Codes from groups and groups from codes

K. J. Horadam

RMIT University, Melbourne, Australia

5th Hadamard Workshop
Budapest, July 10-14 2017

Outline

Outline

Binary Hadamard matrices

H a binary Hadamard matrix of order $4t$ if:

- it is $4t \times 4t$ with entries $\{0, 1\}$
- every pair of distinct rows (and columns) differs in exactly $2t$ places
- usually normalised to all 0 in first row and column

Smallest example [Sylvester 1867]...$\sim$ 150 years ago:

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

The Hadamard Conjecture

- Conjecture (still open after 150 years): there exists a HM order $4t$ for every t. Lowest open order is 668.
- Cocyclic Hadamard Conjecture: there exists a cocyclic HM order $4t$ for every t [De Launey, KJH 1993]. Lowest open order is188. Many construction techniques for HM are cocyclic.
- Won't discuss cocycles here, just the simplest kind: coboundaries.

Coboundaries and Hadamard matrices

For any group function $f : G \to H$ with $f(1) = 1$ its coboundary is

$$\partial f(x, y) = f(x)^{-1} f(y)^{-1} f(xy)$$

- ∂f measures how much f differs from a homomorphism
- Example: for vector spaces, f a quadratic form and ∂f its polar bilinear form
- the corresponding coboundary matrix is

$$[\partial f(x, y)]_{x,y \in G}$$

It is a normalised group-developed/group-invariant matrix.

Coboundaries and Hadamard matrices...cont

eg $f : \mathbb{Z}_4 \to \mathbb{Z}_2$ given by $f(0) = f(1) = f(2) = 0, f(3) = 1$:

$$[f(xy)]_{x,y \in \mathbb{Z}_4} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} = [\partial f(x, y)]_{x,y \in \mathbb{Z}_4}$$

after normalising. These are also Hadamard matrices.

If a coboundary matrix is Hadamard then $4t = (2u)^2$.

Outline

Binary codes

- Binary code C of length n = subset of $\mathbb{Z}_2^n$.
- Parameters of C : (n, M, d) length n, number of codewords M, minimum Hamming distance d
- C is linear if = subgroup of $\mathbb{Z}_2^n$ (ie closed under addition, so $M = 2^k$)
- If C nonlinear it generates a linear code $\langle C \rangle$ with rank r.

Hadamard codes

Hadamard code: rows of binary Hadamard matrix & their complements
Parameters $n = 4t,\ M = 8t,\ d = 2t$, rank ????
Can assume all-zeroes **0** and all-ones **1** are in C
Includes Reed-Muller codes used for US deep space and Mars missions

eg (our coboundary HM) $n = 4,\ M = 8, d = 2$, linear, rank $r = 3$

$$\begin{array}{cccccccc} 0 & 0 & 0 & 0\,, & 1 & 1 & 1 & 1\,, \\ 0 & 0 & 1 & 1\,, & 1 & 1 & 0 & 0\,, \\ 0 & 1 & 0 & 1\,, & 1 & 0 & 1 & 0\,, \\ 0 & 1 & 1 & 0\,, & 1 & 0 & 0 & 1\,. \end{array}$$

This talk now develops in two directions

map $f : \mathbb{Z}_4 \to \mathbb{Z}_2$	Hadamard code
matrix $[\partial f(x,y)]_{x,y \in \mathbb{Z}_4}$	
code $\begin{matrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{matrix}$	$\begin{matrix} 0 & 0 & 0 & 0, & 1 & 1 & 1 & 1, \\ 0 & 0 & 1 & 1, & 1 & 1 & 0 & 0, \\ 0 & 1 & 0 & 1, & 1 & 0 & 1 & 0, \\ 0 & 1 & 1 & 0, & 1 & 0 & 0 & 1. \end{matrix}$
$\Downarrow$	$\Downarrow$
map $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$	A propelinear code is a group
code $\{\partial f(x,y), x, y \in \mathbb{Z}_2^n\}$	Hadamard propelinear code

Outline

Why do we care? The cryptographic imperative

- In cryptography, we are VERY interested in $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ which are as "featureless" as possible
- Use different ideas of featurelessness, ie high nonlinearity
- Measure using eg Discrete Fourier Transform, group characters or difference distributions
- Classify functions f into equivalence classes invariant under these measures
- Two main classifications: CCZ equivalence and EA equivalence; EA $\Rightarrow$ CCZ.
- Look for classes with optimal featurelessness

Outline

The coboundary code

$f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ and $f(0) = 0$. The *coboundary code* of f in $\mathbb{Z}_2^n$ is

$$\mathcal{D}_f = \{\partial f(x, y) \ : \ x,\ y \in \mathbb{Z}_2^n\} = \{f(g)+f(h)+f(g+h) \ : \ x,\ y \in \mathbb{Z}_2^n\}.$$

It generates a *linear* code $\langle \mathcal{D}_f \rangle$.

$$n(f) = \mathrm{rank}_2\, \mathcal{D}_f = \dim_2 \langle \mathcal{D}_f \rangle, \quad 0 \leq n(f) \leq n.$$

Theorem (KJH-Villanueva 2014)

If f and f' are EA equivalent, then $n(f) = n(f')$.

Does the coboundary code $\mathcal{D}_f$ play a similar role for EA classes as the graph code does for CCZ classes?

Outline

The kernel of a code

What other invariants are there?

Kernel introduced in 1983 (Bauer, Ganter and Hergert).

Kernel $K(C)$ of a binary code C of length n is

$$K(C) = \{x \in \mathbb{Z}_2^n \ : \ x + C = C\}.$$

If $\mathbf{0} \in C$, then $K(C)$ is a linear subspace of C and is a union of cosets of C.

- $K(\mathcal{D}_f)$ is a linear subcode of $\mathcal{D}_f$. Set $k(f) = \dim_2 K(\mathcal{D}_f)$.
- We have $K(\mathcal{D}_f) \subseteq \mathcal{D}_f \subseteq \langle \mathcal{D}_f \rangle$, so $0 \leq k(f) \leq n(f) \leq n$.

The kernel of the code $\mathcal{D}_f$

Usually, the dimension $k(f)$ of the kernel is not, by itself, an invariant of EA class

But the SET of dimensions of the kernels of the shifts of f IS an invariant. For $r \in \mathbb{Z}_2^n$ the shift of f by r is

$$f \cdot r(x) = f(x+r) + f(r) \quad [= \partial f(x,r) + f(x)].$$

Theorem (KJH-Villanueva 2014)

Let $M(f) = \{\{k(f \cdot r),\ r \in \mathbb{Z}_2^n\}\}$.
If f and f' are EA equivalent, then $M(f) = M(f')$.

Example: Power functions

i	$M(f(x) = x^i)$
$i \in C_1$	$\{0^\wedge 2^m\}$
$i \notin C_1$	$\{\lvert C_i \rvert^\wedge 2^m\}$

Table: Invariant multiset $M(f)$ for the monomial power functions $f(x) = x^i$ for all $3 \leq m \leq 8$, where C_i is the cyclotomic coset of i mod $2^m - 1$.

In these cases we have very simple and uniform results in terms of the cyclotomic coset C_i of i mod $2^m - 1$. For instance, for $m = 4$, $M(x^5) = \{2^\wedge 16\}$ and for $m = 6$, $M(x^9) = \{3^\wedge 64\}$.

Example: Differentially 4-uniform permutations of order 15

Here there are 10 CCZ classes. The dimension $k(f \cdot r)$ of $K(\mathcal{D}_{f \cdot r})$ CAN vary with the shift r within an EA class.

$M(\sigma_1) = \{0^\wedge 8, 1^\wedge 4, 4^\wedge 4\}$,
$M(\sigma_2) = \{1^\wedge 6, 4^\wedge 10\}$,
$M(\sigma_3) = \{4^\wedge 16\}$,
$M(\sigma_4) = \{0^\wedge 4, 4^\wedge 12\}$,
$M(\sigma_5) = \{0^\wedge 6, 4^\wedge 10\}$,
$M(\sigma_6) = \{0^\wedge 4, 4^\wedge 12\}$,
$M(\sigma_7) = \{0^\wedge 15, 4\}$,
$M(\sigma_8) = \{0^\wedge 10, 4^\wedge 6\}$,
$M(\sigma_9) = \{0^\wedge 8, 4^\wedge 8\}$,
$M(\sigma_{10}) = \{4^\wedge 16\}$.

Further work

Really we know very little about these invariants of equivalence classes:

- So far, calculated for some power functions $f(x) = x^i$, some highly nonlinear functions and some small n.
- How well do they characterise nonlinearity classes for functions over $\mathbb{Z}_2^n$?
- The area is wide open for investigation....

Outline

Propelinear codes

- Introduced by Rifà, Basart, Huguet (1989)
- Binary code C of length n, containing $\mathbf{0}$, is propelinear, if for each codeword $x \in C$ there exists a coordinate permutation $\pi_x \in S_n$ satisfying conditions:
  (i) $\pi_{\mathbf{0}} = Id$,
  (ii) For all $y \in C, x + \pi_x(y) \in C$,
  (iii) For all $x, y \in C, \pi_x \pi_y = \pi_z$, where $z = x + \pi_x(y)$.

Propelinear codes are groups!

Theorem (Rifà et al)

A propelinear code C is a group under the binary operation $\star$, where

$$x \star y = x + \pi_x(y), \quad x, y \in C$$

Proof.

Identity is $\mathbf{0}$: $\mathbf{0} \star x = \mathbf{0} + \pi_{\mathbf{0}}(x) = \mathbf{0} + Id(x) = x$;
$x \star \mathbf{0} = x + \pi_x(\mathbf{0}) = x + \mathbf{0} = x$.
Associativity follows from Condition (iii).
Inverse of x is $x^{-1} = (\pi_x)^{-1}(x)$. eg if $(\pi_x)^{-1}(x) = z$ then $\pi_x(z) = x$, so
$x \star (\pi_x)^{-1}(x) = x + \pi_x((\pi_x)^{-1}(x)) = x + \pi_x(z) = x + x = \mathbf{0}$.
Proof that $(\pi_x)^{-1}(x) \star x = \mathbf{0}$ takes a little more work! □

What group is that?

QUESTION 1 In a propelinear code C, for every $x \in C$, $x + \pi_x(C) = C$. What is the relation (if any) with the Kernel $K(C) = \{x \in \mathbb{Z}_2^n \ : \ x + C = C\}$?

QUESTION 2 What group is the propelinear code $(C, \star)$?

First, $(C, \star)$ is abelian if and only if

$x \star y = x + \pi_x(y) = y + \pi_y(x), x, y \in C$; usually NOT the case.

If C is also a Hadamard code some really lovely results are known.

In a Hadamard propelinear code C, as well as containing $\mathbf{0}$ (with $\pi_{\mathbf{0}} = Id$), C contains $\mathbf{1}$.

In a Hadamard propelinear code C,

$\mathbf{1} \star \mathbf{1} = \mathbf{1} + \pi_{\mathbf{1}}(\mathbf{1}) = \mathbf{1} + \mathbf{1} = \mathbf{0}$ and $\mathbf{1}$ is an involution in C.

Outline

The Hadamard full propelinear code group is known

A Hadamard propelinear code is called full if
(i) $\pi_{\mathbf{0}} = \pi_{\mathbf{1}} = Id$
(ii) for $x \in C$, $x \neq \mathbf{0}$, $x \neq \mathbf{1}$, π_x does not fix any coordinate of C.

Theorem

(Rifà, Suarez 2014) A Hadamard full propelinear code $(C, \star)$ of length $4t$ is a Hadamard group[a] *of order $8t$ with central involution $\mathbf{1}$. Conversely, a Hadamard group of order $8t$ defines a Hadamard full propelinear code $(C, \star)$ of length $4t$.*

[a] Not defined here, introduced by Ito (1994)

Tying it all together

- A cocyclic Hadamard matrix of order $4t$ is equivalent to a $(4t, 2, 4t, 2t)$-difference set of a particular kind (de Launey, Flannery, KJH 2000).
- A cocyclic Hadamard matrix of order $4t$ is equivalent to a Hadamard group of order $8t$ (Flannery 1997)
- A Hadamard group of order $8t$ is equivalent to a Hadamard full propelinear code of length $4t$ (Rifà, Suarez 2014)

References

K.J. Horadam, M. Villanueva, Relationships between CCZ and EA equivalence classes and corresponding code invariants, In: Schmidt KU., Winterhof A. (eds), SETA 2014, LNCS 8865 (2014) 3–17.

J. Rifà, J.M. Basart, L. Huguet, On completely regular propelinear codes, In: Mora T. (eds) AAECC 1988, LNCS 357 (1989) 341–355.

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

THANKYOU.....QUESTIONS?