Doubly even self-orthogonal codes from quasi-symmetric designs

Ana Šumberac (ana.sumberac@math.uniri.hr)

Joint work with Dean Crnković, Doris Dumičić Danilović and Andrea Švob
Faculty of Mathematics, University of Rijeka, Croatia

This work has been fully supported by Croatian Science Foundation under the project 5713.

UNIVERSITY OF RIJEKA
FACULTY OF MATHEMATICS

July 7, 2023

Overview

1. Introduction
   - Designs
   - Linear codes
2. Doubly even self-orthogonal codes from quasi-symmetric designs
   - Codes from quasi-symmetric designs of Blokhuis-Haemers type
   - Codes from orbit matrices of quasi-symmetric designs

$t-(v,k,\lambda)$ design

A t-(v,k,λ) **design** is a finite incidence structure $\mathcal{D}=(\mathcal{P},\mathcal{B},\mathcal{I})$, where $\mathcal{P}$ and $\mathcal{B}$ are disjoint sets and $\mathcal{I}\subseteq\mathcal{P}\times\mathcal{B}$, with the following properties:

1. $|\mathcal{P}|=v$;
2. every element of $\mathcal{B}$ is incident with exactly k elements of $\mathcal{P}$;
3. every t distinct elements of $\mathcal{P}$ are incident with exactly λ elements of $\mathcal{B}$.

The elements of the set $\mathcal{P}$ are called **points** and the elements of the set $\mathcal{B}$ are called **blocks**.

$|\mathcal{B}|=b$.

In a 2-(v,k,λ) design every point is incident with exactly r blocks, $r=\frac{\lambda(v-1)}{k-1}$, and r is called **replication number** of a design.

Quasi-symmetric design

Definition

Number s, $0 \leq s < k$, is called a **block intersection number** of $\mathcal{D}$ if there exist $x, x' \in \mathcal{B}$ such that $|x \cap x'| = s$.

Quasi-symmetric design

Definition

Number s, $0 \le s < k$, is called a **block intersection number** of $\mathcal{D}$ if there exist $x, x' \in \mathcal{B}$ such that $|x \cap x'| = s$.

Definition

A t-design is called **quasi-symmetric** if it has exactly two block intersection numbers x and y, $x < y$.

Quasi-symmetric design

Definition

Number s, $0 \leq s < k$, is called a **block intersection number** of $\mathcal{D}$ if there exist $x, x' \in \mathcal{B}$ such that $|x \cap x'| = s$.

Definition

A t-design is called **quasi-symmetric** if it has exactly two block intersection numbers x and y, $x < y$.

A **complement** of a t-design $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is the design $\mathcal{D}' = (\mathcal{P}, \mathcal{B}', \mathcal{I}')$, where $\mathcal{B}' = \{P \backslash B : B \in \mathcal{B}\}$ and $\mathcal{I}' = (\mathcal{P} \times \mathcal{B}) \backslash \mathcal{I}$.

A complement of a quasi-symmetric design is also quasi-symmetric.

Incidence matrix

The **block-by-point incidence matrix** of a t-(v, k, λ) design is a $b \times v$ matrix whose rows are index by blocks and whose columns are indexed by points, with the entry in the row x and column P being 1 if $(P, x) \in \mathcal{I}$, and 0 otherwise.

Linear code

Let q be a prime power.

A q-ary **linear code** C of length n and dimension k is a k-dimensional subspace of a vector space $\mathbb{F}_q^n$.

Elements of C are called **codewords**.

If $q = 2$, code C is called **binary** code.

Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$.

Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$.

The **Hamming distance** between words x and y is the number $d(x, y) = |\{i : x_i \neq y_i\}|$.

The **minimum distance** of the code C is defined by $d = \min\{d(x, y) : x, y \in C,\ x \neq y\}$.

Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$.

The **Hamming distance** between words x and y is the number $d(x, y) = |\{i : x_i \neq y_i\}|$.

The **minimum distance** of the code C is defined by $d = \min\{d(x, y) : x, y \in C,\ x \neq y\}$.

The **weight** of a codeword x is $w(x) = d(x, 0) = |\{i : x_i \neq 0\}|$.

The **minimum weight** of the code C is defined by $w = \min\{w(x) : x \neq 0\}$.

Let $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n) \in \mathbb{F}_q^n$.

The **Hamming distance** between words x and y is the number $d(x,y) = |\{i : x_i \neq y_i\}|$.

The **minimum distance** of the code C is defined by $d = \min\{d(x,y) : x, y \in C,\ x \neq y\}$.

The **weight** of a codeword x is $w(x) = d(x,0) = |\{i : x_i \neq 0\}|$.

The **minimum weight** of the code C is defined by $w = \min\{w(x) : x \neq 0\}$.

A q-ary linear code of length n, dimension k, and minimum distance d is denoted $[n,k,d]_q$.

Doubly-even code

Definition

A code for which all codewords have weights divisible by 4 is called **doubly-even**.

Self-orthogonal and self-dual code

The **dual** code $C^{\perp}$ of the code C is $C^{\perp} = \{v \in F^n : (v, c) = 0, \forall c \in C\}$.

Self-orthogonal and self-dual code

The **dual** code $C^{\perp}$ of the code C is $C^{\perp} = \{v \in F^n : (v, c) = 0, \forall c \in C\}$.

Definition

A code C is **self-orthogonal** if $C \subseteq C^{\perp}$.

A code C is **self-dual** if $C = C^{\perp}$.

A doubly even self-dual code of length n exists iff $n \equiv 0 \mod 8$.

1

2

A doubly even self-dual code of length n exists iff $n \equiv 0 \mod 8$.

Doubly even self-dual binary codes of lengths less or equal 40 have been completely classified.[1]

[1] K. Betsumiya, M. Harada, A. Munemasa, A complete classification of doubly even self-dual codes of length 40. Electron. J. Combin. 19 (2012), no. 3, Paper 18, 12 pp.

[2]

A doubly even self-dual code of length n exists iff $n \equiv 0 \mod 8$.

Doubly even self-dual binary codes of lengths less or equal 40 have been completely classified.[1]

Rains[2] showed that the minimum distance d of a self-dual code C of length n is bounded by $d \leq 4\lfloor \frac{n}{24} \rfloor + 4$, except for $n \equiv 22 \mod 24$ when $d \leq 4\lfloor \frac{n}{24} \rfloor + 6$.

[1] K. Betsumiya, M. Harada, A. Munemasa, A complete classification of doubly even self-dual codes of length 40. Electron. J. Combin. 19 (2012), no. 3, Paper 18, 12 pp.

[2] E. M. Rains, Shadow bounds for self-dual codes, IEEE Trans. Inf. Theory 44 (1988), 134 – 139.

Generator matrix

A **generator matrix** of a linear code is a matrix whose rows form a basis for a code.

Generator matrix

A **generator matrix** of a linear code is a matrix whose rows form a basis for a code.

It is well known that a binary $[n, k]$ code is self-orthogonal iff the rows of its generator matrix have even weight and are orthogonal to each other.

Theorem [3]

Assume that $\mathcal{D}$ is a 2-(v, k, λ) design with block intersection numbers $s_1, s_2, \ldots, s_m$. Denote by C te binary code spanned by the block-by point incidence matrix od $\mathcal{D}$. If $v \equiv 0 \bmod 8$, $k \equiv 0 \bmod 4$, and $s_1, s_2, \ldots, s_m$ are all even, then C is contained in a doubly even self-dual code of length v.

[3] V. D. Tonchev, Codes, in: Handbook of Combinatorial Designs, 2nd ed., C. J. Colbourn, J. H. Dinitz (eds.), Chapman & Hall/CRC Press, Boca Raton, 2007, pp. 667 – 702.

Theorem [3]

Assume that $\mathcal{D}$ is a 2-(v, k, λ) design with block intersection numbers $s_1, s_2, \ldots, s_m$. Denote by C te binary code spanned by the block-by point incidence matrix od $\mathcal{D}$. If $v \equiv 0 \bmod 8$, $k \equiv 0 \bmod 4$, and $s_1, s_2, \ldots, s_m$ are all even, then C is contained in a doubly even self-dual code of length v.

Theorem

Let $\mathcal{D}$ be a quasi-symmetric 2-(v, k, λ) design with $v \equiv 0 \bmod 8$, $k \equiv 0 \bmod 4$, and even block intersection numbers x and y. Further, let M be a block-by-point incidence matrix of $\mathcal{D}$ and C be a binary code spanned by the rows of M. Then C is contained in a doubly even self-dual binary linear code of lenght v.

[3] V. D. Tonchev, Codes, in: Handbook of Combinatorial Designs, 2nd ed., C. J. Colbourn, J. H. Dinitz (eds.), Chapman & Hall/CRC Press, Boca Raton, 2007, pp. 667 – 702.

Examples

Example

$2-(56, 16, 18)$ [4]

$[n, k, d]_2$	$\#Aut(C)$	# non-equivalent
$[56, 19, 16]_2$	80640	1
$[56, 23, 8]_2$	30720	1
	192	1

[4] Vedran Krčadinac, https://web.math.pmf.unizg.hr/~krcko/results/quasisym.html

A **resolvable** 2-design is a design whose blocks can be partitioned into sets (called *parallel classes*), each of which forms a partition of the point set.

5

A **resolvable** 2-design is a design whose blocks can be partitioned into sets (called *parallel classes*), each of which forms a partition of the point set.

Theorem (D. Raghavarao, S.S. Shrikhande) [5]

The exsistance of a $2-(v_1, k_1, \lambda_1)$ design $\mathcal{D}_1$ and a resolvable $2-(v_2, k_2, \lambda_2)$ design $\mathcal{D}_2$ with $v_2 = v_1 k_2$ implies the existance of a $2-(v, k, \lambda)$ design $\mathcal{D}$ with parameters

$$v = v_1 \cdot k_2, k = k_1 k_2, \lambda = r_1 \lambda_2 + \lambda_1 (r_2 - \lambda_2),$$

where $r_i = \frac{\lambda_i (v_i - 1)}{k_i - 1}$, $i = 1, 2$.

[5] S.S. Shrikhande, D. Raghavarao, A method of construction of incomplete block designs, Sankhyã Ser. A 25 (1963) 399 – 402.

A **resolvable** 2-design is a design whose blocks can be partitioned into sets (called *parallel classes*), each of which forms a partition of the point set.

Theorem (D. Raghavarao, S.S. Shrikhande) [5]

The exsistance of a $2-(v_1, k_1, \lambda_1)$ design $\mathcal{D}_1$ and a resolvable $2-(v_2, k_2, \lambda_2)$ design $\mathcal{D}_2$ with $v_2 = v_1 k_2$ implies the existance of a $2-(v, k, \lambda)$ design $\mathcal{D}$ with parameters

$$v = v_1 \cdot k_2, k = k_1 k_2, \lambda = r_1 \lambda_2 + \lambda_1 (r_2 - \lambda_2),$$

where $r_i = \frac{\lambda_i(v_i - 1)}{k_i - 1}$, $i = 1, 2$.

If q is a power of 2, $\mathcal{D}_1$ is any symmetric 2-$\left(q^2, \frac{q(q-1)}{2}, \frac{q(q-2)}{4}\right)$ design, and $\mathcal{D}_2$ is any resolvable 2-$(q^3, q, 1)$ design, the conditions of the theorem hold.

[5] S.S. Shrikhande, D. Raghavarao, A method of construction of incomplete block designs, Sankhyã Ser. A 25 (1963) 399 – 402.

Designs of Blokhuis-Haemers type

Let q be a power of 2.

Let $\mathcal{D}_2$ be the resolvable 2-$(q^3, q, 1)$ design of the lines in $AG(3, q)$, and let $\mathcal{D}_1$ is a symmetric 2-$\left(q^2, \frac{q(q-1)}{2}, \frac{q(q-2)}{4}\right)$ design whose blocks are maximal arcs in $AG(2, q)$.

6

Designs of Blokhuis-Haemers type

Let q be a power of 2.

Let $\mathcal{D}_2$ be the resolvable 2-$(q^3, q, 1)$ design of the lines in $AG(3, q)$, and let $\mathcal{D}_1$ is a symmetric 2-$\left(q^2, \frac{q(q-1)}{2}, \frac{q(q-2)}{4}\right)$ design whose blocks are maximal arcs in $AG(2, q)$.

Blokhuis and Haemers[6] proved that the resulting 2-$\left(q^3, \frac{q^2(q-1)}{2}, \frac{q(q^3-q^2-2)}{4}\right)$ design $\mathcal{D} = \mathcal{D}(q)$ obtained by the construction given by the theorem is quasi-symmetric with block intersection numbers $\frac{q^2(q-2)}{4}$ and $\frac{q^2(q-1)}{4}$.

[6] A. Blokhuis and W. H. Haemers, An infinite family of quasi-symmetric designs, J. Statist. Plann. Inference 95 (2001) 117 – 119.

Designs of Blokhuis-Haemers type

Let q be a power of 2.

Let $\mathcal{D}_2$ be the resolvable 2-$(q^3, q, 1)$ design of the lines in $AG(3, q)$, and let $\mathcal{D}_1$ is a symmetric 2-$\left(q^2, \frac{q(q-1)}{2}, \frac{q(q-2)}{4}\right)$ design whose blocks are maximal arcs in $AG(2, q)$.

Blokhuis and Haemers[6] proved that the resulting 2-$\left(q^3, \frac{q^2(q-1)}{2}, \frac{q(q^3-q^2-2)}{4}\right)$ design $\mathcal{D} = \mathcal{D}(q)$ obtained by the construction given by the theorem is quasi-symmetric with block intersection numbers $\frac{q^2(q-2)}{4}$ and $\frac{q^2(q-1)}{4}$.

In the sequel, the designs obtained by the above described construction will be called **designs of Blokhuis-Haemers type**.

[6] A. Blokhuis and W. H. Haemers, An infinite family of quasi-symmetric designs, J. Statist. Plann. Inference 95 (2001) 117 – 119.

Corollary

Let $\mathcal{D}(q)$ be a quasi-symmetric design of Blokhuis-Haemers type, where q is a power of 2, $q \geq 4$. Then the binary code spanned by the rows of the block-by-point incidence matrix of $\mathcal{D}(q)$ is doubly even and self-orthogonal.

Examples

Example

$2-(64, 24, 46)$ [7]

$[n, k, d]_2$	$\#Aut(C)$	# non-equivalent
$[64, 13, 24]_2$	23224320	1
$[64, 12, 24]_2$	368640	1

[7] D. Crnković, B. G. Rodrigues, S. Rukavina, V. D. Tonchev, Quasi-symmetric 2-(64,24,46) designs derived from AG(3,4), Discrete Math. 340 (2017), 2472 – 2478.

Orbit matrices of 2-designs

Let $\mathcal{D}$ be a 2-(v,k,λ) design with replication number r, and $G \leq \mathrm{Aut}(\mathcal{D})$.

We denote the G-orbits of points by $\mathcal{P}_1,\dots,\mathcal{P}_m$, G-orbits of blocks by $\mathcal{B}_1,\dots,\mathcal{B}_n$, and put $|\mathcal{P}_i| = \omega_i$, $|\mathcal{B}_j| = \Omega_j$, $1 \leq i \leq m$, $1 \leq j \leq n$.

We denote by γ_{ij} the number of blocks of $\mathcal{B}_j$ incident with a representative of the point orbit $\mathcal{P}_i$.

The following equalities hold:

$$0 \leq \gamma_{ij} \leq \Omega_j, \quad 1 \leq i \leq m, 1 \leq j \leq n, \tag{1}$$

$$\sum_{j=1}^{n} \gamma_{ij} = r, \quad 1 \leq i \leq m, \tag{2}$$

$$\sum_{i=1}^{m} \frac{\omega_i}{\Omega_j}\gamma_{ij} = k, \quad 1 \leq j \leq n, \tag{3}$$

$$\sum_{j=1}^{n} \frac{\omega_t}{\Omega_j}\gamma_{sj}\gamma_{tj} = \lambda\omega_t + \delta_{st}\cdot(r-\lambda), \quad 1 \leq s,t \leq m. \tag{4}$$

A $(m \times n)$-matrix $M = (\gamma_{ij})$ with entries satisfying conditions (1) – (4) is called a point orbit matrix of a design 2-(v,k,λ) with orbit length distributions $(\omega_1,\dots,\omega_m)$ and $(\Omega_1,\dots,\Omega_n)$.

The main idea

We extend some previously done studies[8] using a connection between quasi-symmetric designs and strongly regular graphs by giving one additional condition on orbit matrices that can be applied only to quasi-symmetric designs.

[8] V. Krčadinac, R. Vlahović Kruc, Quasi-symmetric designs on 56 points, Adv. Math. Commun. 15 (2021), 633-646.

Block graph

When design $\mathcal{D}$ is quasi-symmetric, its block graph $\Gamma(\mathcal{D})$ can be defined by vertices representing the blocks such that two vertices are adjacent if the corresponding blocks intersect in y points.

If $\Gamma(\mathcal{D})$ is a connected graph, then it is a strongly regular graph, hence, we can use the known properties of orbit matrices for strongly regular graph and apply them here to orbit matrices of quasi-symmetric design.

Additional condition for quasi-symmetric designs

Let $\Gamma(\mathcal{D})$ be a SRG(b, a, c, d) and A be its adjacency matrix.

The correspondence of the vertices of the graph $\Gamma(\mathcal{D})$ to the blocks of design $\mathcal{D}$ gives us the following. Suppose an automorphism group G of $\Gamma(\mathcal{D})$ partitions the set of vertices V into n orbits $\mathcal{B}_1, \dots, \mathcal{B}_n$, with sizes $\Omega_1, \dots, \Omega_n$, respectively. This partition is equitable and, the quotient matrix $R = [r_{ij}]$, where r_{ij} represents the number of blocks from the block orbit $\mathcal{B}_j$ that intersect the block from the block orbit $\mathcal{B}_i$ in y points, satisfies the following conditions

$$\sum_{j=1}^{n} r_{ij} = \sum_{i=1}^{t} \frac{\Omega_i}{\Omega_j} r_{ij} = a, \tag{5}$$

$$\sum_{s=1}^{n} \frac{\Omega_s}{\Omega_j} r_{si} r_{sj} = \delta_{ij}(a - d) + \mu\Omega_i + (c - d) r_{ji}. \tag{6}$$

A $(n \times n)$-matrix $R = [r_{ij}]$ with entries satisfying conditions (5) and (6) is called a row orbit matrix for a strongly regular graph with parameters (b, a, c, d) and orbit lengths distribution $(\Omega_1, \dots, \Omega_n)$.

Additional condition for quasi-symmetric designs

Since $\Gamma(\mathcal{D})$, for a quasi-symmetric design, is strongly regular, we can obtain a connection of a point orbit matrix of the design and a row orbit matrix of its block graph in order to obtain the equations for point orbit matrix which will be valid just for quasi-symmetric block designs.

Let $B_j \in \mathcal{B}_j$ and lets count the number of elements in the set $\mathcal{S} = \{(P,B) \in \mathcal{P} \times \mathcal{B}_{j'} | P \in \langle B \rangle \cap \langle B_j \rangle\}$, where $\langle B \rangle$ represents the set of points contained in the block B and the same goes for $\langle B_j \rangle$. We get the following condition:

$$\frac{1}{\Omega_j} \sum_{i=1}^{m} \omega_i \gamma_{ij} \gamma_{ij'} = \sum_{B \in \mathcal{B}_{j'}} |\langle B \rangle \cap \langle B_j \rangle \ | = r_{jj'}(y-x) + \Omega_{j'} x + (k-x)\delta_{jj'}. \tag{7}$$

With the equation (7) we can reduce the number of possible point orbit matrices for quasi-symmetric designs with certain parameters and prescribed orbit length distributions.

Theorem

Let G be an automorphism group of a quasi-symmetric (v, k, λ) design $\mathcal{D}$ with intersection numbers x and y. Further, let G act on the set of points and the set of blocks of $\mathcal{D}$ in orbits of the same size m. If p is a prime dividing k, x and y, then the columns of the point orbit matrix of the design $\mathcal{D}$ with respect to G span a self-orthogonal code of length $\frac{v}{m}$ over the field $\mathbb{F}_q$, where $q = p^n$.

Given an orbit matrix M, the rows and columns that correspond to the non-fixed points and the non-fixed blocks form a submatrix called the **non-fixed part of the orbit matrix** M.

Theorem

Let G be an automorphism group of a quasi-symmetric (v, k, λ) design $\mathcal{D}$ with intersection numbers x and y, and M be the point orbit matrix of $\mathcal{D}$ with respect to G. Further, let G act on $\mathcal{D}$ with f fixed points, h fixed blocks, and all other orbits of the same size m. If a prime p divides m, $y - x$ and $k - x$, then the columns of the non-fixed part of the orbit matrix M span a self-orthogonal code over $\mathbb{F}_q$, where $q = p^n$.

Theorem

Let $\mathcal{D}(q)$ be a quasi-symmetric design of Blokhuis-Haemers type, where $q \geq 4$. Further, let G be an automorphism group of $\mathcal{D}(q)$ acting on the set of points and the set of blocks in orbits of length 2. Then the binary code spanned by the columns of the point orbit matrix of $\mathcal{D}(q)$ with respect to G is a doubly even self-orthogonal code of length $\frac{q^3}{2}$.

$$\frac{1}{\Omega_j}\sum_{i=1}^{m}\omega_i\gamma_{ij}\gamma_{ij'} = \sum_{B\in\mathcal{B}_{j'}} |\langle B\rangle \cap \langle B_j\rangle \,| = r_{jj'}(y-x) + \Omega_{j'}x + (k-x)\delta_{jj'}. \quad (8)$$

Thank you for your attention

UNIVERSITY OF RIJEKA
FACULTY OF MATHEMATICS