Block designs from self-dual codes obtained from Paley designs and Paley graphs

Ana Grbac [abaric@math.uniri.hr]
Dean Crnković [deanc@math.uniri.hr]
Andrea Švob[asvob@math.uniri.hr]

Faculty of Mathematics
University of Rijeka, Croatia

Rijeka Conference on Combinatorial Objects and Their Applications

7th July 2023

Outline of the Talk

1. Motivation
2. Preliminaries
3. General constructions of self-dual codes
4. Self-dual binary and ternary codes from Paley designs
5. Self-dual binary and ternary codes from Paley graphs

Motivation

- P. Gaborit, Quadratic double circulant codes over fields, J. Combin. Theory Ser. A 97 (2002), 85–107.
- V. Pless, On a new family of symmetry codes and related new five-designs, Bull. Am. Math. Soc. 75 (1969), 1339–1342.
- S. T. Dougherty, J.-L. Kim, P. Solé, Double circulant codes from two-class association schemes. Adv. Math. Commun. 1 (2007), 45–64.
- D. Crnković, A. Grbac, A. Švob, Formally self-dual LCD codes from two-class association schemes, Appl. Algebra Engrg. Comm. Comput. 34 (2023), 183–200.

Linear code

Definition

A **linear $[\mathbf{n}, \mathbf{k}]_\mathbf{q}$ code** $\mathcal{C}$ of length n and dimension k is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is the finite field with q elements (for a prime power q).

Definition

The **Hamming distance** between two codewords $x, y \in \mathbb{F}_q^n$ is defined by

$$d(x,y) = |\{i \mid x_i \neq y_i,\ 1 \leq i \leq n\}|.$$

The **minimum distance** of a code $\mathcal{C}$ is defined by

$$d = min\{d(x,y) \mid x,y \in \mathcal{C},\ x \neq y\}.$$

An $[n,k]_q$ linear code with minimum distance d will be denoted by $[n,k,d]_q$ code.

Linear code

Definition

The **Hamming weight** of a codeword $x \in \mathbb{F}_q^n$ is defined by

$$w(x) = |\{i \mid x_i \neq 0,\ 1 \leq i \leq n\}| = d(x, 0).$$

Definition

Given a linear $[n, k, d]_q$ code $\mathcal{C}$, a **generator matrix** G of $\mathcal{C}$ is a $k \times n$ matrix whose rows are the vectors of a base of the code.

Definition

Two codes are said to be **isomorphic** if one can be obtained from the other by permuting the coordinate positions.
Two codes over a finite field are called **equivalent** if one of the codes can be obtained from the other by permuting the coordinates and multiplication of components by non-zero elements.

Self-dual code

Definition

The **scalar product** of vectors $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in F_q^n$ is given by

$$x \cdot y = \sum_{i=1}^{n} x_i y_i.$$

Definition

The **dual code** of a linear code $\mathcal{C} \subset F_q^n$ is the code $\mathcal{C}^\perp \subset F_q^n$ where

$$\mathcal{C}^\perp = \{x \in F_q^n \mid x \cdot y = 0, \ \forall y \in \mathcal{C}\}.$$

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

The Paley graph

Definition (SRG(v, k, λ, μ))

A simple graph G of order v is **strongly regular** with parameters (v, k, λ, μ) if

- each vertex has degree k,
- each adjacent pair of vertices has λ common neighbours,
- each nonadjacent pair of vertices has μ common neighbours.

The Paley graph

Let q be a prime power such that $q \equiv 1 \pmod 4$. Then the *Paley graph* has as vertex set the elements of the finite field $GF(q)$, with two vertices being adjacent if and only if their difference is a nonzero square in $GF(q)$.

The Paley graph is SRG$(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$

Design

Definition

A ***t*-(v, k, λ) design** is a finite incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ satisfying:

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 $\mathcal{B}$.

A t-design without repeated blocks is called a *simple design*.
A 2-(v, k, λ) design is called *block design*.
If $b = v$, t-design is *symmetric*.

An automorphism of a design $\mathcal{D}$ is a permutation on $\mathcal{P}$ which sends blocks to blocks.

The Paley design

Definition

An **incidence matrix** $A = [a_{i,j}]$ of a symmetric design $\mathcal{D}$ is a $v \times v$ matrix with entries $0, 1$, having $a_{i,j} = 1$ if and only if $p_j \in B_i$.

The Paley design

Let q be a prime power such that $q \equiv 3 \pmod 4$. Then the *Paley design* has as vertex set the elements of the finite field $GF(q)$, and the blocks are the sets $Q + x$ ($x \in GF(q)$), where Q is the set of nonzero squares in $GF(q)$.

The Paley design is a symmetric design with parameters $(q, \frac{q-1}{2}, \frac{q-3}{4})$.

The support design of a code

Let w_i denote the number of codewords of weight i in a code C of length n.
The weight distribution of C is the list $[\langle i, w_i : 0 \leq i \leq n \rangle]$.
The support of a nonzero vector $x = (x_1, ..., x_n) \in \mathbb{F}_q^n$ is the set of indices of its nonzero coordinates, i.e.

$$\text{supp}(x) = \{i \mid x_i \neq 0\}.$$

The support design of a code of length n for a given nonzero weight w is the design with points the n coordinate indices and blocks the supports of all codewords of weight w.

In the case of binary codes support designs are simple, and otherwise the support designs have repeated blocks.

General constructions of self-dual codes

Let A be an adjacency matrix of a Paley strongly regular graph with parameters $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$, or an incidence matrix of a Paley design with parameters $(q, \frac{q-1}{2}, \frac{q-3}{4})$, and $\overline{A} = J_q - I_q - A$, where I_q and J_q are the identity and the all-one matrix of order q, respectively.

For arbitrary scalars $r, s, t \in R$, where R is a finite commutative ring with identity, let $Q_q^R(r, s, t) = (rI_q + sA + t\overline{A})$.

The pure and the bordered construction

The matrix $P_q^R(r,s,t) = \left[\ I_q \ \middle|\ Q_q^R(r,s,t)\ \right]$ generates a $[2n,n]$ code over R.
The matrix

$$B_q^R(r,s,t) = \left(\begin{array}{c|c|c|c} 1 & 0\ldots0 & \alpha & \beta\ldots\beta \\ \hline 0 & & \gamma & \\ \vdots & I_q & \vdots & Q_q^R(r,s,t) \\ 0 & & \gamma & \end{array}\right),$$

where $\alpha,\beta,\gamma \in R$, generates a $[2n+2,n+1]$ code over R.
The constructions of codes spanned by the matrices $P_q^R(r,s,t)$ and $B_q^R(r,s,t)$ are called the **pure** and the **bordered construction**, respectively.

Codes obtained from Paley designs

Theorem

The code generated by $P_q^R(r,s,t)$ *formed from an incidence matrix of a Paley design with parameters* $(4\lambda+3, 2\lambda+1, \lambda)$, *where* $\lambda = \frac{q-3}{4}$, *is self-dual over* R *if and only if*

$$r^2 + s^2 + t^2 + 2\lambda(s^2+t^2) = -1,$$
$$rt + sr + st + \lambda(s+t)^2 = 0.$$

Furthermore, the self-dual code $P_q^{\mathbb{Z}_{2m}}(r,s,t)$ *is Type II if and only if*

$$1 + r^2 + s^2 + t^2 + 2\lambda(s^2+t^2) \equiv 0 \mod 4m.$$

Theorem

The code generated by $B_q^R(r,s,t)$ *formed from an incidence matrix of a Paley design with parameters* $(4\lambda+3, 2\lambda+1, \lambda)$, $\lambda = \frac{q-3}{4}$, *is self-dual over* R *if and only if*

$$\begin{aligned} r^2+s^2+t^2+2\lambda(s^2+t^2) &= -(1+\gamma^2), \\ rt+sr+st+\lambda(s+t)^2 &= -\gamma^2, \\ 1+\alpha^2+3\beta^2+4\lambda\beta^2 &= 0, \\ \alpha\gamma+\beta(r+s+t)+2\lambda\beta(s+t) &= 0. \end{aligned}$$

The self-dual code $B_q^{\mathbb{Z}_{2m}}(r,s,t)$ *is Type II if and only if*

$$1+\gamma^2+r^2+s^2+t^2+2\lambda(s^2+t^2) \equiv 0 \mod 4m$$

and

$$1+\alpha^2+3\beta^2+4\lambda\beta^2 \equiv 0 \mod 4m.$$

Binary codes from Paley designs

r	s	t	$P_q^{\mathbb{F}_2}(r,s,t)$ self-dual	Type II
0	0	1	λ even	Never
0	1	0	λ even	Never
0	1	1	Never	-
1	0	0	Always	Never
1	0	1	Never	-
1	1	0	Never	-
1	1	1	Never	-

Table: Self-dual binary codes from Paley designs, pure construction

Binary codes from Paley designs

r	s	t	$B_q^{\mathbb{F}_2}(r,s,t)$ self-dual	Type II
0	0	1	λ even, $\gamma = 0$	Never
0	1	0	λ even, $\gamma = 0$	Never
0	1	1	$\gamma = 1$	$1 + \alpha^2 + 3\beta^2 + 4\lambda\beta^2 \equiv 0 \mod 4$
1	0	0	$\gamma = 0$	Never
1	0	1	λ even, $\gamma = 1$	$1 + \alpha^2 + 3\beta^2 + 4\lambda\beta^2 \equiv 0 \mod 4$
1	1	0	λ even, $\gamma = 1$	$1 + \alpha^2 + 3\beta^2 + 4\lambda\beta^2 \equiv 0 \mod 4$
1	1	1	Never	-

Table: Self-dual binary codes from Paley designs, bordered construction

Binary codes from Paley designs

Codes that are interesting in terms of parameters are obtained for a prime power $q = 11 + 8k$, in the following cases:

1. $P_q^{\mathbb{F}_2}(0, 0, 1)$
2. $P_q^{\mathbb{F}_2}(0, 1, 0)$
3. $B_q^{\mathbb{F}_2}(1, 0, 1)$ where $\alpha = 0$, $\beta = \gamma = 1$
4. $B_q^{\mathbb{F}_2}(1, 1, 0)$, where $\alpha = 0$, $\beta = \gamma = 1$.

Designs from binary codes

The Paley design with parameters $(11, 5, 2)$

The binary self-dual code obtained using $P_{11}^{\mathbb{F}_2}(0, 0, 1)$ (an isomorphic code is obtained for $P_{11}^{\mathbb{F}_2}(0, 1, 0)$) has parameters $[22, 11, 6]$.

From supports of the codewords of the binary code we obtained designs with parameters 3-$(22, 6, 1); b = 77$, 3-$(22, 8, 12); b = 330$, and 3-$(22, 10, 48); b = 616$. All the designs have $M_{22} : Z_2$ as the full automorphism group.

The binary self-dual code obtained using $B_{11}^{\mathbb{F}_2}(1, 1, 0)$ (an isomorphic code is obtained for $B_{11}^{\mathbb{F}_2}(1, 0, 1)$) has parameters $[24, 12, 8]$. This is the famous extended binary Golay code.

From supports of the codewords of the code we obtained designs with parameters 5-$(24, 8, 1); b = 77$, 5-$(24, 12, 48); b = 2576$, and 5-$(24, 16, 78); b = 759$. All these designs have the Mathieu group M_{24} as the full automorphism group.

Designs from binary codes

The Paley design with parameters $(27, 13, 6)$

The binary self-dual code obtained using $B_{27}^{\mathbb{F}_2}(1, 1, 0)$ (an isomorphic code is obtained for $B_{27}^{\mathbb{F}_2}(1, 0, 1)$) has parameters $[56, 28, 12]$. This is extremal doubly-even self-dual code described by Harada.

- M. Harada, Self-Orthogonal 3-(56,12,65) Designs and Extremal Doubly-Even Self-Dual Codes of Length 56, Des Codes Crypt 38 (2006), 5–16.

From supports of the codewords of the code we obtained a 3-$(56, 12, 65)$ design; $b = 8190$, and a 3-$(56, 16, 12572)$ design; $b = 622314$. Both designs have $L_2(27) : Z_6$ as the full automorphism group.

Ternary codes from Paley designs

r	s	t	$P_q^{\mathbb{F}_3}(r,s,t)$ self-dual
$\neq 0$	$\neq 0$	0	Never
$\neq 0$	0	$\neq 0$	Never
0	$\neq 0$	0	Never
0	0	$\neq 0$	Never
0	$\neq 0$	$\neq 0$	Never

Table: Self-dual ternary codes from Paley designs, pure construction

Ternary codes from Paley designs

r	s	t	$B_q^{\mathbb{F}_3}(r,s,t)$ self-dual
$\neq 0$	$\neq 0$	0	$\lambda \equiv 1 \mod 3, rs = \gamma^2 = 1$
$\neq 0$	0	$\neq 0$	$\lambda \equiv 1 \mod 3, rt = \gamma^2 = 1$
0	$\neq 0$	0	Never
0	0	$\neq 0$	Never
0	$\neq 0$	$\neq 0$	$\lambda \equiv 2 \mod 3, st = 2, \gamma^2 = 1$

Table: Self-dual ternary codes from Paley designs, bordered construction

Ternary codes from Paley designs

Codes that are interesting in terms of minimum distance are obtained for a prime power $q = 7 + 12k$, in the following cases:

1. $B_q^{\mathbb{F}_3}(a, a, 0)$, where $\alpha\gamma + \alpha\beta = 0, 1 + \alpha^2 + \beta^2 = 0, a, \alpha, \beta, \gamma \in \mathbb{F}_3^*$
2. $B_q^{\mathbb{F}_3}(a, 0, a)$, where $\alpha\gamma + \alpha\beta = 0, 1 + \alpha^2 + \beta^2 = 0, a, \alpha, \beta, \gamma \in \mathbb{F}_3^*$
3. $B_q^{\mathbb{F}_3}(a, a, b)$, where $\alpha\gamma + \alpha\beta = 0, 1 + \alpha^2 + \beta^2 = 0,$ $a, b, \alpha, \beta, \gamma \in \mathbb{F}_3^*, a \neq b$
4. $B_q^{\mathbb{F}_3}(a, b, a)$, where $\alpha\gamma + \alpha\beta = 0, 1 + \alpha^2 + \beta^2 = 0,$ $a, b, \alpha, \beta, \gamma \in \mathbb{F}_3^*, a \neq b,$

and a prime power $q = 11 + 12k$, for

$$B_q^{\mathbb{F}_3}(0, a, b), \text{ where } \alpha = 0, a, b, \beta, \gamma \in \mathbb{F}_3{}^*, a \neq b.$$

Designs from ternary codes

The Paley design with parameters $(7, 3, 1)$ (the Fano plane)

The ternary self-dual code obtained using $B_7^{\mathbb{F}_3}(a, a, 0)$ (equivalent codes are obtained for $B_7^{\mathbb{F}_3}(a, 0, a)$, $B_7^{\mathbb{F}_3}(a, a, b)$, $B_7^{\mathbb{F}_3}(a, b, a)$) has parameters $[16, 8, 6]$. This is an optimal ternary code.

From supports of the codewords of the code we obtained designs with parameters 3-$(16, 6, 4); b = 112$, 3-$(16, 9, 204); b = 1360$, and 3-$(16, 12, 495); b = 1260$. All the designs have $E_{64} : (L_3(2) : Z_2)$ as the full automorphism group.

Designs from ternary codes

The Paley design with parameters $(11, 5, 2)$

The ternary self-dual code obtained using $B_{11}^{\mathbb{F}_3}(0, a, b)$ has parameters $[24, 12, 9]$, and it is an optimal ternary code isomorphic to the one constructed by V. Pless.

- V. Pless, On a new family of symmetry codes and related new five-designs, Bull. Am. Math. Soc. 75 (1969), 1339–1342.
- V. Pless, Symmetry Codes over $GF(3)$ and New Five-Designs, J. Combin. Theory Ser. A 12 (1972), 119–142.

From supports of the codewords of the code we obtained designs with parameters 5-$(24, 9, 6); b = 2024$, 5-$(24, 12, 576); b = 30912$, and 5-$(24, 15, 8580); b = 121440$. All these designs have $Z_2 \times (L_2(11) : Z_2)$ as the full automorphism group.

We also obtained one 3-design with parameters 3-$(24, 18, 29784)$; $b = 73876$.

Designs from ternary codes

The Paley design with parameters $(19, 9, 4)$

The ternary self-dual code obtained using $B_{19}^{\mathbb{F}_3}(a, a, 0)$ (equivalent codes are obtained for $B_{19}^{\mathbb{F}_3}(a, 0, a)$, $B_{19}^{\mathbb{F}_3}(a, a, b)$ and $B_{19}^{\mathbb{F}_3}(a, b, a)$) has parameters $[40, 20, 12]$.

From supports of the codewords of the code we obtained designs with parameters 3-$(40, 12, 220)$; $b = 9880$ and 3-$(40, 15, 26208)$; $b = 569088$. Both the designs have $L_2(19) : Z_2$ as the full automorphism group.

Designs from ternary codes

The Paley design with parameters $(23, 11, 5)$

The ternary self-dual code obtained using $B_{23}^{\mathbb{F}_3}(0, a, b)$ has parameters $[48, 24, 15]$. This is an optimal ternary code isomorphic to the one constructed by V. Pless.
The designs obtained from this optimal code were described by V. Pless and all the designs have $Z_2 \times (L_2(23) : Z_2)$ as the full automorphism group.

Codes obtained from Paley graphs

Theorem

The code generated by $P_q^R(r,s,t)$ formed from an adjacency matrix of a Paley graph with parameters $(4\lambda+5, 2\lambda+2, \lambda, \lambda+1)$, where $\lambda = \frac{q-5}{4}$, is self-dual over R if and only if

$$r^2 + 2s^2 + 2t^2 + 2\lambda(s^2+t^2) = -1,$$
$$2rs + 2st + t^2 + \lambda(s+t)^2 = 0,$$
$$2rt + s^2 + 2st + \lambda(s+t)^2 = 0.$$

The self-dual code $P_q^{\mathbb{Z}_{2m}}(r,s,t)$ is Type II if and only if

$$1 + r^2 + 2s^2 + 2t^2 + 2\lambda(s^2+t^2) \equiv 0 \mod 4m.$$

Theorem

The code generated by $B_q^R(r,s,t)$ *formed from an adjacency matrix of a Paley graph with parameters* $(4\lambda+5, 2\lambda+2, \lambda, \lambda+1)$, *where* $\lambda = \frac{q-5}{4}$, *is self-dual over* R *if and only if*

$$\begin{aligned} r^2 + 2s^2 + 2t^2 + 2\lambda(s^2+t^2) &= -(1+\gamma^2), \\ 2rs + 2st + t^2 + \lambda(s+t)^2 &= -\gamma^2, \\ 2rt + s^2 + 2st + \lambda(s+t)^2 &= -\gamma^2, \\ 1 + \alpha^2 + 5\beta^2 + 4\beta^2\lambda &= 0, \\ \alpha\gamma + \beta(r+2s+2t) + 2\beta\lambda(s+t) &= 0. \end{aligned}$$

The self-dual code $B_q^{\mathbb{Z}_{2m}}(r,s,t)$ *is Type II if and only if*

$$1 + \gamma^2 + r^2 + 2s^2 + 2t^2 + 2\lambda(s^2+t^2) \equiv 0 \mod 4m$$

and

$$1 + \alpha^2 + 5\beta^2 + 4\lambda\beta^2 \equiv 0 \mod 4m.$$

Binary codes form Paley graphs

r	s	t	$P_q^{\mathbb{F}_2}(r,s,t)$ self-dual	Type II
0	0	1	Never	-
0	1	0	Never	-
0	1	1	Never	-
1	0	0	Always	Never
1	0	1	Never	-
1	1	0	Never	-
1	1	1	Never	-

Table: Self-dual binary codes from Paley graphs, pure construction

Binary codes form Paley graphs

r	s	t	$B_q^{\mathbb{F}_2}(r,s,t)$ self-dual	Type II
0	0	1	Never	-
0	1	0	Never	-
0	1	1	$\gamma = 1$	Never
1	0	0	$\gamma = 0$	Never
1	0	1	Never	-
1	1	0	Never	-
1	1	1	Never	-

Table: Self-dual binary codes from Paley graphs, bordered construction

All the binary codes that we obtained from Paley graphs have minimum distance equal to 2 or 4.

Ternary codes form Paley graphs

r	s	t	$P_q^{\mathbb{F}_3}(r,s,t)$ self-dual
$\neq 0$	$\neq 0$	0	Never
$\neq 0$	0	$\neq 0$	Never
0	$\neq 0$	0	Never
0	0	$\neq 0$	Never
0	$\neq 0$	$\neq 0$	Never

Table: Self-dual ternary codes from Paley graphs, pure construction

Ternary codes form Paley graphs

r	s	t	$B_q^{\mathbb{F}_3}(r,s,t)$ self-dual
$\neq 0$	$\neq 0$	0	Never
$\neq 0$	0	$\neq 0$	Never
0	$\neq 0$	0	Never
0	0	$\neq 0$	Never
0	$\neq 0$	$\neq 0$	$\lambda \equiv 0 \mod 3, \gamma^2 = 1, st = 2$

Table: Self-dual ternary codes from Paley graphs, bordered construction

Designs from ternary codes

Codes that are interesting in terms of minimum distance are obtained for a prime power $q = 5 + 12k$, using the construction

$$B_q^{\mathbb{F}_3}(0, a, b), \text{ where } \alpha = 0, a, b, \beta, \gamma \in {\mathbb{F}_3}^*, a \neq b.$$

The Paley SRG$(5, 2, 0, 1)$

The ternary self-dual code obtained using $B_5^{\mathbb{F}_3}(0, 1, 2)$ has parameters $[12, 6, 6]$, it is an optimal ternary code with this parameters. From supports of the codewords of the code we obtained the Witt design 5-$(12, 6, 1), b = 132$ having M_{12} as the full automorphism group.

Designs from ternary codes

The Paley SRG$(17, 8, 3, 4)$

The ternary self-dual code obtained using $B_{17}^{\mathbb{F}_3}(0, 1, 2)$ has parameters $[36, 18, 12]$ and it is isomorphic to the one constructed by V. Pless.

- V. Pless, On a new family of symmetry codes and related new five-designs, Bull. Am. Math. Soc. 75 (1969), 1339–1342.
- V. Pless, Symmetry Codes over $GF(3)$ and New Five-Designs, J. Combin. Theory Ser. A 12 (1972), 119–142.

The designs obtained from this optimal ternary code were described by V. Pless and all the designs have $Z_2 \times (L_2(17) : Z_2)$ as the full automorphism group.

Designs from ternary codes

The Paley SRG$(29, 14, 6, 7)$

The ternary self-dual code obtained using $B_{29}^{\mathbb{F}_3}(0, 1, 2)$ has parameters $[60, 30, 18]$ and it is the best known ternary code with this parameters. It is also constructed by V. Pless.
The designs obtained from this optimal ternary code were described by V. Pless and all the designs have $Z_2 \times (L_2(29) : Z_2)$ as the full automorphism group.