\delta(p+1)-1} = (\omega^i - \omega^j)^{p-1}$. Raising this equality to $p+1$, we obtain $(p+1)(\delta(p+1)-1) \equiv 0 \pmod{p^2-1}$. Reducing

modulo 2ξ , where ξ is the highest power of 2 dividing $p+1$, we obtain $p+1 \equiv 0 \pmod{2\xi}$, which contradicts the definition of ξ . This proves that $H(p^2, 1)$ is a GH matrix.

Finally, by Proposition II.4, we just need to prove that $H(p^2, 1)$ is nonlinear. We see that multiplying \mathbf{v}_1 by ω^p , we obtain a vector which is not any row of the matrix. It is enough to focus on the second column of the matrix. Assume the contrary, that is, there exist $\lambda, \gamma \in \{0, 1, \dots, p-1\}$ such that $\omega^p = \omega^{\lambda(p+1)} + \omega^{\gamma(p+1)}\omega^p$ or, equivalently, $\omega^{\lambda(p+1)} = (1 - \omega^{\gamma(p+1)})\omega^p$. Since $\omega^{\lambda(p+1)}$ and $1 - \omega^{\gamma(p+1)} \in \mathbb{F}_p$, we would have that $\omega^p \in \mathbb{F}_p$, which is a contradiction. \square

Example IV.4. We construct a GH matrix $H(9, 1)$ such that C_H is an additive code over \mathbb{F}_9 of length $n = 9$ with $\ker(C_H) = 1$ and $\text{rank}(C_H) = 3$.

Let $\mathbf{v}_1 = (0, \omega^0, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7)$ and $\mathbf{v}_2 = (0, \omega^3, \omega^6, \omega, \omega^4, \omega^7, \omega^2, \omega^5, \omega^0)$, where ω is a primitive element in \mathbb{F}_{3^2} and $\omega^3 = \omega + 2$. By the proof of Proposition IV.3, we obtain the matrix $H(9, 1)$ as the matrix having as rows all linear combinations over \mathbb{F}_3 of \mathbf{v}_1 and \mathbf{v}_2 , that is,

$$H(3^2, 1) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 0 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 & 1 \\ 0 & \omega^4 & \omega^5 & \omega^6 & \omega^7 & 1 & \omega & \omega^2 & \omega^3 \\ 0 & \omega^7 & \omega^2 & \omega^5 & 1 & \omega^3 & \omega^6 & \omega & \omega^4 \\ 0 & \omega & \omega^3 & 1 & \omega^6 & \omega^5 & \omega^7 & \omega^4 & \omega^2 \\ 0 & \omega^5 & \omega^7 & \omega^4 & \omega^2 & \omega & \omega^3 & 1 & \omega^6 \\ 0 & \omega^6 & \omega^4 & \omega^3 & \omega^5 & \omega^2 & 1 & \omega^7 & \omega \\ 0 & \omega^2 & 1 & \omega^7 & \omega & \omega^6 & \omega^4 & \omega^3 & \omega^5 \end{pmatrix}. \quad (7)$$

\triangle

By Proposition II.4, for $q = p^3$ (that is, for $e = 3$), we have that the rank of an additive GH code C_H of length $n = p^3$ (that is, with $t = e = 3$) is 3 or 4 if the dimension of the kernel is 1. However, by computer search, we found that there is not any additive GH matrix $H(8, 1)$ with C_H of rank 3, and they do exist with rank 4, for example the one given in Example IV.5. Therefore, the lower bound given by Proposition II.4 is not always tight.

Example IV.5. The following GH matrix $H(2^3, 1)$ over \mathbb{F}_{2^3} generates an additive GH code C_H of length $n = 2^3$ with rank equal to 4 and a kernel of dimension 1, where ω is a primitive element in \mathbb{F}_{2^3} and $\omega^3 = \omega + 1$.

$$H(2^3, 1) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega^2 & \omega^5 & \omega^3 & 1 & \omega & \omega^6 & \omega^4 \\ 0 & \omega^3 & \omega & 1 & \omega^6 & \omega^2 & \omega^4 & \omega^5 \\ 0 & 1 & \omega^2 & \omega^6 & \omega^4 & \omega^3 & \omega^5 & \omega \\ 0 & \omega^5 & \omega^6 & \omega & \omega^2 & \omega^4 & \omega^3 & 1 \\ 0 & \omega^6 & \omega^3 & \omega^4 & \omega^5 & 1 & \omega & \omega^2 \\ 0 & \omega & \omega^4 & \omega^2 & \omega^3 & \omega^5 & 1 & \omega^6 \\ 0 & \omega^4 & 1 & \omega^5 & \omega & \omega^6 & \omega^2 & \omega^3 \end{pmatrix}. \quad (8)$$

\triangle

For $t = e = 4$, we have found that there are GH matrices $H(p^4, 1)$ for $p = 3$ and $p = 5$ such that C_H are additive codes with minimum dimension of the kernel $\ker(C_H) = 1$

and minimum rank $\text{rank}(C_H) = 3$, given by the following two examples. We have checked computationally that the technique used in these two examples does not apply for $p = 7$ and $p = 11$.

Example IV.6. Let $H(3^4, 1)$ be the matrix having as rows all linear combinations over \mathbb{F}_3 of $\mathbf{v}_1, \omega\mathbf{v}_1, \mathbf{v}_2$ and $\omega\mathbf{v}_2$, where $\mathbf{v}_1 = (0, \omega^0, \omega^1, \dots, \omega^i, \dots, \omega^{79})$, $\mathbf{v}_2 = (0, \omega^2, \omega^{11}, \dots, \omega^{2+9i}, \dots, \omega^{73})$, and ω is a primitive element in \mathbb{F}_{3^4} . We can check that it is a GH matrix. Clearly, by construction, C_H is an additive code with $\text{rank}(C_H) = 3$. By Lemma II.3, we have that $\ker(C_H) = 1$. \triangle

Example IV.7. Let $H(5^4, 1)$ be the matrix having as rows all linear combinations over \mathbb{F}_5 of $\mathbf{v}_1, \omega\mathbf{v}_1, \mathbf{v}_2$ and $\omega\mathbf{v}_2$, where $\mathbf{v}_1 = (0, \omega^0, \omega^1, \dots, \omega^i, \dots, \omega^{623})$, $\mathbf{v}_2 = (0, \omega^6, \omega^{31}, \dots, \omega^{6+25i}, \dots, \omega^{605})$, and ω is a primitive element in \mathbb{F}_{5^4} . We can check that it is a GH matrix. Clearly, by construction, C_H is an additive code with $\text{rank}(C_H) = 3$. By Lemma II.3, we have that $\ker(C_H) = 1$. \triangle

V. COMBINING DIFFERENT CONSTRUCTIONS

In this section, we use the constructions of additive GH codes given in Sections III and IV, to show the existence of such codes having different ranks between the lower and upper bounds found in Section II, for a fixed dimension of the kernel. We also see that it is only possible to construct codes for all allowable pairs rank and dimension of the kernel when $e = 2$, by using the above constructions. For $e \geq 3$, mainly it is still necessary to prove the existence of additive GH codes with a kernel of dimension 1 and not having the maximum rank.

First, in the next theorem, for $q = p^e$, p prime and any $t > e > 1$, we prove that there is an additive GH code C_H over \mathbb{F}_q of length $n = p^t$ with $\ker(C_H) = k$ for each possible value of k given by item (iv) of Proposition II.4. These codes are the ones having the maximum rank, that is, satisfying the upper bound given by item (iii) of Proposition II.4. This proves that this upper bound for the rank, once the dimension of the kernel is fixed, is tight for all cases with $t > e > 1$.

Note that when $t = e > 1$, there is an additive GH matrix $H(q, 1)$, given by the multiplicative table of \mathbb{F}_q , so the corresponding GH code $C_H = C_{S_q}$ of length $n = p^e = q$ is linear over \mathbb{F}_q and $\ker(C_H) = \text{rank}(C_H) = 2$ [24]. According to Proposition II.4, in this case, there could be additive GH codes C_H having $\ker(C_H) = 1$ and $\text{rank}(C_H) \in \{3, \dots, 1+e\}$. By Proposition IV.3, for $t = e = 2$, there exist such codes having rank 3. However, it is still an open problem to prove their existence when $q = p^e$ and $e \geq 3$ (except for $q = 2^3$, $q = 3^4$ and $q = 5^4$; by Examples IV.5 to IV.7, respectively), even in general for GH codes which are not necessarily additive. These are connected to Latin squares of order $q - 1$ and we could use this approach to construct them.

Theorem V.1. For $q = p^e$, p prime, and any $t > e > 1$, there exists an additive GH code C_H over \mathbb{F}_q of length $n = p^t$ with $\ker(C_H) = k$ if and only if

- (i) $k \in \{1, \dots, \lfloor t/e \rfloor\}$ when $e \nmid t$,
- (ii) $k \in \{1, \dots, t/e + 1\}$, otherwise.

Moreover, $\text{rank}(C_H) = 1 + t - (e - 1)(k - 1)$.

Proof. The general proof is by induction over $t > e$, in steps of e . In this sense, the first point is to show the existence of additive GH codes with the following parameters:

$$k = 1 \text{ when } t \in \{e + 1, \dots, 2e - 1\},$$

$$k \in \{1, 2, 3\} \text{ when } t = 2e.$$

When $t = 2e$, by Corollary III.2, the additive GH code C_H corresponding to $S^2 = S_q \oplus S_q$ has $k = 3$ and $\text{rank}(C_H) = 1 + t - (e - 1)(k - 1) = 3$. By Proposition III.5, there exists an additive GH code C_H over \mathbb{F}_q with $k = 2$ and $\text{rank}(C_H) = 1 + t - (e - 1)(k - 1) = 2 + e$. From Proposition IV.1, the existence of additive GH codes with $k = 1$ and maximum rank is assured for all $t > e > 1$.

By Corollary III.2 and Lemma III.1, we can recursively construct additive GH codes C_H by using the Kronecker sum construction, $H = S_q \oplus B$, where B is an additive GH matrix of size $p^{t'} = p^{t-e}$ constructed in the previous step. Note that if C_B of length $p^{t'}$ has a kernel of dimension k' and maximum rank $r' = 1 + t' - (e - 1)(k' - 1)$, then C_H of length p^t with $t = t' + e$ has a kernel of dimension $k = k' + 1$ and rank $r = r' + 1$. Therefore, $r = 1 + t' - (e - 1)(k' - 1) + 1 = 1 + t - (e - 1)(k - 1)$ and C_H has maximum rank. This construction covers all the values of k in the statement, except $k = 1$. However, Proposition IV.1 assures the existence of additive GH codes with $k = 1$ and maximum rank for all $t > e > 1$. Therefore, the existence for all given parameters is proved.

Finally, by Proposition II.4 and Lemma II.2, we have that these are the only possibilities for the dimension of the kernel of an additive GH code. \square

When $e = 2$, by Corollary II.5, we have that for each possible dimension of the kernel, there is only one possible rank. Therefore, when $t > e = 2$, the above theorem covers all possible pairs (r, k) , where r is the rank and k the dimension of the kernel of the additive GH code. Moreover, since Proposition IV.3 covers the case when $t = e = 2$, we have the following corollary.

Corollary V.2. *For $q = p^2$, p prime, and any $t \geq 2$, there exists an additive GH code C_H over \mathbb{F}_q of length $n = p^t$ with $\ker(C_H) = k$ and $\text{rank}(C_H) = r$ if and only if $r = t + 2 - k$ and k satisfies*

- (i) $k \in \{1, \dots, \lfloor t/e \rfloor\}$ when $e \nmid t$,
- (ii) $k \in \{1, \dots, t/e + 1\}$, otherwise.

Proof. Straightforward by Propositions IV.3 and II.4, Corollary II.5, and Theorem V.1. \square

Example V.3. For $q = p^2$, the second column in Table IV gives all possible values for the rank and dimension of the kernel of additive GH codes over \mathbb{F}_{p^2} of length $n = p^t$ with $2 \leq t \leq 7$, given by Proposition II.4 and Corollary II.5. By Corollary V.2, for each one of these pairs, there exists an additive GH code over \mathbb{F}_{p^2} having these parameters. \triangle

TABLE IV
PARAMETERS $(\text{rank}(C_H), \ker(C_H))$ FOR ALL ADDITIVE GH CODES C_H OVER \mathbb{F}_{p^2} OF LENGTH $n = p^t$ WITH $2 \leq t \leq 7$.

t	$(\text{rank}(C_H), \ker(C_H))$	$\ker_p(C_H) = \text{rank}_p(C_H)$
2	(3,1) (2,2)	2
3	(4,1)	2.5
4	(5,1) (4,2) (3,3)	3
5	(6,1) (5,2)	3.5
6	(7,1) (6,2) (5,3) (4,4)	4
7	(8,1) (7,2) (6,3)	4.5

Example V.4. For $q = 4$, that is when $p = 2$ and $e = 2$, we can take into account some already known results on the classification of GH matrices.

- If $n = 4$ ($t = 2$), there is only one GH matrix $H(4, 1)$ over \mathbb{F}_4 having $\text{rank}(C_H) = \ker(C_H) = 2$. Therefore, C_H is linear over \mathbb{F}_4 , so additive. Actually, $H(4, 1)$ corresponds to the Sylvester GH matrix $S^1 = S_4$.
- If $n = 8$ ($t = 3$), there is only one GH matrix $H(4, 2)$ having $\text{rank}(C_H) = 4$ and $\ker(C_H) = 1$. Therefore, C_H is nonlinear over \mathbb{F}_4 . However, since $\text{rank}_2(C_H) = \ker_2(C_H) = 2.5$, it is additive.
- If $n = 16$ ($t = 4$), it is known that there are 226 nonequivalent GH matrices $H(4, 4)$ over \mathbb{F}_4 [10]. Table V shows the ranks and dimensions of the kernel of the corresponding codes C_H . Moreover, for each case, it also gives the value Na/N , where N is the number of nonequivalent codes and Na the number of such codes that are additive.

TABLE V
NUMBER OF NONEQUIVALENT ADDITIVE GH CODES OF LENGTH 16 OVER \mathbb{F}_4 VERSUS THE TOTAL NUMBER, FOR EACH POSSIBLE RANK AND DIMENSION OF THE KERNEL.

$\ker(C_H)$	$\text{rank}(C_H)$					
	3	4	5	6	7	8
3	1/1					
2		5/7	0/8			
1		0/3	38/92	0/55	0/57	0/3

\triangle

Recall that the more general switching construction, given by Proposition III.6, allows for the construction of additive GH codes having different ranks and dimensions of the kernel, when t is a multiple of e and $k > 1$. Now, we combine this construction with the Kronecker sum construction to cover more cases, proving the existence of additive GH codes C_H over \mathbb{F}_q of length $n = p^t$, where $q = p^e$, when t is not a multiple of e and $k > 1$.

Proposition V.5. *For $q = p^e$, p prime, and any t not a multiple of $e > 1$, there exists an additive GH code C_H over \mathbb{F}_q of length $n = p^t$ with $\text{rank}(C_H) = r$ and $\ker(C_H) = k$, for all $k \in \{2, \dots, h = \lfloor t/e \rfloor\}$ and*

$$r \in \{2h - k + t + e - he, \dots, 1 + t - (e - 1)(k - 1)\}.$$

Proof. Take $q = p^e$, p prime, and any $t > e$ not a multiple of $e > 1$. Set $t = he + h'$, where $h = \lfloor t/e \rfloor$. Hence, we can write $t = (h - 1)e + (e + h')$.

If $h = k$, then $r = 2h - k + t + e - he = 1 + t - (e - 1)(k - 1)$, so the code has the maximum rank r , and its existence is given by Theorem V.1. Note that if $h = 2$, then $k = 2$, so we can focus on the case where $h \geq 3$.

If $h \geq 3$, by Proposition III.6, there exists a GH code D of length $p^{(h-1)e}$ with $\ker(D) = k$ for all $k \in \{2, \dots, h - 1\}$ and $\text{rank}(D) \in \{2(h - 1) - k + 2, \dots, h + (h - k)(e - 1)\}$. Also, by Proposition IV.1, there exists a GH code E of length $p^{e+h'}$ with $\ker(E) = 1$ and $\text{rank}(E) = e + h' + 1$. Then, by Lemma III.1, using the Kronecker sum construction with D and E , we obtain an additive GH code C over \mathbb{F}_q of length $n = p^t$ with $\ker(C) = k$ and $\text{rank}(C) = r$, for all $2 \leq k \leq h - 1$ and $2(h - 1) - k + 2 + e + h' + 1 - 1 \leq r \leq h + (h - k)(e - 1) + e + h' + 1 - 1$, or equivalently, $2h - k + t + e - he \leq r \leq 1 + t - (e - 1)(k - 1)$. Therefore, the result follows. \square

Note that the additive GH codes constructed from the more general switching construction, given by Proposition III.6, do not cover all possible pairs (r, k) , where r is the rank and k the dimension of the kernel, when t is a multiple of e and $k > 1$. The upper bounds in Propositions II.4 and III.6 coincide since $h + 1 + (h - k + 1)(e - 1) = 1 + t - (e - 1)(k - 1)$ if $t = he$. However, the lower bounds do not coincide in general. The smallest case where both propositions disagree is for $e = 3$, $t = 9$, $h = 3$ and $k = 2$. By using Proposition III.6, we know that we can construct additive GH codes with these parameters having rank r for all $r \in \{6, 7, 8\}$. However, from Proposition II.4, we have that $r \in \{5, 6, 7, 8\}$, and it is not known whether there is a code having rank $r = 5$.

As we just noted for the case when t is a multiple of e and $k > 1$, the codes constructed in Proposition V.5 when t is not a multiple of e do not cover all possible pairs (r, k) given by Proposition II.4. Again, the upper bounds coincide, but not the lower bounds. The smallest case where they disagree is for $e = 3$, $t = 7$, $h = 2$ and $k = 2$. By using Proposition V.5, there exist additive GH codes with these parameters having rank $r = 6$. However, from Proposition II.4, we have that $r \in \{4, 5, 6\}$, and the existence of the case with $r \in \{4, 5\}$ is not known.

Theorem V.6. *For $q = p^e$, p prime, and any $t > e > 1$, there exists an additive GH code C_H over \mathbb{F}_q of length $n = p^t$ with $\ker(C_H) = k$ and $\text{rank}(C_H) = r$, for all $k \in \{2, \dots, h = \lfloor t/e \rfloor\}$ and*

$$r \in \{l_k, \dots, 1 + t - (e - 1)(k - 1)\},$$

where

$$l_k = \begin{cases} 2h - k + 2 & \text{if } t \text{ is multiple of } e, \\ 2h - k + t + e - he, & \text{otherwise.} \end{cases}$$

Proof. Straightforward from Propositions V.5 and III.6. \square

Corollary V.7. *For $q = p^e$, p prime, and any $t > e > 1$, there exists an additive GH code C_H over \mathbb{F}_q of length $n = p^t$ with $\ker(C_H) = k$ and $\text{rank}(C_H) = r$, if and only if*

- (i) $r \in \{t/e + 2, \dots, t/e + e\}$ when $k = t/e$ (t is a multiple of e);
- (ii) $r = 1 + t/e$ when $k = 1 + t/e$ (t is a multiple of e).

Proof. By Theorem V.6, we have that there exists an additive GH code C_H over \mathbb{F}_q of length $n = p^t$ with $\ker(C_H) = h$ and $\text{rank}(C_H) = r$ for all $r \in \{h + 2, \dots, h + e\}$, where $h = t/e$. In this case, the value $h + 2$ coincides with the lower bound $\lceil \frac{e+t-t/e}{e-1} \rceil$, given in Proposition II.4. Note that $\lceil \frac{e+t-t/e}{e-1} \rceil = \lceil \frac{e-1+1+t-t/e}{e-1} \rceil = 1 + \lceil \frac{1}{e-1} \rceil + t/e = t/e + 2 = h + 2$. Similarly, the value $h + e$ is equal to the upper bound given by Proposition II.4, since $1 + t - (e - 1)(t/e - 1) = t/e + e = h + e$. \square

Example V.8. In Table I of Example II.6, all possible values for the rank of additive GH codes of length $n = p^t$ with $2 \leq t \leq 12$, once the dimension of the kernel is given, are shown. By Theorem V.6, for each one of these values, except for the ones in bold type, there exists an additive GH code having these parameters.

As it is noticed in Corollary V.7, we can also see in Table I that when $t = 3h$ with $t > 3$, if $k = h$ or $k = h + 1$, we can construct an additive GH code C_H with $\ker(C_H) = k$ and $\text{rank}(C_H) = r$ for all possible values of r between the bounds given by Proposition II.4. \triangle

By using the additive GH codes over \mathbb{F}_{p^4} of length $n = p^4$ (with $p = 3$ and $p = 5$) and a kernel of dimension 1, given in Examples IV.6 and IV.7, along with the Kronecker sum construction, we show the existence of additive GH codes over \mathbb{F}_{p^4} with greater length, kernel of dimension 1 and different ranks.

Proposition V.9. *For $q = p^4$, with $p = 3$ or $p = 5$, and any $t \geq 4$, there exists an additive GH code C_H over \mathbb{F}_q of length $n = p^t$ with $\ker(C_H) = 1$ and $\text{rank}(C_H) = t + 1 - 2i$, for all $i \in \{0, \dots, \lfloor t/4 \rfloor - 2\}$.*

Proof. First, note that the upper bound for the rank is $t + 1$ when the dimension of the kernel is 1. For $t \in \{5, 6, 7, 8\}$, we have that $r = t + 1$ and the statement is true by Theorem V.1. Assume that it is true for $t' \in \{4h' - 3, 4h' - 2, 4h' - 1, 4h'\}$, $h' \geq 2$. That is, by induction hypothesis, there exist an additive GH code C_D with $\ker(C_D) = 1$ and $\text{rank}(C_D) = t' + 1 - 2j$ for all $j \in \{0, \dots, h' - 2\}$. By Examples IV.6 and IV.7, there exists an additive GH code C_E with $\ker(C_E) = 1$ and $\text{rank}(C_E) = 3$. By Lemma III.1, applying the Kronecker sum construction to the corresponding GH matrices D and E , there exist additive GH codes C_H of length $n = p^t$, with $t = t' + 4$ and $h = h' + 1$, having $\ker(C_H) = \ker(C_D) + \ker(C_E) - 1 = 1$ and $\text{rank}(C_H) = \text{rank}(C_D) + \text{rank}(C_E) - 1 = t' + 1 - 2j + 3 - 1$ for all $j \in \{0, \dots, h' - 2\}$, or equivalently, $\text{rank}(C_H) = t - 4 + 1 - 2j + 2 = t + 1 - 2(j + 1) = t + 1 - 2i$ for all $i \in \{1, \dots, h - 2\}$. Finally, again by Theorem V.1, there is a code C_H for $i = 0$, and the result follows. \square

Finally, we show that if the existence of additive GH codes with dimension of the kernel 1 and any rank between the given lower and upper bounds is proved, then we would have the existence of any such code with rank r and kernel of dimension k for any possible pair (r, k) .

Theorem V.10. *Let $q = p^e$, p prime, and $e > 1$. If there exist an additive GH code C_H over \mathbb{F}_q of length $n = p^t$,*

$t > e$, with $\ker(C_H) = 1$ and $\text{rank}(C_H) = r$ for all $r \in \{\lceil \frac{e+t-1}{e-1} \rceil, \dots, 1+t\}$, then there exists an additive GH code C_H over \mathbb{F}_q of length $n = p^t$ with $\ker(C_H) = k$ and $\text{rank}(C_H) = r$, for all $k \in \{2, \dots, \lfloor t/e \rfloor\}$ and $r \in \{\lceil \frac{e+t-k}{e-1} \rceil, \dots, 1+t+(e-1)(k-1)\}$.

Proof. It follows from the same arguments as in the proof of Theorem V.1, by induction over t , in steps of e . Note that, for the lower bound of the rank, by induction hypotheses, there exists an additive GH code of length p^{t-e} with kernel of dimension $k-1$ and $\text{rank} \lceil \frac{e+t-e-(k-1)}{e-1} \rceil$. After applying the Kronecker sum construction, the new additive GH code C_H of length 2^t would have $\ker(C_H) = k$ and $\text{rank}(C_H) = \lceil \frac{e+t-e-(k-1)}{e-1} \rceil + 1 = \lceil \frac{e+t-k}{e-1} \rceil$. \square

VI. SELF-ORTHOGONAL ADDITIVE GH CODES OVER \mathbb{F}_{p^2} AND QUANTUM CODES

The question of finding quantum-error correcting codes is transformed into the question of finding additive codes over a finite field which are self-orthogonal with respect to a certain trace inner product [1], [3]. In this section, we see that the additive GH codes over \mathbb{F}_q with $q = p^2$ constructed in the previous sections are self-orthogonal, so they can be used to produce quantum codes.

For codes of length n over \mathbb{F}_{p^2} , there are other well known inner products besides the Euclidean inner product. Let $\mathbf{v} = (v_1, \dots, v_n)$ and $\mathbf{w} = (w_1, \dots, w_n) \in \mathbb{F}_{p^2}^n$. The *Hermitian inner product*, defined by $[\mathbf{v}, \mathbf{w}]_H = \sum_{i=1}^n v_i w_i^p$ and the *trace Hermitian inner product*, which is used for additive codes over \mathbb{F}_{p^2} , that is $\langle \mathbf{v}, \mathbf{w} \rangle = \sum_{i=1}^n (v_i w_i^p - v_i^p w_i)$ or $\langle \mathbf{v}, \mathbf{w} \rangle = \beta \sum_{i=1}^n (v_i w_i^p - v_i^p w_i)$ depending on whether p is even or odd, respectively [13], where $\beta = \omega^{(p+1)/2}$ and ω is a primitive element in \mathbb{F}_{p^2} . We denote the orthogonal code defined by the trace Hermitian inner product as C^\perp .

Lemma VI.1. *Let \mathbf{v}, \mathbf{w} be two rows of a GH matrix $H(p^2, \lambda)$ with $p \neq 2$. Then $\langle \mathbf{v}, \mathbf{w} \rangle = 0$.*

Proof. Since the nonzero elements of \mathbb{F}_p are the roots of the polynomial $x^{p-1} - 1$, we see that $\sum_{i=0}^{p-2} \alpha^i = 0$, where $\alpha \in \mathbb{F}_p$ is a primitive element and $p \neq 2$.

Now, let ω be a primitive element in \mathbb{F}_{p^2} and take $\alpha = \omega^{p+1}$ which is a primitive element in \mathbb{F}_p . Then

$$\begin{aligned} \sum_{j=0}^{p^2-2} (\omega^j)^{p+1} &= \sum_{i=0}^{p-2} \sum_{t=1}^{p+1} (\omega^{i+t(p-1)})^{p+1} = \\ &= (p+1) \sum_{i=0}^{p-2} (\omega^i)^{p+1} = (p+1) \sum_{i=0}^{p-2} \alpha^i = 0. \end{aligned} \quad (9)$$

For any two rows $\mathbf{v} = (v_1, \dots, v_n)$ and $\mathbf{w} = (w_1, \dots, w_n)$ in a GH matrix $H(p^2, \lambda)$, where $n = p^2 \lambda$, we have

that $\sum_{i=1}^n (v_i - w_i)^{p+1} = \sum_{i=1}^n v_i^{p+1} - \sum_{i=1}^n w_i^{p+1} = \lambda \sum_{j=0}^{p^2-2} (\omega^j)^{p+1} = 0$ by (9). Then we have

$$\begin{aligned} \sum_{i=1}^n (v_i - w_i)^{p+1} &= \sum_{i=1}^n (v_i^p - w_i^p)(v_i - w_i) = \\ &= \sum_{i=1}^n (v_i^{p+1} + w_i^{p+1} - (v_i^p w_i + w_i^p v_i)) = \\ &= - \sum_{i=1}^n (v_i^p w_i + w_i^p v_i) = 0. \end{aligned} \quad (10)$$

Therefore, if p is even, then $\langle \mathbf{v}, \mathbf{w} \rangle = 0$. Otherwise, $0 = -\beta \sum_{i=1}^n (v_i^p w_i + w_i^p v_i) = \sum_{i=1}^n ((\beta v_i)^p w_i - w_i^p (\beta v_i)) = \langle \beta \mathbf{v}, \mathbf{w} \rangle = \beta \langle \mathbf{v}, \mathbf{w} \rangle$ and we also have that $\langle \mathbf{v}, \mathbf{w} \rangle = 0$. Note that since $\beta = \omega^{(p+1)/2}$ when p is odd, $\beta^p = -\beta$. \square

Lemma VI.2. *Let \mathbf{v}, \mathbf{w} be two different rows of a GH matrix $H(4, \lambda)$. Then $\langle \mathbf{v}, \mathbf{w} \rangle \equiv \lambda \pmod{2}$. If $\mathbf{v} = \mathbf{w}$ then $\langle \mathbf{v}, \mathbf{w} \rangle \equiv 0 \pmod{2}$.*

Proof. We note that for a vector $\mathbf{v} = (v_1, \dots, v_n)$, $\sum_{i=1}^n v_i^3$ is the weight of \mathbf{v} since each nonzero element cubed is 1. Let $\mathbf{v} \neq \mathbf{w}$. Note also that $\text{wt}(\mathbf{v}) = \text{wt}(\mathbf{w}) = \text{wt}(\mathbf{v} + \mathbf{w}) = n - \lambda$ by the properties of a GH matrix, where $n = 4\lambda$ is the order. Then we have

$$\begin{aligned} \sum_{i=1}^n (v_i + w_i)^3 &= \sum_{i=1}^n v_i^3 + 3 \sum_{i=1}^n v_i^2 w_i + 3 \sum_{i=1}^n v_i w_i^2 + \sum_{i=1}^n w_i^3 \\ \text{wt}(\mathbf{v} + \mathbf{w}) &= \text{wt}(\mathbf{v}) + 3\langle \mathbf{v}, \mathbf{w} \rangle + \text{wt}(\mathbf{w}). \end{aligned}$$

Hence, $\langle \mathbf{v}, \mathbf{w} \rangle = n - \lambda = 3\lambda$ and so $\langle \mathbf{v}, \mathbf{w} \rangle \equiv \lambda \pmod{2}$.

If $\mathbf{v} = \mathbf{w}$, then $\text{wt}(\mathbf{v} + \mathbf{w}) = 0$ and by the same computation as before we have $\langle \mathbf{v}, \mathbf{w} \rangle \equiv 0 \pmod{2}$. \square

Proposition VI.3. *Let $H(p^2, \lambda)$ be a GH matrix, where λ is even when $p = 2$. Then $F_H \subset F_H^\perp$ is a self-orthogonal code.*

Proof. By Lemmas VI.1 and VI.2, we have that any two vectors are orthogonal with respect to the trace Hermitian inner product. \square

Proposition VI.4. *Let $H(p^2, \lambda)$ be a GH matrix of order $n = p^2 \lambda = p^t$ over \mathbb{F}_{p^2} , where λ is even when $p = 2$, such that C_H is additive. Then C_H is an additive self-orthogonal code, containing p^{t+2} codewords, and the minimum distance of C_H^\perp is 3.*

Proof. By construction and Proposition VI.3, the results are clear and all that is required is to show that the minimum distance of C_H^\perp is 3. For this, we use the MacWilliams identity, which is proved for these codes in [4]. The (Hamming) weight enumerator of C_H is

$$\mathcal{W}_{C_H}(x, y) = x^{p^t} + (p^{t+2} - p^2) x^{p^{t-2}} y^{p^t - p^{t-2}} + (p^2 - 1) y^{p^t}$$

and so, the (Hamming) weight enumerator of C_H^\perp is

$$\begin{aligned} \mathcal{W}_{C_H^\perp}(x, y) &= \frac{1}{|C_H|} \mathcal{W}_{C_H}(x + (p^2 - 1)y, x - y) = \\ &= \frac{1}{|C_H|} \left[(x + (p^2 - 1)y)^{p^t} + \right. \\ &\quad \left. (p^{t+2} - p^2)(x + (p^2 - 1)y)^{p^{t-2}}(x - y)^{p^t - p^{t-2}} + \right. \\ &\quad \left. (p^2 - 1)(x - y)^{p^t} \right]. \end{aligned} \quad (11)$$

Let $a = p^t$, $b = p^{t-2}$ and $c = p^2 - 1$. Note that $bc = a - b$. Then, the coefficient of $x^{p^t-1}y$ in (11) is

$$\frac{1}{|C_H|} [ac - ac + p^2(a - 1)(bc - bc)] = 0.$$

Analogously, the coefficient of $x^{p^t-2}y^2$ is

$$\begin{aligned} &\frac{1}{|C_H|} \left[c^2 \binom{a}{2} + c \binom{a}{2} + p^2(a - 1) \left(c^2 \binom{b}{2} + \binom{bc}{2} - c^2 b^2 \right) \right] = \\ &\frac{1}{|C_H|} \left[c \binom{a}{2} p^2 + p^2(a - 1) \frac{c^2 b(b - 1) + bc(bc - 1) - 2c^2 b^2}{2} \right] = \\ &\frac{p^2}{ap^2} \left[c \binom{a}{2} + (a - 1) \frac{-c^2 b - cb}{2} \right] = \\ &\frac{1}{a} \left[(a - 1) \frac{ca - cb(c + 1)}{2} \right] = \\ &\frac{(a - 1)(ca - cb(c + 1))}{2a} = \frac{(a - 1)(-a + bc + b)}{2a} = 0. \end{aligned} \quad (12)$$

The coefficient of $x^{p^t-3}y^3$ is

$$\begin{aligned} &\frac{1}{|C_H|} \left[c^3 \binom{a}{3} - c \binom{a}{3} \right] + \\ &\frac{p^2(a - 1)}{|C_H|} \left[c^3 \binom{b}{3} - \binom{bc}{3} - c^3 b \binom{b}{2} + bc \binom{bc}{2} \right]. \end{aligned} \quad (13)$$

The first term in (13) is always positive. Therefore, in order to prove that the coefficient of $x^{p^t-3}y^3$ is positive, we only need to check that the second term is non negative. Hence, $6[c^3 \binom{b}{3} - \binom{bc}{3} - c^3 b \binom{b}{2} + bc \binom{bc}{2}] = bc[c^2(b - 1)(b - 2) - (bc - 1)(bc - 2) - 3bc^2(b - 1) + 3bc(bc - 1)] = bc(2c^2 - 2)$, which is non negative since $c = p^2 - 1 \geq 1$. This proves the statement. \square

Finally, we describe the connection of these additive GH matrices or the corresponding C_H codes with quantum codes, by following [5, Theo. 6.10].

A q -ary quantum code of length n and dimension K is a K -dimensional linear subspace Q of \mathbb{C}^{q^n} (a q^n -dimensional Hilbert space). It is denoted by $[[n, k, d]]_q$, where $k = \log_q K$ and d is the minimum distance, which means that Q can detect up to $d - 1$ errors and correct up to $\lfloor \frac{d-1}{2} \rfloor$.

Theorem VI.5. *Let $H(p^2, \lambda)$ be a GH matrix of order $n = p^2\lambda = p^t$ over \mathbb{F}_{p^2} , where λ is even when $p = 2$, such that C_H is additive. Then C_H gives a pure additive quantum-error-correcting code with parameters $[[p^t, p^t - (t + 2), 3]]_p$.*

Proof. It follows from [5] and Proposition VI.4. Note that there are no vectors of weight less than 3 in $C_H^\perp \setminus C_H$. \square

ACKNOWLEDGMENT

This work has been partially funded by the Spanish Government under grant reference PID2019-104664GB-I00 (AEI/10.13039/501100011033).

REFERENCES

- [1] A. E. Ashikhmin, and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Information Theory*, vol. 47(7), pp. 3065-3072, 2001.
- [2] H. Bauer, B. Ganter, and F. Hergert, "Algebraic techniques for nonlinear codes," *Combinatorica*, vol. 3, pp. 21-33, 1983.
- [3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum Error Correction Via Codes Over $GF(4)$," *IEEE Trans. Information Theory*, vol. 44(4), pp. 1369-1387, 1998.
- [4] W. C. Huffman, "On the theory of \mathbb{F}_q -linear \mathbb{F}_{q^t} -codes," *Advances in Mathematics of Communications*, vol. 7(3), pp. 349-378, 2013.
- [5] K. Feng, "Quantum error-correcting codes," in *Coding Theory and Cryptology*, pp. 91-142, 2002.
- [6] 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(2-3), pp. 417-435, 2019.
- [7] C. Fernández-Córdoba, C. Vela, and M. Villanueva, "On \mathbb{Z}_8 -linear Hadamard codes: rank and classification," *IEEE Trans. Information Theory*, vol. 66(2), pp. 970-982, 2019.
- [8] S. T. Dougherty, J. Rifà, and M. Villanueva, "Ranks and kernels of codes from generalized Hadamard matrices," *IEEE Trans. Inform. Theory*, vol. 62(2), pp. 687-694, 2016.
- [9] S. T. Dougherty, J. Rifà, and M. Villanueva, "Constructions of Nonequivalent Fp-Additive Generalised Hadamard Codes," in *Proc. of 2020 IEEE International Symposium on Information Theory in Los Angeles, California, USA*, pp. 150-155, 2020.
- [10] M. Harada, C. Lam, and V. Tonchev, "Symmetric (4, 4)-nets and generalized Hadamard matrices over groups or order 4," *Des. Codes Cryptography*, vol. 34, pp. 71-87, 2005.
- [11] D. Jungnickel, "On difference matrices, resolvable designs and generalized Hadamard matrices," *Math. Z.*, vol. 167, pp. 49-60, 1979.
- [12] A. Ketkar, A. Klappenecker S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Inform. Theory*, vol. 52(11), pp. 4892-4914, 2006.
- [13] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory*, Algorithms and Computation in Mathematics, Berlin/Heidelberg: Springer-Verlag, vol. 17, 2006.
- [14] Jong-Seon No and H.Y. Song, "Generalized Sylvester-type Hadamard matrices," *IEEE International Symposium on Information Theory*, June 2000, pp. 472.
- [15] E. Petrank, and R.M. Roth, "Is code equivalence easy to decide?" *IEEE Trans. Inform. Theory*, vol. 43, pp. 1602-1604, 1997.
- [16] K. T. Phelps, M. LeVan, "Kernels of nonlinear Hamming codes," *Des. Codes Cryptography*, vol. 6, pp. 247-257, 1995.
- [17] K. T. Phelps, J. Rifà, and M. Villanueva, "Kernels and p -kernels of p^r -ary 1-perfect codes," *Des. Codes Cryptography*, vol. 37, pp. 243-261, 2005.
- [18] K. T. Phelps, J. Rifà, and M. Villanueva, "Rank and kernel of binary Hadamard codes," *IEEE Trans. Inform. Theory*, vol. 51, no. 11, pp. 3931-3937, 2005.
- [19] K. T. Phelps, J. Rifà, and M. Villanueva, "Hadamard codes of length $2^t s$ (s odd): Rank and kernel," *Lecture Notes in Computer Science*, vol. 3857, pp. 328-337, 2006.
- [20] K. T. Phelps, J. Rifà, and M. Villanueva, "On the additive (\mathbb{Z}_4 -linear and non- \mathbb{Z}_4 -linear) Hadamard codes: rank and kernel," *IEEE Trans. Inform. Theory*, vol. 52(1), pp. 316-319, 2006.
- [21] K. T. Phelps and M. Villanueva, "Ranks of q -ary 1-perfect codes," *Des. Codes Cryptography*, vol. 27, pp. 139-144, 2002.
- [22] K. T. Phelps and M. Villanueva, "On perfect codes: rank and kernel," *Des. Codes Cryptography*, vol. 27, pp. 183-194, 2002.
- [23] S. S. Shrikhande, "Generalized Hadamard matrices and orthogonal arrays of strength two," *Canad. J. Math.*, vol. 16, pp. 736-740, 1964.
- [24] V. D. Tonchev, "On generalized Hadamard matrices of minimum rank," *Finite Fields Appl.*, vol. 10, pp. 522-529, 2004.

Steven T. Dougherty is a professor of Mathematics and the 2005 recipient of the Hasse Prize. He is the author of *Combinatorics and Finite Geometry* and *Algebraic Coding Theory over Finite Commutative Rings*. He has published over 100 papers and has lectured extensively in 12 countries. His research interests include coding theory, combinatorics, finite geometry and number theory.

Josep Rifà was born in Manlleu, Catalonia (Spain) in July 1951. He received the graduate degree in Sciences (Mathematical Section) in 1973, from the University of Barcelona and the Ph.D. degree in Sciences (Computer Sciences Section) in 1987, from the UAB (Autonomous University of Barcelona). Since 1974 he was an assistant professor in the Mathematics Department, Barcelona University. In 1987 he joined the UAB and since 1992 he has been a full professor in this University. He was the former Head of Information and Communications Engineering Department at UAB as well as the former Vice-chairman of the Spanish Chapter of Information Theory of IEEE. He has worked in several projects of 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. Currently, he serves as a Professor Emeritus at UAB.

Mercè Villanueva was born in Roses, Catalonia, in January 1972. She received the B.Sc. degree in Mathematics in 1994 from the Autonomous University of Barcelona, the M.Sc. degree in Computer Science in 1996, and the Ph.D. degree in Science (Computer Science Section) in 2001 from the same university. In 1994 she joined the Department of Information and Communications Engineering, at the Autonomous University of Barcelona, as an Assistant Professor, and was promoted to Associate Professor in 2002. Her research interests include subjects related to combinatorics, algebra, coding theory, and graph theory.