Glasnik Matematički

SERIJA III

www.math.hr/glasnik

Dean Crnković, Ana Grbac and Andrea Švob

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

Manuscript accepted
January 24, 2023.

BLOCK DESIGNS FROM SELF-DUAL CODES OBTAINED FROM PALEY DESIGNS AND PALEY GRAPHS

Dean Crnković, Ana Grbac and Andrea Švob
University of Rijeka, Croatia

Dedicated to the memory of Professor Zvonimir Janko

Abstract. In 2002, P. Gaborit introduced two constructions of self-dual codes using quadratic residues, so-called pure and bordered construction, as a generalization of the Pless symmetry codes. In this paper, we further study conditions under which the pure and the bordered construction using Paley designs and Paley graphs yield self-dual codes. Special attention is given to the binary and ternary codes. Further, we construct t-designs from supports of the codewords of a particular weight in the binary and ternary codes obtained.

1. Introduction

We assume that the reader is familiar with basic concepts of design theory, graph theory and coding theory. We refer the reader to [2] for background in design theory and to [14] for coding theory.

In [10], P. Gaborit introduced two constructions of self-dual codes from Paley designs and Paley graphs, so-called pure and bordered construction. The Gaborit's construction is a generalization of the construction of Pless symmetry codes [19]. This concept is further generalized in [9], where the authors studied codes obtained by the pure and bordered constructions from two-class association schemes. They applied this method to construct self-dual codes from some strongly regular graphs and doubly regular tournaments, including some rank 3 graphs and line graphs of complete or complete bipartite graphs and Steiner systems. Among others, in [9] the authors constructed two binary self-dual $[200, 100, 12]$ codes (Type I and Type II, respectively)

2020 *Mathematics Subject Classification.* 05B05, 05E30, 94B05.
Key words and phrases. Paley design, Paley graph, self-dual code, block design.

invariant under the action of the Higman-Sims group [12], and two binary self-dual $[200, 100, 16]$ codes (Type I and Type II, respectively) invariant under the action of the Janko group J_2 [15]. These self-dual codes with parameters $[200, 100, 12]$ and $[200, 100, 16]$ are constructed using the Higman-Sims graph [12] and the Hall-Janko graph [13], respectively. Recently, the pure and the bordered construction were used for a construction of formally self-dual LCD codes from two-class association schemes [7].

In this paper, we extend the study of self-dual codes obtained from Paley designs and Paley graphs using the pure and the bordered construction. We give conditions under which binary and ternary codes obtained by the pure and the bordered construction are self-dual and cover the cases not studied before. Further, we construct t-designs from supports of the codewords of a particular weight in the binary and ternary codes obtained by applying the pure and the bordered construction to some Paley designs and Paley graphs.

2. Preliminaries

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are jointly incident with precisely λ blocks. A design is called symmetric if it has the same number of points and blocks, and 2-designs are usually called block designs. An automorphism of a design $\mathcal{D}$ is a permutation on $\mathcal{P}$ which sends blocks to blocks. A design is called simple if it has no repeated blocks. Methods for constructing t-designs include the Kramer-Mesner method [18], the method using orbit matrices of a prescribed automorphism group [16], and constructions from codes (see, e.g., [3, 8, 19]).

A regular graph is strongly regular with parameters (v, k, λ, μ) if it has v vertices, degree k, and if any two adjacent vertices are jointly adjacent to λ vertices, while any two non-adjacent vertices are jointly adjacent to μ vertices. A strongly regular graph with parameters (v, k, λ, μ) is usually denoted by $\mathrm{SRG}(v, k, \lambda, \mu)$. A strongly regular graph is a distance-regular graph with diameter 2 whenever $\mu \neq 0$. The intersection array of an SRG is given by $\{k, k-1-\lambda; 1, \mu\}$ (see [5]). More on strongly graphs the reader can find in [6].

Let q be a prime power and let $\mathbb{F}_q$ be the field of order q. If $q \equiv 3 \mod 4$ then the non-zero squares in $\mathbb{F}_q$ form a Paley difference set, which leads to a symmetric $(q, \frac{q-1}{2}, \frac{q-3}{4})$ design called a Paley design (see [2]). In case when $q \equiv 1 \mod 4$, then the non-zero squares in $\mathbb{F}_q$ form a Paley partial difference set leading to a strongly regular graph with parameters $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$, called a Paley strongly regular graph.

A q-ary linear code C of dimension k, is a k-dimensional subspace of a vector space $\mathbb{F}_q^n$. The elements of C are called codewords. Let $x = (x_1, ..., x_n)$

and $y = (y_1, ..., y_n) \in \mathbb{F}_q^n$. 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 $d = \min\{d(x, y) : x, y \in C,\ x \neq y\}$. A q-ary linear code of length n and dimension k is called an $[n, k]_q$ code. An $[n, k]_q$ code of minimum distance d is called an $[n, k, d]_q$ code, or $[n, k, d]$ code when the order q of the field is understood. A linear $[n, k, d]$ code can detect at most $d - 1$ errors in one codeword and correct at most $t = \lfloor \frac{d-1}{2} \rfloor$ errors. A linear $[n, k, d]_q$ code C is called optimal if the minimum weight of C achieves the theoretical upper bound on the minimum weight of linear $[n, k]_q$ codes. Let w_i denote the number of codewords of weight i in a code C of length n. The weight of a codeword x is $w(x) = d(x, 0) = |\{i : x_i \neq 0\}|$. For a linear code, $d = \min\{w(x) : x \in C, x \neq 0\}$. The weight distribution of C is the list $[\langle i, w_i \rangle : 0 \leq i \leq n]$. 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. $\mathrm{supp}(x) = \{i | x_i \neq 0\}$. 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. Two codes are said to be isomorphic if one can be obtained from the other by permuting the coordinate positions. An automorphism of the code C is an isomorphism from C to C. 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. A generator matrix of an $[n, k]$ code is a $k \times n$ matrix whose rows are the vectors of a basis of the code.

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 following theorem, which is used for constructing self-dual codes, is given in [10].

THEOREM 2.1 (Theorem 3.1, [10]). *Let q be a power of an odd prime and let $Q_q^R(a, b, c)$ be a quadratic residue circulant matrix with a, b and c elements of R. If $q = 4k + 1$, then*

$$Q_q^R(a,b,c)Q_q^R(a,b,c)^t = Q_q^R(a^2 + 2k(b^2 + c^2), 2ab - b^2 + k(b+c)^2, 2ac - c^2 + k(b+c)^2)$$

and

$$Q_q^R(a,b,c)Q_q^R(a,b,c)^t = Q_q^R(a^2+4bck, ab+ac-bc+(b+c)^2k, \\ ab+ac-bc+(b+c)^2k).$$

If $q = 4k+3$*, then*

$$Q_q^R(a,b,c)Q_q^R(a,b,c)^t = Q_q^R(a^2+(2k+1)(b^2+c^2), ab+ac+k(b^2+c^2)+ \\ (2k+1)bc, ab+ac+k(b^2+c^2)+(2k+1)bc)$$

and

$$Q_q^R(a,b,c)Q_q^R(a,b,c)^t = Q_q^R(a^2+2bc(2k+1), 2ab+c^2+(b+c)^2k, \\ 2ac+b^2+(b+c)^2k).$$

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. Further, 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.

In the sequel, let R be a finite commutative ring with identity. A code of length n over R is a subset of R^n and the code is said to be linear if it is an R-submodule of R^n. Minimum distance, the weight and the support of a codeword, as well as an isomorphism between two codes, for codes over rings are defined in the same way as for codes over fields. The standard scalar product on R^n is defined as $x \cdot y = \sum x_i y_i$. The dual code $C^\perp$ of C is the orthogonal complement of C with respect to the standard scalar product. A code C is called self-orthogonal if $C \subseteq C^\perp$ and self-dual if $C = C^\perp$. A self-dual code C over $\mathbb{Z}_{2m}$ is called Type II if the Euclidean norm of every codeword of C is divisible by $4m$, otherwise it is called Type I. Computations in this paper consist of programs written for Magma [4].

3. Codes obtained from Paley designs

Note that the Paley construction from non-zero squares in a field $\mathbb{F}_q$, $q \equiv 3 \mod 4$, gives a symmetric design with parameters $(q, \frac{q-1}{2}, \frac{q-3}{4})$ having a skew incidence matrix. This skew matrix is an adjacency matrix of a doubly regular tournament with parameters $(q, \frac{q-1}{2}, \frac{q-3}{4}, \frac{q+1}{4})$.

The following statement follows from Theorem 3.4 in [9].

THEOREM 3.1. *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

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

PROOF. The statement follows from the equations given in [9, Theorem 3.4] and the fact that a skew incidence matrix of the Paley design with parameters $(4\lambda+3, 2\lambda+1, \lambda)$ is an adjacency matrix of a doubly regular tournament with parameters $(4\lambda+3, 2\lambda+1, \lambda, \lambda+1)$. □

Similarly, the following theorem follows from Theorem 3.5 given in [9].

THEOREM 3.2. *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*

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

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

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

3.1. *Binary codes form Paley designs.* In Tables 1 and 2, we give conditions under which the constructions from Paley designs yield self-dual binary codes, and which of the self-dual codes are Type II. These conditions follow from Theorems 3.1 and 3.2.

It turns out that codes that are interesting in terms of parameters are obtained for a prime power $q = 3+8k$, where k is a positive integer, 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 $\alpha = 0$, $\beta = \gamma = 1$.

TABLE 1. Self-dual binary codes from Paley designs, pure construction

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 2. Self-dual binary codes from Paley designs, bordered construction

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	-

3.1.1. *Designs from binary codes.* Using computations in Magma we obtained self-dual codes from Paley designs taking into consideration particular prime powers of the form $q = 3 + 8k$, where k is a positive integer. Further, we construct t-designs from supports of the codewords of a particular weight.

- Let $q = 11$. Then, the Paley design has 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 $M_{22} \rtimes Z_2$ as the full automorphism group. Since the Mathieu group M_{22} acts 3-transitively on 22 points, one can easily obtain above mentioned designs from the group action.

  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 $[24, 12, 8]$, i.e., it 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 and their existence has been known long ago. For more information see [1].

- Let $q = 27$. The Paley design has 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 $[56, 28, 12]$ and it is extremal doubly-even self-dual code described by Harada in [11]. From supports of the codewords of the code we obtained a 3-$(56, 12, 65)$ design; $b = 8190$, isomorphic to the one obtained in [11], and a 3-$(56, 16, 12572)$ design; $b = 622314$. Both designs have $L_2(27) \rtimes Z_6$ as the full automorphism group.

REMARK 3.3. If the weight distribution of a code and its dual code satisfy certain conditions, then the Assmus-Matson theorem (see [1]) guarantees that the codewords of these codes hold t-designs. In the examples described above, the existence of the designs in the codes constructed can be explained by the Assmus-Matson theorem.

3.2. *Ternary codes from Paley designs.* In Tables 3 and 4, we give conditions under which the constructions from Paley designs yield self-dual ternary codes. These conditions follow from Theorems 3.1 and 3.2. In the tables, we observe the case when the product $srt = 0$. The case $s = t = 0$ can not occur.

TABLE 3. Self-dual ternary codes from Paley designs, pure construction

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 4. Self-dual ternary codes from Paley designs, bordered construction

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	$\neq 0$	$\neq 0$	$\lambda \equiv 2 \mod 3$, $st = 2$, $\gamma^2 = 1$

Codes that are interesting in terms of minimum distance are obtained for a prime power $q = 7 + 12k$, k a non-negative integer, 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 $q=11+12k$, k a non-negative integer, for

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

3.2.1. *Designs from ternary codes.* Using computations in Magma we obtained self-dual codes from Paley designs taking into consideration the particular prime power q. Further, we construct t-designs from supports of the codewords of a particular weight in these ternary codes, as described below.

- Let $q=7$. In this case one obtains the Paley design with parameters $(7,3,1)$, known as 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 $[16,8,6]$, i.e., it 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 $E_{64}\rtimes(L_3(2)\rtimes Z_2)$ as the full automorphism group. By [17], the designs with these parameters were all known before.
- Let $q=11$. The Paley design has 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 in [19, 20]. From supports of the codewords of the code one obtains 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 $Z_2\times(L_2(11)\rtimes Z_2)$ as the full automorphism group. They are isomorphic to the 5-designs constructed by V. Pless in [19, 20]. Further, we obtained one 3-design with parameters 3-$(24,18,29784);b=73876$ which is not described by V. Pless in [19, 20] and one cannot find it in [17] also.
- Let $q=19$. The Paley design has 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 $L_2(19)\rtimes Z_2$ as the full automorphism group.
- Let $q=23$. Then the Paley design has parameters $(23,11,5)$. The ternary self-dual code obtained by using $B_{23}^{\mathbb{F}_3}(0,a,b)$ has parameters $[48,24,15]$, i.e., it is an optimal ternary code isomorphic to the one constructed by V. Pless in [19, 20]. The designs obtained from this

optimal code were described by V. Pless in [19, 20]. All the designs have $Z_2 \times (L_2(23) \rtimes Z_2)$ as the full automorphism group.

REMARK 3.4. The design with parameters 3-$(24, 18, 29784)$ having 73876 blocks obtained from Paley design for $q = 11$ is the only among the examples described above that cannot be described by Assmus-Matson theorem (see[1]). To our best knowledge it has not been known before.

4. Codes obtained from Paley graphs

The following theorem is a consequence of Theorem 3.4 given in [9].

THEOREM 4.1. *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*

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

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

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

PROOF. The statement follows from the equations given in [9, Theorem 3.4], taking into account the parameters of a Paley graph. □

Similarly, the following theorem is a consequence of Theorem 3.5 from [9].

THEOREM 4.2. *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

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

4.1. *Binary codes from Paley graphs.* In Tables 5 and 6, we present conditions under which the constructions from Paley graphs produce self-dual binary codes, and which of the self-dual codes are Type II. These conditions follow from Theorems 4.1 and 4.2.

TABLE 5. Self-dual binary codes from Paley graphs, pure construction

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 6. Self-dual binary codes from Paley graphs, bordered construction

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	-

REMARK 4.3. All the binary codes that we obtained from Paley graphs have minimum distance equal to 2 or 4.

4.2. *Ternary codes from Paley graphs.* In Tables 7 and 8, we give conditions under which the constructions from Paley graphs produce self-dual binary codes. These conditions follow from Theorems 4.1 and 4.2. In the tables, we observe the case when the product $srt = 0$. The case $s = t = 0$ can not occur.

We will investigate codes obtained in the case of prime powers of the form $q = 5 + 12k$, k is a non-negative integer, using the construction

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

4.2.1. *Designs from ternary codes.* Here we give self-dual codes from Paley graphs taking into consideration prime powers of the form $q = 5 + 12k$, k is a non-negative integer. Further, we construct t-designs from supports of the codewords of a particular weight in these ternary codes. The results are described below.

TABLE 7. Self-dual ternary codes from Paley graphs, pure construction

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 8. Self-dual ternary codes from Paley graphs, bordered construction

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	$\neq 0$	$\neq 0$	$\lambda \equiv 0 \mod 3$, $\gamma^2 = 1$, $st = 2$

- Let $q = 5$. Then, the strongly regular Paley graph has parameters $(5, 2, 0, 1)$. 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 famous Witt design 5-$(12, 6, 1)$; $b = 132$ having M_{12} as the full automorphism group.
- Let $q = 17$. Then the strongly regular Paley graph has parameters $(17, 8, 3, 4)$. 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 in [19, 20]. The designs obtained from this optimal ternary code were described by V. Pless in [19, 20]. All the designs have $Z_2 \times (L_2(17) \rtimes Z_2)$ as the full automorphism group.
- Let $q = 29$. In this case the strongly regular Paley graph has parameters $(29, 14, 6, 7)$. 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 constructed by V. Pless in [19, 20]. The designs obtained from this optimal ternary code were described by V. Pless in [19, 20]. The designs have $Z_2 \times (L_2(29) \rtimes Z_2)$ as the full automorphism group.

Acknowledgement
This work has been supported in part by Croatian Science Foundation under the project 5713. The authors would like to thank the anonymous referee for helpful comments that improved the presentation of the paper.

References

[1] E. F. Assmus, H. F. Matson, New 5-designs, J. Combinatorial Theory 6 (1969), 122–151.

[2] T. Beth, D. Jungnickel, H. Lenz, Design Theory, 2nd Edition, Cambridge University Press, Cambridge, 1999.

[3] A. Bonnecaze, P. Solé, The extended binary quadratic residue code of length 42 holds a 3-design, J. Combin. Des. 29 (2021), 528–532.

[4] W. Bosma, J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, 1994. http://magma.maths.usyd.edu.au/magma.

[5] A. E. Brouwer, A. M. Cohen, A. Neumaier, Distance-Regular Graphs, Springer-Verlag, Berlin, 1989.

[6] A. E. Brouwer, H. Van Maldeghem, Strongly regular graphs, Encyclopedia of Mathematics and its Applications 182, Cambridge University Press, Cambridge, 2022.

[7] D. Crnković, A. Grbac, A. Švob, Formally self-dual LCD codes from two-class association schemes, Appl. Algebra Engrg. Comm. Comput., 2021. https://doi.org/10.1007/s00200-021-00497-5

[8] D. Crnković, N. Mostarac, A. Švob, Distance-regular graphs and new block designs obtained from the Mathieu groups, Appl. Algebra Engrg. Comm. Comput., 2022. https://doi.org/10.1007/s00200-022-00542-x

[9] S. T. Dougherty, J.-L. Kim, P. Solé, Double circulant codes from two-class association schemes. Adv. Math. Commun. 1 (2007), 45–64.

[10] P. Gaborit, Quadratic double circulant codes over fields, J. Combin. Theory Ser. A 97 (2002), 85–107.

[11] 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.

[12] D. G. Higman, C. C. Sims, A simple group of order 44,352,000, Math. Z. 105 (1968), 110–113.

[13] M. Hall Jr., D. Wales, The simple group of order 604,800, J. Algebra 9 (1968), 417–450.

[14] W. C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.

[15] Z. Janko, Some new simple groups of finite order, I, Symposia Mathematica (INDAM, Rome, 1967/68), Vol. 1, Academic Press, London, 1969, pp. 25–64.

[16] Z. Janko, Coset enumeration in groups and constructions of symmetric designs, Combinatorics '90 (Gaeta, 1990), Ann. Discrete Math. 52 (1992), 275–277.

[17] G. B. Khosrovshahi, R. Laue, t-Designs with $t \geq 3$, in: C. J. Colbourn, J. H. Dinitz (Eds.), Handbook of Combinatorial Designs, 2^{nd} ed., Chapman & Hall/CRC, Boca Raton, 2007, pp. 852–868.

[18] E. S. Kramer, D. M. Mesner, t-designs on hypergraphs, Discrete Math. 15 (1976), 263–296.

[19] V. Pless, On a new family of symmetry codes and related new five-designs, Bull. Am. Math. Soc. 75 (1969), 1339–1342.

[20] V. Pless, Symmetry Codes over $GF(3)$ and New Five-Designs, J. Combin. Theory Ser. A 12 (1972), 119–142.

D. Crnković
Faculty of Mathematics
University of Rijeka
51000 Rijeka
Croatia
E-mail: deanc@math.uniri.hr

A. Grbac
Faculty of Mathematics
University of Rijeka
51000 Rijeka
Croatia
E-mail: agrbac@math.uniri.hr

A. Švob
Faculty of Mathematics
University of Rijeka
51000 Rijeka
Croatia
E-mail: asvob@math.uniri.hr