Hadamard full propelinear codes of type CQ. Rank and Kernel

Iván Bailera, Joaquim Borges, and Josep Rifà

Department of Information and Communications Engineering

Universitat Autònoma de Barcelona

5th Workshop on Real and Complex Hadamard Matrices and Applications
Budapest, 10 - 14 July 2017

Outline

Outline

Motivation

Conjecture (Hadamard, XIX c.)

A Hadamard matrix of order $4t$ exists for every positive integer t.

Conjecture (De Launey and Horadam, 1993)

There is a cocyclic Hadamard matrix of order $4t$ for every positive integer t.

Conjecture (Ito, 1994)

There exists a Hadamard group of order $8t$ for every positive integer t.

Outline

Preliminaries

A (binary) **code**, C, over $\mathbb{F}$ is a subset of the vector space $\mathbb{F}^n$.

- A codeword is an element of C.
- n is the length of the code.
- $M = |C|$.
- **Hamming distance**: $d_H(x, y)$ is the number of the coordinates in which x and y differ, $x, y \in \mathbb{F}^n$.
- **Minimum distance**: $d_H(u, v) \geq d \ \forall u, v \in C$ with $u \neq v$.
- **Hamming weight**: $\mathrm{wt}_H(x) = d_H(x, \mathbf{e})$.
- $\mathbf{e} = (0, \ldots, 0)$, $\mathbf{u} = (1, \ldots, 1)$.

Notation: **(n, M, d)-code**

Code

Example

$$C = \{(0,0,0,0,0,0),(0,0,1,1,1,0),(0,1,0,1,0,1),(0,1,1,0,1,1),(1,0,0,0,1,1),(1,0,1,1,0,1),(1,1,0,1,1,0),(1,1,1,0,0,0)\}$$

C is a $(6,8,3)$*-binary code.* $C = \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&1&1&1&0\\ 0&1&0&1&0&1\\ 0&1&1&0&1&1\\ 1&0&0&0&1&1\\ 1&0&1&1&0&1\\ 1&1&0&1&1&0\\ 1&1&1&0&0&0 \end{bmatrix}$

Rank and Kernel

The **rank** of a code C is the dimension of the linear span of C.
The **kernel** of a code is the set of words which keeps the code invariant by translation

$$K(C) := \{z \in \mathbb{F}^n \mid C + z = C\} \subseteq \mathbb{F}^n$$

Notation:
rank: r
the dimension of the kernel: k.

Hadamard matrix

Definition

A **Hadamard matrix** is a $n \times n$ matrix H containing entries from the set $\{1, -1\}$, with the property that:

$$HH^T = nI,$$

where I is the identity matrix.

Binary Hadamard matrix

Definition

The matrix obtained from a Hadamard matrix, by replacing all 1's by 0's and all -1's by 1's, is called **binary Hadamard matrix**.

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix} \longrightarrow \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

Hadamard code

Definition

A binary **Hadamard code** is the binary code consisting of the rows of a binary Hadamard matrix and their complements.

$$H_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \; C = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

C is a $(4, 8, 2)$-code.

In general, a Hadamard code of length n is a $(n, 2n, n/2)$-code.

Propelinear code

Definition

A binary code C of length n has a **propelinear structure** if for each codeword $x \in C$ there exists $\pi_x \in S_n$ satisfying the following conditions:

i) For all $x, y \in C$, $x + \pi_x(y) \in C$,

ii) For all $x, y \in C$, $\pi_x \pi_y = \pi_z$, where $z = x + \pi_x(y)$.

- $(C, *)$ is a group, where $*$ is the **propelinear operation** $x * y = x + \pi_x(y)$, $\forall x \in C$, $\forall y \in \mathbb{F}^n$.
- We call $(C, *)$ a **propelinear code**.

RIFÀ J., BASART J. M., AND L. HUGUET, *On completely regular propelinear codes*, Lecture Notes in Computer Science **357** (1989), pp. 341–355.

Hadamard full propelinear code

Definition

A **Hadamard full propelinear code** (HFP) is a Hadamard propelinear code C such that for every $\mathbf{a} \in C$, $\mathbf{a} \neq \mathbf{e}$, $\mathbf{a} \neq \mathbf{u}$ the permutation $\pi_{\mathbf{a}}$ has not any fixed coordinate and $\pi_{\mathbf{e}} = \pi_{\mathbf{u}} = Id$.

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

Hadamard full propelinear code

$$C = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}, \qquad \begin{aligned} \pi_{\mathbf{e}} &= Id \\ \pi_{(0011)} &= (1\,2)(3\,4) \\ \pi_{(0110)} &= (1\,4)(2\,3) \\ \pi_{(0101)} &= (1\,3)(2\,4) \\ \pi_{\mathbf{u}} &= Id \\ \pi_{(1100)} &= (1\,2)(3\,4) \\ \pi_{(1001)} &= (1\,4)(2\,3) \\ \pi_{(1010)} &= (1\,3)(2\,4) \end{aligned}$$

$$C \simeq C_2 \times C_2 \times C_2$$

Relative difference set

Definition

A set D of k elements in a group G of order mn is a **difference set of G relative to a normal subgroup** N of order $n \neq mn$ if the collection of the products $d_i d_j^{-1}$ of distinct elements $d_i, d_j \in D$ contains only elements of G which are not in N, and contains every such element exactly λ times.

Elliot, J. E. H. and A. T. Butson, *Relative difference sets*, Illinois J. Math **10** (1966), pp. 517–531.

Hadamard group

Definition

G is a **Hadamard group** of order $8t$, if it is a finite group containing a $4t$-subset D and a central involution $\mathbf{u}$ (D is called Hadamard subset corresponding to $\mathbf{u}$), such that

i) D and $\mathbf{u}D$ are disjoint and $D \cup \mathbf{u}D = G$,

ii) aD and D intersect exactly in $2t$ elements, for any $a \notin \langle \mathbf{u} \rangle \subset G$,

iii) aD and $\{b, b\mathbf{u}\}$ intersect exactly in one element, for any $a, b \in G$.

Ito, N., *On Hadamard groups*, Journal of Algebra **168** (1994), pp. 981–987.

Ito, N., *On Hadamard groups II*, Journal of Algebra **169** (1994), pp. 936–942.

Ito, N., *On Hadamard groups III*, Kyushu Journal of Mathematics **51** (1997), pp. 369–379.

Cocyclic matrix

Definition

A **cocycle** (over G) is a map $f : G \times G \to \mathbb{F}$ which satisfies $\psi(g,h)\psi(gh,k) = \psi(g,hk)\psi(h,k)$, $\forall g,h,k \in G$.

Definition

A $n \times n$ binary matrix M is **cocyclic** (over G, developed by ψ) if there exists a group development function $\phi : G \to \mathbb{F}$ and a cocycle ψ such that $M = [\psi(g,h)\phi(gh)]$, $\forall g,h \in G$.

HORADAM, K. J. AND W. DE LAUNEY, *A weak difference set construction for higher-dimensional designs*, Designs, Codes and Cryptography **3** (1993), pp. 75–87.

HORADAM, K. J. AND W. DE LAUNEY, *Generation of cocyclic Hadamard matrices*, Computational Algebra and Number Theory **325** (1995), pp. 279–290.

Relations

Difference set - Hadamard group.

ITO, N., *On Hadamard groups II*, Journal of Algebra **169** (1994), pp. 936–942.

Cocyclic Hadamard matrix - Hadamard group

FLANNERY, D., *Cocyclic Hadamard matrices and Hadamard groups are equivalent*, Journal of Algebra **192** (1997), pp. 749–779.

Cocyclic Hadamard matrix - Difference set

DE LAUNEY, W., D. L. FLANNERY, AND K.J. HORADAM, *Cocyclic Hadamard matrices and difference sets*, Discrete Applied Mathematics **102** (2000), pp. 47–61.

HFP-code - Hadamard group

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

Outline

HFP-codes of type CQ

Definition

Let C be an HFP code of length $4t$. We will say that C is an HFP-code of type CQ when C is the direct product $C_t \times Q$, where C_t is a cyclic group of order t and Q is the quaternion group of eight elements.

Its group of permutations $(\{\pi_x \in S_n : x \in C\})$ is $C_t \times C_2^2$.

BALIGA, A. AND K. J. HORADAM, *Cocyclic Hadamard matrices over* $\mathbb{Z}_n \times \mathbb{Z}_2^2$, Australasian Journal of Compinatorics **11** (1995), pp. 123–134.

HFP-codes of type CQ

Let C be an HFP-code of type CQ. A presentation of C is:

$$C = \langle \mathbf{d}, \mathbf{a}, \mathbf{b} \mid \mathbf{d}^t = \mathbf{a}^4 = \mathbf{b}^4 = \mathbf{e}, \mathbf{a}^2 = \mathbf{b}^2 = \mathbf{u}, \mathbf{aba} = \mathbf{b} \rangle.$$

HFP-codes of type CQ

Proposition

Let C be an HFP*-code of type CQ of length $4t$. Then, up to equivalence, we have*

i) $\pi_{\mathbf{d}} = (1, 5, \dots, 4t-3)(2, 6, \dots, 4t-2)(3, 7, \dots, 4t-1)$ $(4, 8, \dots, 4t)$,

ii) $\pi_{\mathbf{a}} = (1, 2)(3, 4) \dots (4t-1, 4t)$,

iii) $\pi_{\mathbf{b}} = (1, 3)(2, 4) \dots (4t-3, 4t-1)(4t-2, 4t)$,

iv) $\mathbf{a} = (A_1, A_2, \dots, A_t)$ *where* $A_i \in \{(0, 1, 0, 1), (1, 0, 1, 0), (0, 1, 1, 0), (1, 0, 0, 1)\}$.

v) *Knowing the value of* $\mathbf{d}$ *is enough to define* $\mathbf{a}$ *and* $\mathbf{b}$.

vi) $\{\pi_x \in S_n : x \in C\} = C_t \times C_2^2$.

Rank and dimension of the kernel

Proposition

Let C be an HFP*-code of type CQ of length $4t$ which is not linear*

i) *If t is odd, then $r = 4t - 1$ and $k = 1$.*

ii) *If t is even, then $r \leq 2t$, and $r = 2t$ if $t \equiv 2 \pmod 4$.*

Proof. Easy from

Assmus, E. and J.D. Key, *Designs and their codes*, Cambridge Tracts in Mathematics **103** (1992).

Kernel

Theorem

Let C be an HFP*-code of type $CQ = \langle \mathbf{d}, \mathbf{a}, \mathbf{b} \rangle$ of length $4t$. Then*

i) $k \leq 3$.

ii) *If $k = 3$, then $K(C) = \langle \mathbf{u}, \mathbf{d}^{t/2}, \mathbf{g} \rangle$, where $\mathbf{g} \in \langle \mathbf{a}, \mathbf{b} \rangle$.*

iii) *If $k = 2$, then $K(C) = \langle \mathbf{u}, \mathbf{d}^{t/2}\mathbf{g} \rangle$, where $\mathbf{g} \in \langle \mathbf{a}, \mathbf{b} \rangle$.*

iv) *If $k = 1$, then $K(C) = \langle \mathbf{u} \rangle$.*

Example

Example

We have constructed all codes of type $CQ = \langle \mathbf{d}, \mathbf{a}, \mathbf{b} \rangle$ *of length* 16, *i.e.* $t = 4$. *There are two types of generated codes, one of them are linear codes with* $r = 5$ *and* $k = 5$, *and the other are nonlinear codes with* $r = 7$ *and* $k = 2$. *For instance, the values for the generators* $\mathbf{d}$, $\mathbf{a}$ *and* $\mathbf{b}$ *are the following:*

$$\begin{aligned}
\mathbf{d} &= (0,1,1,1,\quad 0,1,1,1,\quad 1,0,0,0,\quad 1,0,0,0),\\
\mathbf{a} &= (1,0,0,1,\quad 0,1,0,1,\quad 1,0,0,1,\quad 0,1,0,1),\\
\mathbf{b} &= (1,1,0,0,\quad 0,1,1,0,\quad 1,1,0,0,\quad 0,1,1,0),\\
\pi_{\mathbf{d}} &= (1,5,9,13)(2,6,10,14)(3,7,11,15)(4,8,12,16),\\
\pi_{\mathbf{a}} &= (1,2)(3,4)(5,6)(7,8)(9,10)(11,12)(13,14)(15,16),\\
\pi_{\mathbf{b}} &= (1,3)(2,4)(5,7)(6,8)(9,11)(10,12)(13,15)(14,16).
\end{aligned}$$

Magma results

t		2	3	4		5	6	7	8			9	10	11	12	13	14	15	16	17	18	19
$C_t \times Q$	r	4	11	5	7	19	12	27	8	9	11	35	20		13	51	22	59			36	75
	k	4	1	5	2	1	2	1	3	2	2	1	2		3	1	2	1			2	1

t		20	21	22	23	24	25	26	27	28	30	36	38	42	50	52	54	60	76	84	100	108
$C_t \times Q$	r	21	83				99	52	107	23	60	37	76	84	100	108	61	83	77	85	101	109
	k	23	1				1	2	1	3	2	3	2	2	2	3	2	3	3	3	3	3

Outline

Summary

- A new subclass of Hadamard full propelinear codes is introduced.
- We define the HFP-codes of type CQ as codes with a group structure isomorphic to $C_t \times Q$.
- For t odd, $r = 4t - 1$ and $k = 1$. For t even, $r \leq 2t$, and $r = 2t$ if $t \equiv 2 \pmod 4$.
- The dimension of the kernel is less than or equal to 3.
    - $K(C) = \langle \mathbf{u}, \mathbf{d}^{t/2}, \mathbf{g} \rangle$, where $\mathbf{g} \in \langle \mathbf{a}, \mathbf{b} \rangle$.
    - $K(C) = \langle \mathbf{u}, \mathbf{d}^{t/2}\mathbf{g} \rangle$, where $\mathbf{g} \in \langle \mathbf{a}, \mathbf{b} \rangle$.
    - $K(C) = \langle \mathbf{u} \rangle$.

PhD on-going work

- HFP-codes which are extensions of $C_t \times C_2^2$ by C_2:
  - $C_t \times C_2^3$, $C_{2t} \times C_2^2$.
  - $C_t \times C_4 \times C_2$, $C_{2t} \times C_4$, $C_{4t} \times C_2$.
  - $C_t \times D$.

More references

- BORGES, J., I. Y. MOGILNNYKH, J. RIFÀ, AND F. I. SOLOV'EVA, *Structural properties of binary propelinear codes*, Advances in Mathematics of Communications **6** (2012), pp. 329–343.
- ITO, N., *Some results on Hadamard groups*, Proc. Groups Korea 1994 (1995), pp. 149–155.
- SCHMIDT, B., *Williamson matrices and a conjecture of Ito's*, Designs, Codes and Cryptography **17** (1999), pp. 61–68.

Thanks for your attention!