Generalized Hadamard Additive Codes

S. T. Dougherty[1], J. Rifà[2], M. Villanueva[2]

[1] *University of Scranton, Scranton, USA, steven.dougherty@scranton.edu*
[2] *Universitat Autònoma de Barcelona, Spain, {josep.rifa, merce.villanueva}@uab.cat*

This work was partially supported by the Spanish MINECO under Grants TIN2013-40524-P and MTM2015-69138-REDT, and by the Catalan AGAUR under Grant 2014SGR-691.

Let $\mathbb{F}_q = \mathrm{GF}(q)$ 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 *K-additive* if it is a linear space over a subfield $K \subset \mathbb{F}_q$. The dimension of a K-additive code C over $\mathbb{F}_q$ is defined as the number k such that $q^k = |C|$. Note that k is not necessarily an integer, but ke is an integer, where $q = |K|^e$. 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 $C_2 = \{\sigma(c_1,c_2,\ldots,c_n) = (c_{\sigma^{-1}(1)},\ldots,c_{\sigma^{-1}(n)}) : (c_1,c_2,\ldots,c_n) \in C_1\}$, [2], [6]. 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 $\mathscr{R}(C)$, is the subspace over $\mathbb{F}_q$ spanned by C, that is $\mathscr{R}(C) = \langle C \rangle$. The dimension of $\mathscr{R}(C)$ is called the *rank* of C and is denoted by $\mathrm{rank}(C)$. If $q = p^e$, p prime, we can also define $\mathscr{R}_p(C)$ and $\mathrm{rank}_p(C)$ as the subspace over $\mathbb{F}_p$ spanned by C and its dimension, respectively. The *kernel* of a code C over $\mathbb{F}_q$, denoted by $\mathscr{K}(C)$, is defined as $\mathscr{K}(C) = \{\mathbf{x} \in \mathbb{F}_q^n \ : \ \alpha\mathbf{x} + C = C \text{ for all } \alpha \in \mathbb{F}_q\}$. If $q = p^e$, p prime, we can also define the *p-kernel* of C as $\mathscr{K}_p(C) = \{\mathbf{x} \in \mathbb{F}_q^n \ : \ \mathbf{x} + C = C\}$. Since we assume that $\mathbf{0} \in C$, then $\mathscr{K}(C)$ is a linear subcode of C and $\mathscr{K}_p(C)$ is an $\mathbb{F}_p$-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 [9] for codes over $\mathbb{F}_q$, generalizing the binary case described previously in [1], [8]. In [9], it was proved that the code C over $\mathbb{F}_q$ can be written as the union of cosets of $\mathscr{K}(C)$ (resp., $\mathscr{K}_p(C)$), and $\mathscr{K}(C)$ (resp., $\mathscr{K}_p(C)$) is the largest such linear code over $\mathbb{F}_q$ (resp., $\mathbb{F}_p$) for which this is true. Moreover, it is clear that $\mathscr{K}(C) \subseteq \mathscr{K}_p(C)$.

A *generalized 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 $H(q,\lambda)$ [5]. 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 Hadamard 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 *generalized Hadamard* (GH) *code*. Note that F_H and C_H are generally nonlinear codes over $\mathbb{F}_q$.

To check whether two GH matrices are equivalent is known to be an NP-hard problem. 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 GH matrices are nonequivalent.

The rank and dimension of the kernel for ordinary Hadamard codes over $\mathbb{F}_2$ have 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 [10], [11]. Moreover, the rank and dimension of the kernel for each nonisomorphic $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard code were also established [12]. The $\mathbb{Z}_2\mathbb{Z}_4$-linear codes are the Gray map image of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, which are subgroups of $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$. Some of these results have been generalized to GH codes over $\mathbb{F}_q$ [3]. In this paper, we continue studying the rank and dimension of the kernel for GH codes over $\mathbb{F}_q$. Now, we focus on an specific family of GH codes, namely the GH additive codes, that is, additive codes obtained from GH matrices.

1 Kronecker sum construction

A standard method to construct GH matrices from other GH matrices is given by the *Kronecker sum construction* [7], [13]. That is, if $H(q,\lambda) = (h_{ij})$ is any $q\lambda \times q\lambda$ GH matrix over $\mathbb{F}_q$, and $B_1, B_2, \ldots, B_{q\lambda}$ are any $q\mu \times q\mu$ GH matrices over $\mathbb{F}_q$, then the matrix in Table 1 gives a $q^2\lambda\mu \times q^2\lambda\mu$ GH matrix over $\mathbb{F}_q$, denoted by $H \oplus [B_1, B_2, \ldots, B_n]$, where $n = q\lambda$. If $B_1 = B_2 = \cdots = B_n = B$, then we write $H \oplus [B_1, B_2, \ldots, B_n] = H \oplus B$.

Table 1: Kronecker sum construction

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

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^t as a GH matrix $H(q, q^{t-1})$, constructed as $S^t = S_q \oplus [S^{t-1}, S^{t-1}, \ldots, S^{t-1}] = S_q \oplus S^{t-1}$ for $t > 1$, which is called a *Sylvester* GH *matrix*.

2 Generalized Hadamard $\mathbb{F}_p$-additive codes

In this section, we state some new results on generalized Hadamard additive codes.

Proposition 2.1 *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 $\mathbb{F}_p$-additive code, then $s = 1$.

(ii) The code C_H is an $\mathbb{F}_p$-additive code if and only if

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

(iii) If C_H is an $\mathbb{F}_p$-additive code and $\ker(C_H) = k$*, then*

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

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

We introduce a new construction of GH codes which allows us to guarantee that the obtained code C_H of length $n = p^t$ is $\mathbb{F}_p$-additive, has kernel of dimension 1, and rank $t+1$.

Proposition 2.2 *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 a $\mathbb{F}_p$-additive code over $\mathbb{F}_{p^e}$ of length $n = p^t$ with* $\ker(C_H) = 1$ *and* $\mathrm{rank}(C_H) = t+1$.

Example 2.3 *In this example, we construct a* GH *matrix* $H(2^2,2)$ *such that* C_H *is a* $\mathbb{F}_2$*-additive code over* $\mathbb{F}_{2^2}$ *of length* $n = 2^3$ *with* $\ker(C_H) = 1$ *and* $\operatorname{rank}(C_H) = 4$. *We begin with the* GH *matrix* $H(2^3,1)$ *given by the multiplicative table of* $\mathbb{F}_{2^3}$, *where* ω *is a primitive element in* $\mathbb{F}_{2^3}$ *and* $\omega^3 = \omega + 1$.

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

Next, we write each entry of the matrix (1) using coordinates over $\mathbb{F}_2$ *and projecting over* $\mathbb{F}_{2^2}$. *By Proposition 2.2, we obtain the* GH *matrix* $H(2^2,2)$, *where* α *is a primitive element in* $\mathbb{F}_{2^2}$ *and* $\alpha^2 = \alpha + 1$. *Note that* $\bar{0} = \overline{(0,0,0)} = (0,0) = 0$, $\bar{1} = \overline{(1,0,0)} = (1,0) = 1$, $\bar{\omega} = \overline{(0,1,0)} = (0,1) = \alpha$, $\bar{\omega}^2 = \overline{(0,0,1)} = (0,0) = 0$, $\bar{\omega}^3 = \overline{(1,1,0)} = (1,1) = \alpha^2$, $\bar{\omega}^4 = \overline{(0,1,1)} = (0,1) = \alpha$, $\bar{\omega}^5 = \overline{(1,1,1)} = (1,1) = \alpha^2$, $\bar{\omega}^6 = \overline{(1,0,1)} = (1,0) = 1$.

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

Proposition 2.4 *For* $q = p^e$, p *prime, and any* $t \geq e > 1$, *there exists a* GH $\mathbb{F}_p$*-additive code* C_H *over* $\mathbb{F}_q$ *of length* $n = p^t$ *with* $\ker(C_H) = k$ *if and only if*

$$\begin{aligned} &(i) \quad k = 2 \text{ when } t = e, \\ &(ii) \quad k \in \{1, \ldots, \lfloor t/e \rfloor\} \text{ when } e \nmid t, \\ &(iii) \quad k \in \{1, \ldots, t/e + 1\} \text{ otherwise.} \end{aligned}$$

Proposition 2.5 *For* $q = p^e$, p *prime, and any* $t \geq e > 1$, *there exists a* GH $\mathbb{F}_p$*-additive code* C_H *over* $\mathbb{F}_q$ *of length* $n = p^t$ *with* $\operatorname{rank}(C_H) = r$ *if and only if*

$$\begin{aligned} &(i) \quad r = 2 \text{ when } t = e, \\ &(ii) \quad r \in \{e + t - (e-1)\lfloor t/e \rfloor, \ldots, t+1 \,|\, \text{in steps of } e-1\} \text{ when } e \nmid t, \\ &(iii) \quad r \in \{t/e + 1, \ldots, t+1 \,|\, \text{in steps of } e-1\} \text{ otherwise.} \end{aligned}$$

Example 2.6 *For $q = 4$, we have the following results:*

- *If $n = 4$, there is only one* GH *matrix $H(4,1)$ over $\mathbb{F}_4$ having* $\mathrm{rank}(C_H) = \mathrm{rank}_2(C_H) = \ker(C_H) = \ker_2(C_H) = 2$. *Therefore, C_H is a linear code and an $\mathbb{F}_2$-additive code, which corresponds to the Sylvester* GH *matrix $S^1 = S_4$.*
- *If $n = 8$, there is only one* GH *matrix $H(4,2)$ over $\mathbb{F}_4$ having* $\mathrm{rank}(C_H) = 4$ *and* $\ker(C_H) = 1$. *Therefore, C_H is nonlinear over $\mathbb{F}_4$. However, it has* $\mathrm{rank}_2(C_H) = \ker_2(C_H) = 2.5$, *so it is an $\mathbb{F}_2$-additive code.*
- *If $n = 16$, it is known that there are 226 nonequivalent* GH *matrices $H(4,4)$ over $\mathbb{F}_4$ [4], which satisfy that* $(\mathrm{rank}(C_H), \ker(C_H)) \in \{(3,3),(4,2),(4,1),(5,2),(5,1),(6,1),(7,1),(8,1)\}$ *[3]. Moreover, if we focus on the $\mathbb{F}_2$-additive codes, we have that they must satisfy* $\mathrm{rank}_2(C_H) = \ker_2(C_H) = 3$. *In this case,* $(\mathrm{rank}(C_H), \ker(C_H)) \in \{(3,3),(4,2),(5,1)\}$. *The first one corresponds to the Sylvester* GH *matrix S^2, which is also linear over $\mathbb{F}_4$.*

References

[1] H. Bauer, B. Ganter, and F. Hergert, "Algebraic techniques for nonlinear codes," Combinatorica, vol. 3, pp. 21–33, 1983.

[2] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*, North-Holland, 1997.

[3] 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.

[4] 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.

[5] D. Jungnickel, "On difference matrices, resolvable designs and generalized Hadamard matrices," Math. Z., vol. 167, pp. 49–60, 1979.

[6] F. I. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, New York, 1977.

[7] Jong-Seon No and H.Y. Song, "Generalized Sylvester-type Hadamard matrices," IEEE International Symposium on Information Theory, pp. 472, 2000.

[8] K. T. Phelps, M. LeVan, "Kernels of nonlinear Hamming codes," Des. Codes Cryptography, vol. 6, pp. 247–257, 1995.

[9] 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.

[10] 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.

[11] 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.

[12] K. T. Phelps, J. Rifà, and M. Villanueva, "On the additive (Z4-linear and non-Z4- linear) Hadamard codes: rank and kernel," IEEE Trans. Inform. Theory, vol. 52(1), pp. 316–319, 2006.

[13] S. S. Shrikhande, "Generalized Hadamard matrices and orthogonal arrays of strength two," Canad. J. Math., vol. 16, pp. 736–740, 1964.