Quantum codes via Hermitian self-orthogonal codes over $\mathbb{F}_4$

Lijun Zou

Supervisor: Dr. Ronan Egan

National University of Ireland, Galway

NUI Galway
OÉ Gaillimh

Background

Definition (Coding theory basics)

Coding theory | $[n, k, d]_q$-linear code | Hamming distance | minimum distance | minimum weight | information rate | optimal | best known

Definition (Hermitian self-orthogonal code on $\mathbb{F}_4$)

Let C be an $[n, k]_4$ code. The *Hermitian dual* of C is the code $C^H = \{x \in \mathbb{F}_4^n : \langle x, c \rangle = 0 \ \forall\ c \in C\}$, where $\langle x, c \rangle$ is defined as

$$\langle x, y \rangle_H = \sum_{i=1}^{n} x_i y_i^2. \tag{1}$$

If $C \subseteq C^H$ we say that C is *Hermitian self-orthogonal.*

Remark. We will see on $\mathbb{F}_4$, (1) is closely related to the classical Hermitian inner product over complex numbers.

Background

Definition (Complex generalized weighing matrices)

An $n \times n$ matrix H of weight w with non-zero entries in the set $\langle \zeta_k \rangle$ is a *complex generalized weighing matrix* if

$$HH^* = wI_n.$$

If $w = n$, then H is called a *Butson Hadamard matrix*.

Example (BH(6,3))

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & z & z & z^2 & z^2 \\ 1 & z & 1 & z^2 & z^2 & z \\ 1 & z & z^2 & 1 & z & z^2 \\ 1 & z^2 & z^2 & z & 1 & z \\ 1 & z^2 & z & z^2 & z & 1 \end{pmatrix} \Longrightarrow \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 1 & 0 & 2 & 2 & 1 \\ 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 & 0 & 1 \\ 0 & 2 & 1 & 2 & 1 & 0 \end{pmatrix}.$$

Main theorem

Theorem (Main theorem)

Given a Hermitian self-orthogonal $[n, k]_4$-code C such that no codeword in $C^H \setminus C$ has weight less than d, one can construct a quantum $[[n, n-2k, d]]$-code.

The Main theorem is based on the paper of A. Robert Calderbank et al.

Theorem (A.Robert Calderbank et al.[1])

Let $C^\perp$ be the trace dual of code C and C^H be the Hermitian dual of C.

- *Theorem 2. Suppose C is an additive self-orthogonal subcode over $\mathbb{F}_4$, containing 2^{n-k} vectors, such that there are no vectors of weight $< d$ in $C^\perp \setminus C$. Then any eigenspace $\phi^{-1}(C)$ is an additive quantum error-correcting code with parameters $[[n, k, d]]$.*
- *Theorem 3.*

$$C \subseteq C^\perp \Longleftrightarrow C \subseteq C^H.$$

Construct Hermitian self-orthogonal code over $\mathbb{F}_4$

We first need to connect matrices in $\mathrm{CGW}(n, w; 3)$ to generator matrices of codes over $\mathbb{F}_4$. Define the map $\phi : \{0\} \cup \langle \zeta_3 \rangle \to \mathbb{F}_4$ such that

$$\begin{aligned}\phi(0) &= 0\\ \phi(1) &= 1\\ \phi(z) &= x\\ \phi(z^2) &= x^2.\end{aligned}$$

Example (BH(6,3))

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & z & z & z^2 & z^2 \\ 1 & z & 1 & z^2 & z^2 & z \\ 1 & z & z^2 & 1 & z & z^2 \\ 1 & z^2 & z^2 & z & 1 & z \\ 1 & z^2 & z & z^2 & z & 1 \end{pmatrix} \Longrightarrow \phi(H) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & x & x & x^2 & x^2 \\ 1 & x & 1 & x^2 & x^2 & x \\ 1 & x & x^2 & 1 & x & x^2 \\ 1 & x^2 & x^2 & x & 1 & x \\ 1 & x^2 & x & x^2 & x & 1 \end{pmatrix}$$

Construct Hermitian self-orthogonal code over $\mathbb{F}_4$

Proposition

If H is an element of $\mathrm{CGW}(n, w; 3)$, then the rows of $\phi(H)$ are pairwise orthogonal with respect to the Hermitian inner product.

Proof.

We can show that for $x, y \in \{0\} \cup \langle \zeta_3 \rangle$,

$$\phi(xy) = \phi(x)\phi(y)$$

and for rows H_i and H_j of H,

$$\langle H_i, H_j \rangle = 0 \implies \langle \phi(H_i), \phi(H_j) \rangle = 0.$$

$\square$

Remark. $\phi(x + y) \neq \phi(x) + \phi(y)$.

Construct Hermitian self-orthogonal code over $\mathbb{F}_4$

It follows that if the rows of $\phi(H)$ are also orthogonal to themselves, then the rows of $\phi(H)$ will generate a Hermitian self-orthogonal code.

Proposition (Paper of D. Crnkovic, R. Egan, A. Svob [2])

If H is a $\mathrm{CGW}(n, w; 3)$ matrix, where w is even, then $\phi(H)$ generates a Hermitian self-orthogonal linear code over $\mathbb{F}_4$.

Remark. Any subset of $\phi(H)$ also generate a Hermitian self-orthogonal code.

Why do we choose $\mathrm{CGW}(n, w; 3)$ matrix?

Proposition

If $w > 1$ is even, and C is the code generated by $\phi(H)$, then the minimum distance of C will be at least 4.

Determine the parameters of quantum code - GAP code

```
LoadPackage("guava");
G := One(GF(4)) * [[Z(2)^0,Z(2)^0,Z(2)^0,Z(2)^0,Z(2)^0,Z(2)^0],
[Z(2)^0,Z(2)^0,Z(2^2),Z(2^2),Z(2^2)^2,Z(2^2)^2],
[Z(2)^0,Z(2^2),Z(2)^0,Z(2^2)^2,Z(2^2)^2,Z(2^2)],
[Z(2)^0,Z(2^2),Z(2^2)^2,Z(2)^0,Z(2^2),Z(2^2)^2],
[Z(2)^0,Z(2^2)^2,Z(2^2)^2,Z(2^2),Z(2)^0,Z(2^2)],
[Z(2)^0,Z(2^2)^2,Z(2^2),Z(2^2)^2,Z(2^2),Z(2)^0]];

#Write a function takes a matrix as input and outputs the parameters of the quantum code.
MyQuantumD := function(G)
local IndList, i, D, j, C, C_H, CHH, CH;
IndList := MyLinearVector(G);
for i in [1 .. Length(IndList)] do
   D := Combinations(IndList, i);
   for j in D do
     C := GeneratorMatCode(j, GF(4));
     C_H := S_Mat(j); CHH := GeneratorMatCode(C_H, GF(4));
     CH := DualCode(CHH);
     Print(j,"\n"); Myresult(CH,C);
   od;
od; end;

#Write a function that computes the minimum weight of a code C over F_4.
F4_MinimumWeight := function(C)
     local list1, list2, list3, MW;
     list1 := WeightDistribution(C); list2 := ShallowCopy(list1);
     Remove(list2,1);
     MW := PositionNonZero(list2);
     return MW; end;
```

Determine the parameters of quantum code

Proposition

Let C be a code over $\mathbb{F}_4$, generated by a matrix M. Let N be the matrix obtained from M by replacing each entry with its conjugate. The Dual of N is equal to the Hermitian Dual of M.

Proof.

Let $x \in C$. Let M_i be a row of M and $N_i := \overline{M_i}$ be a row of N. Then

$$\langle x, M_i \rangle_H = 0 \Longleftrightarrow \sum_{j=1}^{n} x_j \overline{M_{ij}} = \sum_{j=1}^{n} x_j N_{ij} = 0 \Longleftrightarrow \langle x, N_i \rangle = 0.$$

$\square$

Results- BH(6,3)

Table: Buston Hadamard matrix of order 6, BH(6,3)

Generators	Parameters of quantum code	Optimal?
(1 1 1 1 1 1)	$[6, 4, 2]$	Yes
(1 1 x x x^2 x^2)	$[6, 4, 2]$	Yes
(1 x 1 x^2 x^2 x)	$[6, 4, 2]$	Yes
(1 1 1 1 1 1), (1 1 x x x^2 x^2)	$[6, 2, 2]$	Yes
(1 1 1 1 1 1), (1 x 1 x^2 x^2 x)	$[6, 2, 2]$	Yes
(1 1 x x x^2 x^2),(1 x 1 x^2 x^2 x)	$[6, 2, 2]$	Yes

Results- all Buston matrices up to order 18

Lemma

- $\mathrm{BH}(n,3)$ *is non-empty only if n is a multiple of* 3.
- *There are one matrix of* $\mathrm{BH}(6,3)$*, two matrices of* $\mathrm{BH}(12,3)$ *and* 85 *matrices* $\mathrm{BH}(18,3)$ *of order* 18 *up to monomial equivalence[4].*
- *The weight distribution of the trace dual of C is determined by the weight distribution of C [1].*

Results. (compared with [3])

$$[6,4,2] \quad [6,2,2]$$

$$[12,2,4] \quad [12,4,4] \quad [12,10,2]$$

$$[18,16,2] \quad [18,14,2] \quad [18,12,2] \quad [18,10,3] \quad [18,8,4] \quad [18,4,5] \quad [18,2,6]$$

Construct CGW(n,w;3) matrices

Proposition

Let $H \in \mathrm{CGW}(n, w; k)$ *and* $K \in \mathrm{CGW}(m, v; \ell)$*. Then* $H \otimes K \in \mathrm{CGW}(mn, wv; \mathrm{lcm}(k, \ell))$*, where* $\mathrm{lcm}(k, \ell)$ *denotes the least common multiple of* k *and* ℓ*.*

We use $\mathrm{BH}(n, 3)$ matrices up to order 18 and the following type of matrices to construct new $\mathrm{CGW}(\mathrm{n}, \mathrm{w}; 3)$ matrices.

$$\mathrm{CGW}(5, 4; 3) \quad \mathrm{CGW}(21, 16; 3) \quad \mathrm{BH}(3, 3) \quad \mathrm{BH}(9, 3)$$

Results

$$[5, 1, 3] \quad [5, 3, 1] \quad [21, 15, 3] \quad [21, 19, 1]$$

$$[15, 13, 1] \quad [15, 11, 2] \quad [15, 7, 3] \quad [25, 23, 1] \quad [25, 17, 3]$$

$$[30, 26, 1] \quad [30, 24, 2] \quad [60, 56, 2] \quad [60, 54, 2]$$

$$[90, 86, 2] \quad [90, 84, 2] \quad [90, 82, 2]$$

$$[63, 61, 1] \quad [63, 57, 2] \quad [105, 103, 1]$$

$$[126, 120, 2] \quad [126, 118, 2] \quad [252, 246, 2] \quad [252, 244, 2]$$

$$[36, 34, 2] \quad [36, 32, 2] \quad [36, 30, 2] \quad [36, 26, 3] \quad [36, 24, 4] \quad [36, 22, 4]$$

$$[54, 52, 2] \quad [54, 50, 2] \quad [54, 48, 2] \quad [54, 44, 3] \quad [54, 40, 4]$$

Reference

[1] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over $\mathrm{GF}(4)$. *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998.

[2] D. Crnković, R. Egan, and A. Švob. Constructing self-orthogonal and Hermitian self-orthogonal codes via weighing matrices and orbit matrices. *Finite Fields Appl.*, 55:64–77, 2019.

[3] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. `http://www.codetables.de`. Retrieved 23/6/2021.

[4] M. Harada, C. Lam, A. Munemasa, and V. D. Tonchev. Classification of generalized Hadamard matrices $H(6,3)$ and quaternary Hermitian self-dual codes of length 18. *Electron. J. Combin.*, 17(1):Research Paper 171, 14, 2010.