A survey of complex generalized weighing matrices, and a construction of quantum error-correcting codes

Ronan Egan
Dublin City University

Outline

- Introducing complex generalized weighing matrices (CGWs).
- Existence conditions.
- Some known constructions, including recursive constructions.
- Collecting the data (in progress).
- An application to quantum error correcting codes.

But first...

Some notation

Throughout this talk...

- n and k are positive integers, q is a prime power;
- $\zeta_k = e^{\frac{2\pi\sqrt{-1}}{k}}$ is a primitive k^{th} root of unity;
- $\langle \zeta_k \rangle = \{\zeta_k^j \ : \ 0 \leq j \leq k-1\}$;
- $\mathcal{U}_k = \langle \zeta_k \rangle \cup \{0\}$;
- $\mathbb{F}_q$ is the finite field of order q;
- $\mathcal{M}_n(k)$ is the set of $n \times n$ matrices with entries in $\mathcal{U}_k$;
- $\mathcal{M}_n(\mathbb{F})$ is the set of $n \times n$ matrices with entries in a field $\mathbb{F}$;
- If M is a matrix, M^* is the complex conjugate transpose.
- For $0 \neq x \in \mathbb{F}$, $x^* = x^{-1}$ and $0^* = 0$.
- I_n and J_n denote the $n \times n$ identity and all ones matrices.

Definition

Let $W \in \mathcal{M}_n(k)$. Then W is a *complex generalized weighing matrix* with parameters $\mathrm{CGW}(n, w; k)$ if

$$WW^* = wI_n.$$

It follows that $|\det(W)| = w^{\frac{n}{2}}$. Equivalently, $W \in \mathrm{CGW}(n, w; k)$, if the rows/columns of W all have precisely w non-zero entries, and distinct rows/columns are orthogonal. The parameter w is the *weight* of the matrix.

Example

The matrix

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \zeta_3 & \zeta_3^2 \\ 1 & 1 & 0 & \zeta_3^2 & \zeta_3 \\ 1 & \zeta_3 & \zeta_3^2 & 0 & 1 \\ 1 & \zeta_3^2 & \zeta_3 & 1 & 0 \end{bmatrix}$$

is a $\mathrm{CGW}(5, 4; 3)$.

Equivalence

Let $W \in \mathrm{CGW}(n, w; k)$, and let P and Q be monomial matrices in $\mathcal{M}_n(k)$. Any matrix

$$W' = PWQ^*$$

is also a $\mathrm{CGW}(n, w; k)$, and is said to be *equivalent* to W.

Any $\mathrm{CGW}(n, w; k)$ can be normalized so that the first non-zero entry in any row or column is 1.

Special cases

• A $\mathrm{CGW}(n, n; k)$ is a *Butson Hadamard matrix*. These are reasonably well studied, but usually with restrictions on k being a prime power, or quite small. Classifications are hard, but there are lots of constructions.

• A $\mathrm{CGW}(n, w; 2)$ is a *weighing matrix*. Quite well studied: numerous classifications at small orders and weights, well known existence conditions, lots of constructions.

• A $\mathrm{CGW}(n, n; 2)$ is a *Hadamard matrix*. Literature is enormous: The Hadamard conjecture well known; constructions up order 664 and at infinitely many orders besides; classified up to order 32; various extra conditions considered, i.e., group developed, cocyclic, symmetric, skew-symmetric, etc.

An important related case

Let G be a finite group. A $n \times n$ matrix W with entries from $\{0\} \cup G$ such that

$$WW^* = wI_n$$

over $\mathbb{Z}[G]/\mathbb{Z}G$ is a *generalized weighing matrix*, $\mathrm{GW}(n, w; G)$.

Let k be prime. Since

$$\sum_{j=0}^{k-1} a_j \zeta_k^j = 0 \;\Leftrightarrow\; a_0 = a_1 = \cdots = a_{k-1},$$

when k is prime, we know that a $\mathrm{GW}(n, w; \langle \zeta_k \rangle)$ is also a $\mathrm{CGW}(n, w; k)$.

One more useful definition

Let $M \in \mathcal{M}_n(k)$. Let S be the matrix obtained by replacing all non-zero entries of M with 1. This matrix S is called the *support* matrix of M, and we say that S supports M.

We will also say that S *lifts* to M.

Lifting Problem: Given an $n \times n$ $(0,1)$-matrix S of weight w, does S lift to a $\mathrm{CGW}(n, w; k)$?

Another diversion

Existence Conditions

Existence conditions

Many of the most significant barriers to the existence of a $\mathrm{CGW}(n, w; k)$ stem from a condition on vanishing sums of roots of unity due to Lam and Leung.

Theorem (Lam, Leung, 2000)

If $\sum_{j=0}^{k-1} c_j \zeta_k^j = 0$ for non-negative integers $c_0, \ldots, c_{k-1}$, and $p_1, \ldots, p_r$ are the primes dividing k, then $\sum_{j=0}^{k-1} c_j = \sum_{\ell=1}^{r} d_\ell p_\ell$ where $d_1, \ldots, d_\ell$ are non-negative integers.

Most significantly, when $k = p^r$ is a prime power, the non-zero entries in any pair of distinct rows must coincide in mp positions for some non-negative integer m.

T. Y. Lam, K. H. Leung, On vanishing sums of roots of unity, J. Algebra, 224, 1, 91–109, 2000.

Existence conditions

For k prime, non-existence conditions for $\mathrm{GW}(n, w; \langle \zeta_k \rangle)$, due mostly to de Launey, can be applied.

Theorem (de Launey, 84)

If there exists a $\mathrm{CGW}(n, w; k)$ with $n \neq w$ and k a prime, then the following must hold:

1. $w(w-1) \equiv 0 \mod k$.
2. $(n-w)^2 - (n-w) \geq \sigma(n-1)$ *where* $0 \leq \sigma \leq k-1$ *and* $\sigma \equiv n - 2w \mod k$.
3. *If n is odd and $k = 2$, then w is a square.*

W. de Launey. On the nonexistence of generalised weighing matrices. Ars Combin., 17(A):117–132, 1984.

Sketch proof of part 1

- Suppose $W \in \mathrm{CGW}(n, w; k)$.
- In each of the w columns such that there is a non-zero entry in the first row of W, there are $w - 1$ non-zero entries in subsequent rows.
- It follows that the sum of the inner products of row 1 with the $n - 1$ remaining rows has $w(w - 1)$ terms.
- This sum is zero only if $w(w - 1) \equiv 0 \mod k$.

Example

There is no $\mathrm{CGW}(n, w; 3)$ if $w \equiv 2 \mod 3$.

de Launey continued

Theorem (de Launey, 84)

Suppose there exists a $\mathrm{CGW}(n, w; k)$ *with* n *odd and* k *a prime. Suppose that* $m \not\equiv 0 \mod k$ *is an integer dividing the square free part of* w*. Then the order of* m *modulo* k *is odd.*

Example

As de Launey observed, this eliminated the possible existence of $\mathrm{CGW}(19, 10; 5)$, which was not previously known at the time.

Block designs

Let n, w and λ be integers where $n > w > \lambda \geq 0$. Let X be a set of size n. A *symmetric balanced incomplete block design* $\mathrm{SBIBD}(n, w, \lambda)$ is a set of n subsets of X of size w, called *blocks* such that each unordered pair of distinct elements of X are contained in exactly λ blocks. If A is the incidence matrix of the $\mathrm{SBIBD}(n, w, \lambda)$, then

$$AA^\top = wI_n + \lambda(J_n - I_n).$$

It is a well known necessary condition that a $\mathrm{SBIBD}(n, w, \lambda)$ exists only if

$$\lambda(n-1) = w(w-1).$$

Specialised non-existence results

Proposition

A $\mathrm{CGW}(11,5;4)$ *does not exist.*

Proof (sketch):

- Suppose $W \in \mathrm{CGW}(11,5;4)$ and let S be the support matrix. The inner product of any two rows of S must be even, so must be 0, 2 or 4.
- It can be shown that the only possibility is for such a matrix S is for the inner product of every distinct pair of rows to be 2.
- This means that S is the incidence matrix of a $(11,5,2)$-design. This exists, but there is only one up to equivalence.
- Show that this S cannot lift to a $\mathrm{CGW}(11,5;4)$ (can be done easily by hand).

Something more general for $k = 4$

Theorem (Turyn, 70)

If there exists a $\mathrm{CGW}(n, w; 4)$ *then there exists a* $\mathrm{CGW}(2n, 2w; 2)$.

Theorem (Seberry, 79)

If $n \equiv 2 \bmod 4$ *and there exists* $W \in \mathrm{CGW}(n, w; 2)$, *then* w *is the sum of two integer squares.*

R. J. Turyn, Complex Hadamard matrices. In Combinatorial Structures and their Applications (Proc. Calgary Internat. Conf., Calgary, Alta., 1969), pages 435–437. Gordon and Breach, New York, 1970.

J. Seberry. Orthogonal designs. Springer, Cham, 2017. Hadamard matrices, quadratic forms and algebras, Revised and updated edition of the 1979 original.

Corollary

If n is odd and there exists $W \in \mathrm{CGW}(n, w; 4)$, then w is the sum of two integer squares. Equivalently, by the Sum of Two Squares Theorem, the square free part of w is not divisible by any prime $p \equiv 3 \mod 4$.

Example

There is no $\mathrm{CGW}(11, 6; 4)$ or $\mathrm{CGW}(11, 7, 4)$.

Examples for composite k

Proposition (Szöllősi, 11)

There is no $\mathrm{CGW}(n, w; 6)$ *when* n *is odd and* $w \equiv 2 \mod 3$.

Proof: Suppose $W \in \mathrm{CGW}(n, w; 6)$. Then $|\mathrm{det}(W)|^2 = w^n$. Since any element of $\mathcal{U}_6$ can be written in the form $a + b\zeta_3$ for integers a and b, it follows that there are integers a and b such that

$$w^n = |\mathrm{det}(W)|^2 = |a + b\zeta_3|^2 = a^2 + b^2 - ab.$$

It is not possible that $a^2 + b^2 - ab \equiv 2 \mod 3$, and so it cannot be that n is odd and $w \equiv 2 \mod 3$. □

F. Szöllősi. Construction, classification and parametrization of complex Hadamard matrices. ArXiv math/1150.5590.

One for composite k

Proposition

There is no $\mathrm{CGW}(n, w; 6)$ *when* n *is odd and* $w \equiv 2 \mod 4$.

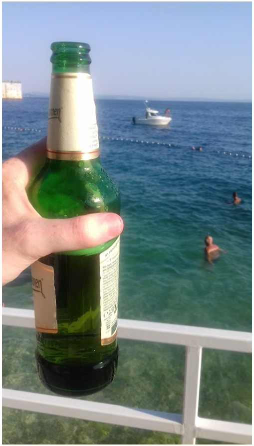
The proof is similar to begin with, but need to show that there is no solution to

$$(2m)^n = a^2 + b^2 - ab,$$

for odd m and n. (A little more work, but not much).

It's hot here!


CITIES
ADD
MORE
Rijeka
38°C
Sunny
Sat, 8 July
33° / 20°
HOURLY
DAILY
32°
32°
27°
21°
20°
29°
13:00
17:00
21:00
01:00
05:00
09:00
Chance of rain 6%
UV Index Moderate
AccuWeather
Updated 08/07/2017 12:10



Constructions

Generalized Paley construction

The most famous constructions of an infinite family of Hadamard matrices are due to Paley. There are two constructions yielding what are now known as the type I and type II Paley Hadamard matrices.

Both constructions are built on circulant cores, obtained by applying the quadratic character to the elements of a finite field $\mathbb{F}_q$.

The following bears a strong enough resemblance that we refer to this as a generalized Paley construction.

Generalized Paley construction

Let p and q be primes, with $q \equiv 1 \mod p$. Let α be a multiplicative generator of the non-zero elements of $\mathbb{Z}_q$. Consider the map $\phi : \mathbb{Z}_q \to \langle \zeta_p \rangle \cup \{0\}$ defined by setting $\phi(\alpha^j) = \zeta_p^j$ for all $1 \leq j \leq q-1$, and setting $\phi(0) = 0$. Then ϕ has the following two properties:

- $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in \mathbb{Z}_q$; and
- $\phi(x^*) = \phi(x)^*$ for all $x \in \mathbb{Z}_q$.

Lemma

Let $C = \mathrm{circ}([\phi(x) \ : \ 0 \leq x \leq q-1])$. *Then* $CC^* = qI_q - J_q$.

Generalized Paley construction

Theorem

Let $C = \mathrm{circ}([\phi(x) \ : \ 0 \leq x \leq q-1])$. *Then the matrix*

$$W = \left[\begin{array}{c|c} 0 & \mathbf{1} \\ \hline \mathbf{1}^\top & C \end{array}\right],$$

is a $\mathrm{CGW}(q+1, q; p)$.

All parameters are in some way restricted by this construction, but it is quite simple to build.

Berman's construction

Berman's construction is the most general direct construction we know of - it relies heavily on finite geometry.

It builds a CGW on a support matrix that corresponds to a type of incidence structure of build from points and hyperplanes in $\mathbb{F}_{p^n}^t$.

Berman's construction

Theorem

Let p, n, t, d and r be any positive integers such that p is prime, $d \mid r$, and $r \mid (p^n - 1)$. Then there exists a matrix W in $\mathrm{CGW}((p^{tn} - 1)/r, p^{(t-1)n}; d)$.

Berman's construction gives a CGW with plenty of freedom to choose the parameters. The main restriction is on the weight, which is necessarily a prime power.

Examples include the $\mathrm{CGW}(5, 4; 3)$ we have seen, and a $\mathrm{CGW}(26, 25; 6)$ where $n = 2$, $t = 2$, $p = 5$, $d = 6$ and $r = 24$.

G. Berman. Families of generalized weighing matrices. Canad. J. Math., 30(5):1016–1028, 1978.

Complementary sequences

For any $\alpha \in \mathcal{U}_k$, define the α-circulant matrix

$$C_\alpha = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & & 0 & 0 \\ 0 & 0 & 0 & & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & & 0 & 1 \\ \alpha & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

The α-*phased periodic autocorrelation function* of a $\mathcal{U}_k$-sequence a of length v and shift s to be

$$\mathrm{PAF}_{\alpha,s}(a) = a \cdot \overline{aC_\alpha^s}.$$

R. Egan, Generalizing pairs of complementary sequences and a construction of combinatorial structures. Discrete Math., 343(5):111795, 10, 2020.

Complementary sequences

Let (a, b) be a pair of $\mathcal{U}_k$-sequences. Let w_a denote the weight of a sequence a, and let $w = w_a + w_b$ be the weight of a pair (a, b).

A pair of sequences (a, b) is a *weighted α-phased periodic Golay pair* $(\mathrm{WPGP}(\mathcal{U}_k, v, \alpha, w))$ if

$$\mathrm{PAF}_{\alpha,s}(a) + \mathrm{PAF}_{\alpha,s}(b) = 0.$$

for all $1 \leq s \leq v - 1$.

Complementary sequences

Theorem (E, 20)

Let $(a, b) \in \mathrm{WPGP}(\mathcal{U}_k, v, \alpha, w)$ *and let* A *and* B *be the* α*-circulant matrices with first row* a *and* b *respectively. Then*

$$W = \begin{bmatrix} A & B \\ -B^* & A^* \end{bmatrix},$$

is a $\mathrm{CGW}(2v, w; 2k)$ *if* k *is odd, and* W *is a* $\mathrm{CGW}(2v, w; k)$ *if* k *is even.*

Example

A $\mathrm{CGW}(10, 6; 4)$ can be constructed from a $\mathrm{WPGP}(\mathcal{U}_4, 5, 1, 6)$ where $a = (1, \zeta_4, 1, 0, 0)$ and $b = (1, -1, -1, 0, 0)$. There is no $\mathrm{CGW}(10, 6; 2)$.

Complementary sequences

A *ternary Golay pair* of is a pair of $(0, \pm 1)$-sequences (a, b) of length n such that

$$\sum_{j=0}^{n-1-s} a_j a_{j+s} + b_j b_{j+s} = 0$$

for all $1 \leq s \leq n-1$.

Theorem (E, 20)

Let (a, b) be a ternary Golay pair of length n and weight w. Then $(a, b) \in \mathrm{WPGP}(\mathcal{U}_k, n, \alpha, w)$ for any even k, and any $\alpha \in \langle \zeta_k \rangle$.

Given (a, b) we can construct several distinct matrices in $\mathrm{CGW}(2n, w; k)$ that are not equivalent to a $\mathrm{CGW}(2n, w; 2)$.

R. Craigen and C. Koukouvinos. A theory of ternary complementary pairs. J. Combin. Theory Ser. A, 96(2):358–375, 2001.

Seberry-Whiteman construction

The Seberry and Whiteman construction is fairly specialized. It constructs a $\mathrm{CGW}(q+1, q, 4)$ where $q \equiv 1 \bmod 8$ is a prime power.

It's really an example of a construction of complementary sequences $(r, s) \in \mathrm{WPGP}(\mathcal{U}_4, n, 1, q)$ where $n = \frac{q+1}{2}$. The $\mathrm{CGW}(q+1, q, 4)$ is constructed as before.

J. Seberry and A. L. Whiteman. Complex weighing matrices and orthogonal designs. Ars Combin., 9:149–162, 1980.

Recursive constructions

Direct sum type

We define the direct sum of an $m \times m$ matrix A and a $n \times n$ matrix B to be

$$A \oplus B = \begin{bmatrix} A & 0_{m,n} \\ 0_{n,m} & B \end{bmatrix}.$$

Proposition

If $A \in \mathrm{CGW}(m, w; k_1)$ and $B \in \mathrm{CGW}(n, w; k_2)$, then $A \oplus B \in \mathrm{CGW}(m+n, w; k)$ where $k = \mathrm{lcm}(k_1, k_2)$.

A familiar block construction

Proposition

Let $A \in \mathrm{CGW}(n, w_1; k_1)$ *and* $B \in \mathrm{CGW}(n, w_2; k_2)$ *be such that* $AB = BA$. *Then the matrix*

$$\begin{bmatrix} A & B \\ -B^* & A^* \end{bmatrix}$$

is a $\mathrm{CGW}(2n, w; k)$ *where* $w = w_1 + w_2$ *and* $k = \mathrm{lcm}(k_1, k_2, 2)$.

The α-circulant matrices generated by complementary sequences meet this condition.

Tensor product type

The Kronecker product of A and B is defined to be the block matrix

$$A \otimes B = [a_{ij} B].$$

Proposition

Let $A \in \mathrm{CGW}(n_1, w_1; k_1)$ and $B \in \mathrm{CGW}(n_2, w_2; k_2)$. Then $A \otimes B \in \mathrm{CGW}(n, w; k)$ where $n = n_1 n_2$, $w = w_1 w_2$ and $k = \mathrm{lcm}(k_1, k_2)$.

Diță type

For this construction we require a matrix $A \in \mathrm{CGW}(n, w_a; k_a)$ and a set of matrices $\{B_1, \ldots, B_n\}$ with each $B_i \in \mathrm{CGW}(m, w_{b,i}; k_{b,i})$.

Proposition

Let $A, B_1, \ldots, B_n$ be as described above. Then

$$D = \begin{bmatrix} a_{11}B_1 & a_{12}B_2 & \cdots & a_{1n}B_n \\ a_{21}B_1 & a_{22}B_2 & \cdots & a_{2n}B_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B_1 & a_{n2}B_2 & \cdots & a_{nn}B_n \end{bmatrix}$$

is a $\mathrm{CGW}(mn, w; k)$ where $w = w_a\left(\sum_{i=1}^{n} w_{b,i}\right)$ and $k = \mathrm{lcm}(k_a, k_{b,1}, \ldots, k_{b,n})$.

P. Diță. Some results on the parametrization of complex Hadamard matrices. J. Phys. A, 37(20):5355–5374, 2004.

Weaving

The idea of weaving is to knit together weighing matrices of different orders to form a larger one, without relying on a tensor product type construction that forces the order to be the product of the orders of its constituents.

Theorem (Craigen, 95)

Let $M = (m_{ij})$ be a $m \times n$ $(0,1)$-matrix with row sums $r_1, \ldots, r_m$ and column sums $c_1, \ldots, c_n$. If for fixed integers a and b there are matrices $A_i \in \mathrm{CGW}(r_i, a; k_1)$ and $B_j \in CGW(c_j, b; k_2)$ for $1 \leq i \leq m$ and $1 \leq j \leq n$, then there is a $\mathrm{CGW}(\sigma(M), ab; k)$ where

$$\sigma(M) = \sum_{i=1}^{m} r_i = \sum_{j=1}^{n} c_j,$$

and $k = \mathrm{lcm}(k_1, k_2)$.

R. Craigen. Constructing weighing matrices by the method of weaving. J. Combin. Des., 3(1):1–13, 1995.

$$
\left[\begin{array}{ccc|ccc|ccc|ccc|ccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega & \omega & \omega & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega^2 & \omega^2 & \omega^2 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & \omega & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega & \omega & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 1 & \omega^2 & \omega & 1 & \omega & \omega^2 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & \omega^2 & \omega & \omega & \omega^2 & 1 & \omega^2 & \omega^2 & \omega^2 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & \omega^2 & \omega & \omega^2 & 1 & \omega & \omega & \omega & \omega \\
\hline
1 & \omega & \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \omega^2 & \omega & 1 & \omega & \omega^2 \\
1 & \omega & \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 & \omega & 1 & \omega^2 & \omega^2 & 1 & \omega \\
1 & \omega & \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 & \omega & 1 & \omega & \omega^2 & 1 \\
\hline
1 & \omega^2 & \omega & 1 & \omega^2 & \omega & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \omega^2 & \omega \\
1 & \omega^2 & \omega & \omega & 1 & \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 & \omega & 1 \\
1 & \omega^2 & \omega & \omega^2 & \omega & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \omega & 1 & \omega^2
\end{array}\right]
$$

is a $\mathrm{CGW}(15, 9; 3)$. A $\mathrm{CGW}(15, 9; 3)$ cannot be obtained by a Tensor product.

Existence data

$n \setminus w$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	E														
2	E	E													
3	E	N	N												
4	E	E	E	E											
5	E	N	N	E	N										
6	E	E	N	E	E	N									
7	E	N	N	E	N	N	N								
8	E	E	E	E	E	E	E	E							
9	E	N	N	N	N	N	N	N	N						
10	E	E	N	E	E	N	N	E	E	N					
11	E	N	N	E	N	N	N	N	N	N	N				
12	E	E	E	E	E	E	E	E	E	E	E	E			
13	E	N	N	E	N	N	N	N	E	N	N	N	N		
14	E	E	N	E	E	N	N	E	E	E	N	N	E	N	
15	E	N	N	E	N	N	N	N	E	N	N	N	N	N	N

Table: $k = 2$

M. Harada and A. Munemasa. On the classification of weighing matrices and self-orthogonal codes. J. Combin. Des., 20(1):40–57, 2012.

Existence data

$n \setminus w$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	E														
2	E	N													
3	E	N	E												
4	E	N	N	N											
5	E	N	N	E	N										
6	E	N	E	N	N	E									
7	E	N	N	N	N	N	N								
8	E	N	N	N	N	N	E	N							
9	E	N	E	N	N	N	N	N	E						
10	E	N	N	E	N	N	N	N	N	N					
11	E	N	N	N	N	N	N	N	N	N	N				
12	E	N	E	N	N	E	N	N	?	N	N	E			
13	E	N	N	N	N	N	N	N	?	N	N	N	N		
14	E	N	N	N	N	N	N	N	N	N	N	N	E	N	
15	E	N	N	E	N	N	?	N	E	N	N	E	N	N	N

Table: $k = 3$

Existence data

$n \setminus w$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	E														
2	E	E													
3	E	N	N												
4	E	E	E	E											
5	E	N	N	E	N										
6	E	E	N	E	E	E									
7	E	N	N	E	N	N	N								
8	E	E	E	E	E	E	E	E							
9	E	N	N	N	N	N	N	N	N						
10	E	E	N	E	E	E	N	E	E	E					
11	E	N	N	E	N	N	N	N	N	N	N				
12	E	E	E	E	E	E	E	E	E	E	E	E			
13	E	N	N	E	N	N	N	?	E	N	N	N	N		
14	E	E	N	E	E	E	?	E	E	E	N	?	E	E	
15	E	N	N	E	?	N	N	?	E	N	N	N	N	N	N

Table: $k = 4$

Existence data

$n \setminus w$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	E														
2	E	N													
3	E	N	N												
4	E	N	N	N											
5	E	N	N	N	E										
6	E	N	N	N	N	N									
7	E	N	N	N	N	N	N								
8	E	N	N	N	N	N	N	N							
9	E	N	N	N	N	N	N	N	N						
10	E	N	N	N	E	N	N	N	N	E					
11	E	N	N	N	N	N	N	N	N	N	N				
12	E	N	N	N	N	N	N	N	N	N	E	N			
13	E	N	N	N	N	N	N	N	N	N	N	N	N		
14	E	N	N	N	N	N	N	N	N	N	N	N	N	N	
15	E	N	N	N	N	N	N	N	N	N	N	N	N	N	N

Table: $k = 5$

Existence data

$n \setminus w$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	E														
2	E	E													
3	E	N	E												
4	E	E	E	E											
5	E	N	N	E	N										
6	E	E	E	E	E	E									
7	E	N	E	E	N	N	E								
8	E	E	E	E	E	E	E	E							
9	E	N	E	E	N	N	?	N	E						
10	E	E	E	E	E	?	?	E	E	E					
11	E	N	E	E	N	N	?	N	?	N	N				
12	E	E	E	E	E	E	E	E	E	E	E	E			
13	E	N	E	E	N	N	?	N	E	N	N	?	E		
14	E	E	E	E	E	E	E	E	E	E	?	?	E	E	
15	E	N	E	E	N	N	E	N	E	N	N	E	?	N	N

Table: $k = 6$

The carnival in Rijeka

Towards quantum codes

Hermitian self-orthogonal codes

Let C be a $[n, k]_{q^2}$ code. The *Hermitian inner product* of codewords $x, y \in C$ is defined by

$$\langle x, y \rangle = \sum_{i=0}^{n-1} x_i y_i^q.$$

The *Hermitian Dual* of C is the code

$$C^H = \{x \in C \mid \langle x, y \rangle = 0 \, \forall \, y \in C\}.$$

The code C is *Hermitian self-orthogonal* if $C \subseteq C^H$, and *Hermitian self-dual* if $C = C^H$.

Quantum codes

Calderbank an Shor define a *quantum error-correcting code* to be a unitary mapping (encoding) of k qubits into a subspace of the quantum state space of n qubits such that if any t of the qubits undergo arbitrary decoherence, not necessarily independently, the resulting n qubits can be used to faithfully reconstruct the original quantum state of the k encoded qubits.

Quantum codes are typically linear. For a quantum code with parameters n, k and d, we typically denote it as an $[[n, k, d]]_q$-code.

A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. Phys Rev A., 54(2):1098–1105, 1996.

Quantum codes

Calderbank, Rains, Shor and Sloane prove that given a Hermitian self-orthogonal $[n, k]_4$-linear code C such that no codeword in $C^H \setminus C$ has weight less than d, one can construct a quantum $[[n, n-2k, d]]_2$-code.

Theorem

If there exists a linear Hermitian self-orthogonal $[n, k]_{q^2}$ code C such that the minimum weight of C^H is d, then there exists an $[[n, n-2k, \geq d]]_q$ quantum code.

A quantum code can be 0-dimensional, and so it is possible to construct a quantum $[[n, 0, d]]_q$-code given a Hermitian self-dual $[n, n/2, d]_{q^2}$ code.

A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. Phys Rev A., 54(2):1098–1105, 1996.

A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. IEEE Trans. Inform. Theory, 52(11):4892–4914, 2006.

Quantum codes

We want to build Hermitian self-orthogonal codes over $\mathbb{F}_{q^2}$. With some restrictions, complex generalized Hadamard matrices provide the perfect tool.

To begin, observe that when $k = q+1$, we can translate the set of k^{th} roots of unity into $\mathbb{F}_{q^2}$, because k divides $q^2 - 1$.

Proposition

Let q be a prime power, let $k = q+1$ and let α be a primitive k^{th} root of unity in $\mathbb{F}_{q^2}$. Define the homomorphism $f : \mathcal{U}_k \to \mathbb{F}_{q^2}$ so that $f(0) = 0$ and $f(\zeta_k^j) = \alpha^j$ for $j = 0, 1, \ldots, q$. Let x be a $\mathcal{U}_k$-vector of length n and let $f(x) = [f(x_i)]_{0 \leq i \leq n-1}$. Then for any $\mathcal{U}_k$-vectors x and y,

$$\langle x, y \rangle = 0 \quad \Longrightarrow \quad \langle f(x), f(y) \rangle_H = 0.$$

Quantum codes

Proposition

Let W be a $\mathrm{CGW}(n, w; q+1)$ for some prime power q and let f be the homomorphism defined in the previous Proposition, with $f(W) = [f(W_{ij})]_{1 \leq i,j, \leq n}$. If w is divisible by the characteristic of $\mathbb{F}_{q^2}$, then $f(W)$ generates a Hermitian self-orthogonal F_{q^2}-code.

As a consequence we can use a $\mathrm{CGW}(n, w; k)$ with appropriate weight to build quantum codes for any $k = q + 1$ where q is a prime power, which includes any $k \in \{3, 4, 5, 6, 8, 9, 10\}$.

Some early results

New $[[n,k]]_q$ code	Best known $[[n,k]]_2$	New $[[n,k]]_q$ code	Best known $[[n,k]]_2$
$[[6,0,4]]_3$	$[[6,0,4]]_2$	$[[20,2,6]]_4$	$[[20,2,6]]_2$
$[[9,1,5]]_9^*$	$[[9,1,3]]_2$	$[[20,4,6]]_3$	$[[20,4,6]]_2$
$[[10,0,4]]_3$	$[[10,0,4]]_2$	$[[21,15,3]]_2$	$[[21,15,3]]_2$
$[[10,0,5]]_5^*$	$[[10,0,4]]_2$	$[[24,0,9]]_3$	$[[24,0,8]]_2$
$[[10,0,6]]_4^*$	$[[10,0,4]]_2$	$[[25,7,6]]_5$	$[[25,7,5]]_2$
$[[12,0,6]]_5$	$[[12,0,6]]_2$	$[[26,16,6]]_5^*$	$[[26,16,4]]_2$
$[[14,0,8]]_7^*$	$[[14,0,6]]_2$	$[[30,0,12]]_3$	$[[30,0,12]]_2$
$[[18,0,8]]_3$	$[[18,0,8]]_2$	$[[36,0,12]]_2$	$[[36,0,12]]_2$
$[[20,0,8]]_5$	$[[20,0,8]]_2$	$[[42,0,14]]_3$	$[[42,0,12]]_2$

Table: Some new quantum codes

M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. http://www.codetables.de.

Open problems

- Complete/extend the tables of CGWs.
- Develop a database of CGWs.
- Build lots Hermitian self-orthogonal codes and related quantum codes.

Hvala!