Butson Hadamard full propelinear codes

José Andrés Armario[1], Ivan Bailera[2], Ronan Egan[3]

[1] Universidad de Sevilla, Spain
[2] Universidad de Zaragoza, Spain
[3] National University of Ireland Galway, Ireland

Combinatorial Designs and Codes 2021
Satellite event of the 8th European Congress of Mathematics
July 13, 2021

Outline

Outline

1. Introduction
2. Constructing Butson Hadamard matrices and related codes
   - A Fourier type construction
   - Generalized Gray map
3. Propelinear codes and cocyclic matrices
4. Propelinear codes via the Gray map
5. Conclusions

Butson Hadamard matrix

A matrix $H \in \mathcal{M}_n(\langle \zeta_k \rangle)$ is a **Butson Hadamard matrix** of order n and phase k if fulfils

$$HH^* = nI_n,$$

where I_n denotes the identity matrix of order n and H^* denotes the conjugate transpose of H. Let $\mathrm{BH}(n,k)$ be the set of such matrices.

Example

The Fourier matrices $F_n = [\zeta_n^{(i-1)(j-1)}]_{i,j=1}^n \in \mathrm{BH}(n,n)$.

$$F_n = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_n & \zeta_n^2 & \zeta_n^3 & \cdots & \zeta_n^{n-1} \\ 1 & \zeta_n^2 & \zeta_n^4 & \zeta_n^6 & \cdots & \zeta_n^{2(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_n^{n-1} & \zeta_n^{2(n-1)} & \zeta_n^{3(n-1)} & \cdots & \zeta_n^{(n-1)(n-1)} \end{pmatrix}$$

Logarithmic form

Example

The following is a matrix $H \in \mathrm{BH}(4,8)$*, displayed in logarithmic form*

$$L(H) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 4 & 6 \\ 0 & 4 & 0 & 4 \\ 0 & 6 & 4 & 2 \end{pmatrix}$$

Butson Hadamard code

Given $H \in \mathrm{BH}(n,k)$:

- F_H is the $\mathbb{Z}_k$-code consisting of the rows of $L(H)$.
- C_H is the $\mathbb{Z}_k$-code defined as $C_H = \bigcup_{\alpha \in \mathbb{Z}_k} (F_H + \alpha \mathbf{1})$.

The code C_H over $\mathbb{Z}_k$ is called a **Butson Hadamard code**.

Example

$$F_H = \{[0,0,0,0],[0,2,4,6],[0,4,0,4],[0,6,4,2]\},$$

$$C_H = \left\{ \begin{array}{cccc} [0,0,0,0], & [0,2,4,6], & [0,4,0,4], & [0,6,4,2], \\ [1,1,1,1], & [1,3,5,7], & [1,5,1,5], & [1,7,5,3], \\ [2,2,2,2], & [2,4,6,0], & [2,6,2,6], & [2,0,6,4], \\ [3,3,3,3], & [3,5,7,1], & [3,7,3,7], & [3,1,7,5], \\ [4,4,4,4], & [4,6,0,2], & [4,0,4,0], & [4,2,0,6], \\ [5,5,5,5], & [5,7,1,3], & [5,1,5,1], & [5,3,1,7], \\ [6,6,6,6], & [6,0,2,4], & [6,2,6,2], & [6,4,2,0], \\ [7,7,7,7], & [7,1,3,5], & [7,3,7,3], & [7,5,3,1] \end{array} \right\}.$$

Propelinear structure

Group of all isometries of $\mathbb{Z}_k^n$:

$$\mathrm{Aut}(\mathbb{Z}_k^n) = \{(\sigma, \pi) : \sigma = (\sigma_1, \ldots, \sigma_n),\ \sigma_i \in \mathrm{Sym}\,\mathbb{Z}_k,\ \pi \in \mathcal{S}_n\}$$

Definition

*A code C of length n over $\mathbb{Z}_k$ has a **propelinear structure** if for any codeword $\mathbf{x} \in C$ there exist $\sigma_{\mathbf{x}} = (\sigma_{\mathbf{x},1}, \ldots, \sigma_{\mathbf{x},n})$ with $\sigma_{\mathbf{x},i} \in \mathrm{Sym}\,\mathbb{Z}_k$ and $\pi_{\mathbf{x}} \in \mathcal{S}_n$ satisfying:*

(i) $(\sigma_{\mathbf{x}}, \pi_{\mathbf{x}})(C) = C$ *and* $(\sigma_{\mathbf{x}}, \pi_{\mathbf{x}})(\mathbf{0}) = \mathbf{x}$,

(ii) *if* $\mathbf{y} \in C$ *and* $\mathbf{z} = (\sigma_{\mathbf{x}}, \pi_{\mathbf{x}})(\mathbf{y})$, *then* $(\sigma_{\mathbf{z}}, \pi_{\mathbf{z}}) = (\sigma_{\mathbf{x}}, \pi_{\mathbf{x}}) \circ (\sigma_{\mathbf{y}}, \pi_{\mathbf{y}})$.

Rifà J., Basart J.M., Huguet L., *On completely regular propelinear codes*, Lecture Notes in Computer Science **357**, pp. 341–355 (1989).

Borges J., Mogilnykh I.Y., Rifà J., Solov'eva F., *On the number of nonequivalent propelinear extended perfect codes*, Electronic J. Combinatorics **20**, pp. 1–14, 2013.

Propelinear code

Assuming that C has a propelinear structure, then a binary operation $\star$ can be defined as

$$\mathbf{x} \star \mathbf{y} = (\sigma_{\mathbf{x}}, \pi_{\mathbf{x}})(\mathbf{y}) \quad \text{for any } \mathbf{x}, \mathbf{y} \in C.$$

$(C, \star)$ is a code which is also a group: **propelinear code**.

Full propelinear code

Definition

*A **full propelinear code** is a propelinear code C such that for every $\mathbf{a} \in C$, $\sigma_{\mathbf{a}}(\mathbf{x}) = \mathbf{a} + \mathbf{x}$ and $\pi_{\mathbf{a}}$ has not any fixed coordinate when $\mathbf{a} \neq \alpha\mathbf{1}$ for $\alpha \in \mathbb{Z}_k$. Otherwise, $\pi_{\mathbf{a}} = Id_n$.*

Rifà J., Suárez E., *About a class of Hadamard propelinear codes*, Electronic Notes in Discrete Mathematics **46**, pp. 289–296 (2014).

Armario J.A., Bailera I., Egan R., *Generalized Hadamard full propelinear codes*, Des. Codes Cryptogr. **89**, pp. 599–615 (2021).

Butson Hadamard code + full propelinear code $\Rightarrow$ **Butson Hadamard full propelinear code** (BHFP-code)

Outline

Outline

Kronecker product of Fourier matrix

Example

Let p be a prime number. If $L(D) = [xy^T]_{x,y \in \mathbb{Z}_p^n}$*, then* $D \in \mathrm{BH}(p^n, p)$*. In fact D is the n-fold Kronecker product of the Fourier matrix of order p.*
$p = 3$*,* $n = 1$ *and* $n = 2$

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 \\ 0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \end{pmatrix}$$

When $p = 2$ this is the Sylvester Hadamard matrix of order 2^n.

Recursive matrices

s: positive integer; $t_1, t_2, \ldots, t_s$: non negative integers with $t_1 \geq 1$

$A^{t_1,t_2,\ldots,t_s}$ is defined recursively according to the following algorithm

$(t'_1, t'_2, \ldots, t'_s) \leftarrow (1, 0, \ldots, 0)$

$A^{1,0,\ldots,0} \leftarrow [0]$

for i=1 until s **do**

while $t'_i < t_i$ **do**

$A \leftarrow A^{t'_1,\ldots,t'_s}$

$t'_i \leftarrow t'_i + 1$

$$A^{t'_1,\ldots,t'_s} \leftarrow A_i = \left[\begin{array}{cccc} A & A & \ldots & A \\ 0 \cdot \mathbf{p^{i-1}} & 1 \cdot \mathbf{p^{i-1}} & \ldots & (p^{s-i+1}-1) \cdot \mathbf{p^{i-1}} \end{array}\right]$$

end while

end for

Pinnawala N., Rao A., *Cocyclic simplex codes of type α over Z_4 and $\mathbb{Z}_{2^s}$*, IEEE Trans. Inf. Theory **50**, pp. 2165–2169 (2004).

Recursive matrices

s: positive integer; $t_1, t_2, \ldots, t_s$: non negative integers with $t_1 \geq 1$
$A^{t_1,t_2,\ldots,t_s}$ is defined recursively according to the following algorithm

$(t'_1, t'_2, \ldots, t'_s) \leftarrow (1, 0, \ldots, 0)$
$A^{1,0,\ldots,0} \leftarrow [0]$
for i=1 until s **do**
  while $t'_i < t_i$ **do**
    $A \leftarrow A^{t'_1,\ldots,t'_s}$
    $t'_i \leftarrow t'_i + 1$
    $$A^{t'_1,\ldots,t'_s} \leftarrow A_i = \begin{bmatrix} A & A & \ldots & A \\ 0 \cdot \mathbf{p^{i-1}} & 1 \cdot \mathbf{p^{i-1}} & \ldots & (p^{s-i+1} - 1) \cdot \mathbf{p^{i-1}} \end{bmatrix}$$
  end while
end for

Example

For $p = 2$ and $s = 3$. We have

$$A^{1,1,0} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 4 & 6 \end{bmatrix}, \quad A^{1,1,1} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 4 & 6 & 0 & 2 & 4 & 6 \\ 0 & 0 & 0 & 0 & 4 & 4 & 4 & 4 \end{bmatrix}.$$

Theorem

Let $n = p^{st_1+(s-1)t_2+\ldots+t_s-s}$ and $L(H)$ be the $n \times n$ matrix whose rows are the n possible linear combinations (with coefficients in $\mathbb{Z}_{p^s}$) of the rows of $A^{t_1,t_2,\ldots,t_s}$. Then, $H \in \mathrm{BH}(n, p^s)$.

Proposition

Let $n = p^{st_1+(s-1)t_2+\ldots+t_s-s}$ and $L(H)$ be the $n \times n$ matrix of the previous theorem. Then, H is equivalent to

$$(F_p)^{t_s} \otimes (F_{p^2})^{t_{s-1}} \otimes \ldots \otimes (F_{p^{s-1}})^{t_2} \otimes (F_{p^s})^{t_1-1}$$

where $F_{p^{s-j}}$ denotes the Fourier matrix of order p^{s-j} embedded in $\mathrm{BH}(p^{s-j}, p^s)$ using that $\zeta_{p^{s-j}} = \zeta_{p^s}^{p^j}$, and $(M)^r$ denotes the r-fold Kronecker product of the matrix M.

$\mathbb{Z}_{p^s}$-additive codes

Taking $A^{1,0,\ldots,0} = [1]$ instead of $[0]$
$A^{t_1,t_2,\ldots,t_s}$ is a generator matrix for a $\mathbb{Z}_{p^s}$-additive code of type $(n; t_1, \ldots, t_s)$ where $n = p^{st_1+(s-1)t_2+\ldots+t_s-s}$.

- For $p = 2$

FERNÁNDEZ-CÓRDOBA C.,VELA C., VILLANUEVA M., *On $\mathbb{Z}_{2^s}$-linear Hadamard codes: kernel and partial classification*, Des. Codes and Cryptogr. **87**, pp. 417–435 (2019).

KROTOV D.S., *$\mathbb{Z}_4$-linear Hadamard and extended perfect codes*, International workshop on coding and cryptography, ser. *Electron. Notes Discret. Math.* **6**, pp. 107–112 (2001).

KROTOV D.S., *On $\mathbb{Z}_{2^k}$-dual binary codes*, IEEE Trans. Inf. Theory **53**, pp. 1532–1537 (2007).

- For $p \neq 2$

SHI M., WU R., KROTOV D.S., *On $\mathbb{Z}_p\mathbb{Z}_{p^k}$-additive codes and their duality*, IEEE trans. Inf. Theory **65**, pp. 3841–3847 (2019).

The codes associated to these matrices are denoted by $\mathcal{H}^{t_1,\cdots,t_s}$.

Proposition

For $t_1 > 0$, every $\mathcal{H}^{t_1,\cdots,t_s}$ is a BH-code where the Butson Hadamard matrix is a Kronecker product of Fourier matrices.

Outline

Generalized Gray map

Let $L(D) = [xy^T]_{x,y\in\mathbb{Z}_p^{s-1}}$, then $D \in \mathrm{BH}(p^{s-1}, p)$.

Label the rows of $L(D)$ in the order $0, 1, \ldots, p^{s-1} - 1$.

Let $[L(D)]_i$ denote the row of $L(D)$ labeled by i.

$$\Phi_p : \mathbb{Z}_{p^s} \to \mathbb{Z}_p^{p^{s-1}}$$

$$\Phi_p(x) = [L(D)]_b + a\mathbf{1}, \quad x = ap^{s-1} + b.$$

- For $p = 2$

  Carlet C., $\mathbb{Z}_{2^k}$*-linear codes*, IEEE Trans. Inf. Theory **44**, pp. 1543–1547 (1998).

- For $p > 2$

  Shi M., Wu R., Krotov D.S., *On* $\mathbb{Z}_p\mathbb{Z}_{p^k}$*-additive codes and their duality*, IEEE trans. Inf. Theory **65**, pp. 3841–3847 (2019).

Given $H \in \mathcal{M}_n(\langle \zeta_{p^s} \rangle)$, we write $L(H^{\Phi_p})$ for the entrywise application of Φ_p to

$$\begin{bmatrix} L(H) \\ L(H)+J \\ L(H)+2J \\ \vdots \\ L(H)+(p^{s-1}-1)J \end{bmatrix}$$

where J denotes the $n \times n$ matrix of all ones. Then H^{Φ_p} is the corresponding matrix in $\mathcal{M}_{np^{s-1}}(\langle \zeta_p \rangle)$.

Theorem

If $H \in \mathrm{BH}(n, p^s)$, then $H^{\Phi_p} \in \mathrm{BH}(np^{s-1}, p)$.

Corollary

The image of any BH-code over $\mathbb{Z}_{p^s}$ of length n by Φ_p is a BH-code over $\mathbb{Z}_p$ of length $n \cdot p^{s-1}$ and minimum Hamming distance $d_H = np^{s-2}(p-1)$.

Let $k = p^s m$ where p does not divide m.

Recall that every element $x \in \mathbb{Z}_k$ can be written uniquely as $x = ap^s + bm \mod k$ for some $0 \le a \le m-1$ and $0 \le b \le p^s - 1$.

$$\Psi_p : \mathbb{Z}_k \to \mathbb{Z}_{pm}^{p^{s-1}}$$
$$\Psi_p(x) = m\Phi_p(b) + ap\mathbf{1}$$

Given $H \in \mathcal{M}_n(\langle \zeta_k \rangle)$ where $k = p^s m$, we write $L(H^{\Psi_p})$ for the entrywise application of Ψ_p to

$$\begin{bmatrix} L(H) \\ L(H) + mJ \\ L(H) + 2mJ \\ \vdots \\ L(H) + (p^{s-1} - 1)mJ \end{bmatrix}.$$

Then H^{Ψ_p} is the corresponding matrix in $\mathcal{M}_{np^{s-1}}(\langle \zeta_{pm} \rangle)$.

Theorem

If $H \in \mathrm{BH}(n, k)$ where $k = p^s m$, then $H^{\Psi_p} \in \mathrm{BH}(np^{s-1}, pm)$.

Repeated application of Ψ_p for all primes p dividing k gives the following.

Corollary

If $H \in \mathrm{BH}(n,k)$ where $k = p_1^{s_1} \cdots p_r^{s_r}$, then $H^{\Psi} \in \mathrm{BH}(nk/\ell, \ell)$ where $\ell = p_1 \cdots p_r$, and $\Psi = \Psi_{p_1} \cdots \Psi_{p_r}$.

Ó Catháin P., Swartz E., *Homomorphisms of matrix algebras and constructions of Butson-Hadamard matrices*, Disc. Math. **342**(12), 111606 (2019).

Proposition

Let $H \in \mathrm{BH}(n, p^s m)$ with p a prime not dividing m. Let d be the minimum Hamming distance of C_H. Then the minimum distance d' of $\Psi(C_H)$ is in the range $d(p-1)p^{s-2} \leq d' \leq dp^{s-1}$.

Outline

Proposition

Given $\psi \in Z^2(G, \langle \zeta_k \rangle)$ *and* $\mathbf{x} = \zeta_k^{\lambda}\,[\psi(g, g_1), \ldots, \psi(g, g_n)]$ *for a fixed order in* $G = \{g_1 = 1, g_2, \ldots, g_n\}$*. Define* $\pi_{\mathbf{x}} \in \mathcal{S}_n$ *so that* $\pi_{\mathbf{x}}^{-1}(j) = k$ *where* $g_k = gg_j$*. Then*

1. $\mathbf{x} + \pi_{\mathbf{x}}(y) = \zeta_k^{\lambda+\mu}\,\psi(h, g)\,[\psi(hg, g_1), \ldots, \psi(hg, g_n)]$ *where* $+$ *means the componentwise product and* $\mathbf{y} = \zeta_k^{\mu}\,[\psi(h, g_1), \ldots, \psi(h, g_n)]$.
2. $\pi_{\mathbf{x}+\pi_{\mathbf{x}}(\mathbf{y})} = \pi_{\mathbf{x}}(\pi_{\mathbf{y}})$.

Corollary

Let $\psi \in Z^2(G, \langle \zeta_k \rangle)$ *and* $H_\psi \in \mathrm{BH}(n, k)$*. Then the corresponding BH-code* C_{H_ψ} *is a BHFP-code where* $\mathbf{x} \star \mathbf{y} = \mathbf{x} + \pi_{\mathbf{x}}(\mathbf{y})$ *for all* $\mathbf{x}, \mathbf{y} \in C_{H_\psi}$*.*

Corollary

Let C_H *be a BHFP-code of length* n *over* $\mathbb{Z}_k$ *coming from* $H \in \mathrm{BH}(n, k)$*, where* H *is row and column balanced. Then* H *is cocyclic.*

Example

Considering $\mathcal{H}^{1,1,1}$, the $\mathbb{Z}_8$-additive code of length $n = 8$ associated to

$$L(H) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 4 & 6 & 0 & 2 & 4 & 6 \\ 0 & 4 & 0 & 4 & 0 & 4 & 0 & 4 \\ 0 & 6 & 4 & 2 & 0 & 6 & 4 & 2 \\ 0 & 0 & 0 & 0 & 4 & 4 & 4 & 4 \\ 0 & 2 & 4 & 6 & 4 & 6 & 0 & 2 \\ 0 & 4 & 0 & 4 & 4 & 0 & 4 & 0 \\ 0 & 6 & 4 & 2 & 4 & 2 & 0 & 6 \end{pmatrix}.$$

Then, it can be endowed with a ***full propelinear structure*** *with the group of permutations $\Pi \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ generated by $\pi_{\mathbf{x}}$ and $\pi_{\mathbf{y}}$ where*

$$\mathbf{x} = [0,2,4,6,0,2,4,6], \qquad \mathbf{y} = [0,0,0,0,4,4,4,4],$$
$$\pi_{\mathbf{x}} = (1,4,3,2)(5,8,7,6), \quad \pi_{\mathbf{y}} = (1,5)(2,6)(3,7)(4,8).$$

The full propelinear code is a group $(\mathcal{H}^{1,1,1}, \star) \cong \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2 = \langle \mathbf{x}, \mathbf{y}, \mathbf{1} \mid \mathbf{x}^8 = \mathbf{0},\ \mathbf{y}^2 = \mathbf{1}^4 = \mathbf{x}^4 \rangle$.

Outline

Full propelinear codes via the Gray map

Theorem

Let m be an odd positive integer, and let $C \subseteq \mathbb{Z}_{4m}^n$ be a full propelinear code. Then the code $C' = \Psi_2(C)$ is full propelinear with group structure $(C', \star') \cong (C, \star)$.

Corollary

Let m be an odd positive integer, and let $H \in \mathrm{BH}(n, 4m)$. If the BH-code C obtained from H is full propelinear with group structure G, then the BH-code C' obtained from H^{Ψ_2} is full propelinear with group structure $G' \cong G$.

Example

Let $\mathcal{H}^{3,0}$ be the BH-code associated to $F_4 \otimes F_4 \in \mathrm{BH}(16,4)$ and $H^{3,0}$ be its image by the Gray map which is known to be a non-linear code.
$\mathcal{H}^{3,0}$ is full propelinear, with permutation group $\mathbb{Z}_4^2$ generated by $\pi_{\mathbf{x}}$ and $\pi_{\mathbf{y}}$ where

$$\mathbf{x} = [0,1,2,3,0,1,2,3,0,1,2,3,0,1,2,3],$$
$$\mathbf{y} = [0,0,0,0,1,1,1,1,2,2,2,2,3,3,3,3],$$
$$\pi_{\mathbf{x}} = (1,4,3,2)(5,8,7,6)(9,12,11,10)(13,16,15,14),$$
$$\pi_{\mathbf{y}} = (1,13,9,5)(2,14,10,6)(3,15,11,7)(4,16,12,8).$$

$H^{3,0}$ can be endowed with a **full propelinear structure** with permutation group $\langle \pi_{\Psi_2(x)}, \pi_{\Psi_2(y)} \rangle$, which is non-abelian of order 32.

Example

$$\pi_{\Psi_2(x)} = (1,7,6,4)(2,8,5,3)(9,15,14,12)(10,16,13,11)(17,23,22,20)(18,24,21,19)(25,31,30,28)(26,32,29,27),$$

$$\pi_{\Psi_2(y)} = (1,25,17,9)(2,26,18,10)(3,28,19,12)(4,27,20,11)(5,29,21,13)(6,30,22,14)(7,32,23,16)(8,31,24,15).$$

The groups $(\mathcal{H}^{3,0},\star) \cong (H^{3,0},\star')$ are isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8$.

Outline

Conclusions

- We introduce a new morphism of Butson Hadamard matrices $\mathrm{BH}(n,k) \to \mathrm{BH}(nk/\ell, \ell)$ through a generalized Gray map on the matrices in logarithmic form.

$$\Psi_p : \mathbb{Z}_k \to \mathbb{Z}_{mp}^{p^{s-1}}$$

$$\Psi_p(x) = m\Phi_p(b) + ap\mathbf{1}$$

- We give an equivalence between cocyclic Butson Hadamard matrices and BHFP-codes.
- We find that for the special case $\Psi_2 : \mathbb{Z}_{4m} \to \mathbb{Z}_{2m}^2$, we can construct an isomorphism between the groups of codewords C and $C' = \Psi_2(C)$, and determine the group operation $\star'$ so that $(C, \star) \cong (C', \star')$.

Thanks for your attention

Hvala na pozornosti