Advances in Mathematics of Communications

doi:10.3934/amc.2024040

LCD CODES CONSTRUCTED FROM WEAKLY p-SELF-ORTHOGONAL 1-DESIGNS

Vedrana Mikulić Crnković[*1], Ivona Traunkar[1] and Bernardo G. Rodrigues[2]

[1]Faculty of Mathematics, University of Rijeka, Radmile Matejčić 2, 51000 Rijeka, Croatia

[2]Department of Mathematics and Applied Mathematics, University of Pretoria, Private Bag X20, Hatfield, Pretoria 0028, South Africa

(Communicated by Ferruh Özbudak)

Abstract. By a suitable extension of incidence matrices, orbit matrices, and submatrices of orbit matrices of weakly p-self-orthogonal 1-designs, in this paper we describe a construction of LCD codes over a finite field. To illustrate the construction, we determine some binary LCD codes from self-orthogonal 1-designs which are invariant under the transitive non-regular action of the alternating group of order 60. With the described construction, we have obtained 6 optimal codes and 3 near-optimal codes.

1. **Introduction.** LCD codes (linear codes with complementary dual) are linear codes whose intersection with their dual codes is trivial. This particular type of code was introduced by Massey in [25], and over time a number of applications have been brought to light, particularly in communication systems, electronics, and cryptography. In addition, Massey showed that this class of codes provides an optimal linear coding solution for a binary adder channel with two users. It is known that LCD codes can be used for protection from side-channel attacks (SCA) and fault injection attacks (FIA), see [6]. In [20], Dougherty, Kim, Ozkaya, Sok, and Solé constructed binary LCD codes using self-dual codes, orthogonal matrices, and block designs. In [7], Carlet, Mesnager, Tang, and Qi described the general construction of LCD codes from linear codes and showed that any linear code over $\mathbb{F}_q$ $(q > 3)$ is equivalent to a Euclidean LCD code, and every linear code over $\mathbb{F}_{q^2}$ $(q > 2)$ is equivalent to a Hermitian LCD code. For binary codes and for some lengths n and dimensions k, there is no optimal linear $[n, k]$ LCD code. The bounds for minimal distance of binary and ternary LCD codes are more restrictive than those for linear codes in general, since LCD codes satisfy more conditions. Recently, in [5], Bouyuklieva extended the classification of optimal linear binary LCD codes up to length 40. In [13], Crnković, Egan, Rodrigues, and Švob constructed LCD codes using weighing matrices, including Paley conference matrices and Hadamard

2020 *Mathematics Subject Classification.* Primary: 05E18, 94B05; Secondary: 20D08, 05B05, 05E30.

Key words and phrases. Design, weakly p-self-orthogonal design, LCD code.

The first two authors are supported by [Croatian Science Foundation under the project 4571].

The third author is supported by [the National Research Foundation of South Africa (Grant Number CPRR23041894647)].

*Corresponding author: Vedrana Mikulić Crnković.

matrices, and extended their construction to obtain Hermitian LCD codes over the field $\mathbb{F}_4$.

In [27], Tonchev described some extensions of the incidence matrix of a weakly self-orthogonal design to obtain self-orthogonal codes, and in [15] the authors studied similar extensions of orbit matrices and submatrices of orbit matrices of 1-designs to construct binary self-orthogonal codes from Held's simple group **He**. In [26], the authors constructed self-orthogonal codes from weakly p-self-orthogonal 1-designs by defining suitable extensions of incidence matrices, orbit matrices, and submatrices of orbit matrices of 1-designs. In this paper, we use similar extensions of incidence matrices (Section 3.1), orbit matrices (Section 3.2.1), and submatrices of orbit matrices (Section 3.2.2, Section 3.2.3) of 1-designs and construct LCD codes over finite fields. In Section 4, we give some examples of known infinite families of weakly p-self-orthogonal designs and examples of LCD codes constructed from these designs.

2. Preliminaries.

Our notation for designs and groups will be standard, and it is as in [1] and the ATLAS [10].

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, and if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points together are incident with exactly λ blocks. An incidence matrix of a t-(v, k, λ) design $\mathcal{D}$ with b blocks is a $b \times v$ matrix $M = [m_{i,j}]$, where $m_{i,j} = 1$ if the point P_j is incident with the block B_i and 0 otherwise. If $b = v$, the design is called symmetric.

With M_p we denote the matrix obtained from the matrix M such that all entries of M_p are entries from M modulo p. With $M[i]$ we denote the i-th row of the matrix M.

A t-(v, k, λ) design is called **weakly self-orthogonal** if all block intersection numbers have the same parity. A design is **self-orthogonal** if it is weakly self-orthogonal and if the block intersection numbers and the block size are even numbers. A design is **weakly p-self-orthogonal** if all block intersection numbers give the same residue modulo p. A weakly p-self-orthogonal design is **p-self-orthogonal** if the block intersection numbers and the block sizes are multiples of p.

An isomorphism from one design to another is a bijective mapping from points to points and from blocks to blocks that preserves incidence. An isomorphism from a design $\mathcal{D}$ on itself is called an automorphism of $\mathcal{D}$. The set of all automorphisms of $\mathcal{D}$ forms its full automorphism group, which is denoted by $\mathrm{Aut}(\mathcal{D})$.

The **code $C_{\mathbb{F}}(\mathcal{D})$ of the design $\mathcal{D}$** over the finite field $\mathbb{F}$ is the space spanned by the incidence vectors of the blocks over $\mathbb{F}$. A code C over a field of order q with length n, dimension k, and minimum weight d is denoted by an $[n, k, d]_q$ code. If $q = 2$, we denote the code C by an $[n, k, d]$ code. The **dual** code $C^\perp$ is the orthogonal under the standard product, i.e. $C^\perp = \{v \in \mathbb{F}^n \mid vc = 0 \text{ for all } c \in C\}$.

A code C is **optimal** if for given n, k its minimum distance meets the theoretical bound. A code C is near-optimal if its minimum distance is one less than the minimum distance of an optimal code with the same parameters n, k. The optimality of LCD codes with length up to 40 is examined in [5] and in [21] for other lengths.

A code C is **self-orthogonal** if $C \subseteq C^\perp$, **self-dual** if $C = C^\perp$, and **LCD** if $C \cap C^\perp = \mathbf{0}$. If $\mathcal{D}$ is a self-orthogonal design, then the binary code of the design $\mathcal{D}$ is self-orthogonal. The all-one matrix of dimension n is denoted by J_n and is the $n \times n$ matrix with all entries equal to 1, and the all-one vector is denoted by $\mathbf{1}$

and is the constant vector with all coordinate entries equal to 1. Two linear codes are **equivalent** if they can be obtained by multiplying the coordinate positions with non-zero field elements or by permutation of the coordinate positions. An **automorphism** of a code C is an isomorphism from C to C. The full automorphism group is denoted by $\mathrm{Aut}(C)$. If the code $C_{\mathbb{F}}(\mathcal{D})$ is a linear code of a design $\mathcal{D}$ over a finite field $\mathbb{F}$, then the full automorphism group of $\mathcal{D}$ is contained in the full automorphism group of the code $C_{\mathbb{F}}(\mathcal{D})$.

A graph $\mathcal{G}$ is a **strongly regular** graph with parameters (v, k, λ, μ) if $\mathcal{G}$ is a k-regular graph with v vertices such that every two adjacent neighbours λ are common neighbours and every two non-adjacent neighbours μ are common neighbours. An adjacency matrix of a graph is the $v \times v$ matrix $A = [a_{i,j}]$, where $a_{i,j} = 1$ if vertex v_i and v_j are connected, and 0 otherwise.

3. Methods for constructing LCD codes from weakly p-self-orthogonal 1-designs.

3.1. **Constructions of LCD codes from incidence matrices.** In the following, we discuss the construction method we used to obtain the LCD codes presented in this article. But, first we state the following lemma, the proof of which follows from a standard computation.

Lemma 3.1. *Let a and d be real numbers. Then*

$$\det(dJ_n + (a-d)I_n) = (a-d)^{n-1}[a + (n-1)d].$$

Proof. Follows by induction on n. □

Remark 3.2. Let M be the $b \times v$ incidence matrix of a 1-design $\mathcal{D}$ with parameters 1-(v, k, λ) and b blocks $x_1, \ldots, x_b$. Denote by $B_{i,j}$ the size of the intersection of two distinct blocks x_i and x_j, for $i, j \in \{1, \ldots, b\}$. Then, the following holds.

1. $MM^T = \begin{bmatrix} B_{1,1} & B_{1,2} & \cdots & B_{1,b} \\ B_{2,1} & B_{2,2} & \cdots & B_{2,b} \\ \vdots & \vdots & \ddots & \vdots \\ B_{b,1} & B_{b,2} & \cdots & B_{b,b} \end{bmatrix}$.
2. $[M, xI_b][M, xI_b]^T = MM^T + x^2 I_b$.
3. $[M, y\mathbf{1}][M, y\mathbf{1}]^T = MM^T + y^2 J_b$.
4. $[M, xI_b, y\mathbf{1}][M, xI_b, y\mathbf{1}]^T = MM^T + x^2 I_b + y^2 J_b$.

Corollary 3.3. *Let $q = p^l$ be a prime power and let M be the $b \times v$ incidence matrix of a weakly p-self-orthogonal 1-design such that $k \equiv a \mod p$ and $B_{i,j} \equiv d \mod p$, and let x and y be non-zero elements of the field $\mathbb{F}_q$. Then, considering matrix multiplication in the field F_q, with respect to 0 being the addition neutral and 1 being multiplication neutral, the following holds:*

1. $\det(MM^T) = (a-d)^{b-1}[a + (b-1)d]$;
2. $\det([M, xI_b][M, xI_b]^T) = (a - d + x^2)^{b-1}[a + (b-1)d + x^2]$;
3. $\det([M, y\mathbf{1}][M, y\mathbf{1}]^T) = (a-d)^{b-1}[a + (b-1)d + by^2]$;
4. $\det([M, xI_b, y\mathbf{1}][M_p, xI_b, y\mathbf{1}]^T) = (a - d + x^2)^{b-1}[a + (b-1)d + x^2 + by^2]$.

Proof. The proof follows by a direct application of Lemma 3.1 and Remark 3.2. □

The following theorem can be deduced from the fact that a full rank matrix M is a generator matrix of an LCD code over the field $\mathbb{F}_q$ if and only if $\det(MM^T) \neq 0$.

Theorem 3.4. *Let $q = p^l$ be a prime power and let M be the $b \times v$ incidence matrix of a weakly p-self-orthogonal 1-design such that $k \equiv a \mod p$ and $B_{i,j} \equiv d \mod p$, and let x and y be non-zero elements of the field $\mathbb{F}_q$. Then, the following holds.*

1. *If $a = d = 0$, then*
   (a) *the matrix $[M, xI_b]$, and*
   (b) *the matrix $[M, xI_b, y\mathbf{1}]$ for $x^2 + by^2 \neq 0$,*
   generate an LCD code over the field $\mathbb{F}_q$.
2. *If $a = 0$ and $d \neq 0$, then*
   (a) *the matrix M if rows of M are linearly independent, and $b - 1 \neq 0$, and*
   (b) *the matrix $[M, xI_b]$ for $x^2 - d \neq 0$ and $x^2 + (b-1)d \neq 0$,*
   (c) *the matrix $[M, y\mathbf{1}]$ if rows of M are linearly independent, and for $by^2 + (b-1)d \neq 0$,*
   (d) *the matrix $[M, xI_b, y\mathbf{1}]$ for $x^2 - d \neq 0$ and $x^2 + by^2 + (b-1)d \neq 0$,*
   generate an LCD code over the field $\mathbb{F}_q$.
3. *If $a \neq 0$ and $d = 0$, then*
   (a) *the matrix M if rows of M are linearly independent, and*
   (b) *the matrix $[M, xI_b]$ for $x^2 + a \neq 0$,*
   (c) *the matrix $[M, y\mathbf{1}]$ if rows of M are linearly independent, and for $by^2 + a \neq 0$,*
   (d) *the matrix $[M, xI_b, y\mathbf{1}]$ for $x^2 + a \neq 0$ and $x^2 + by^2 + a \neq 0$,*
   generate an LCD code over the field $\mathbb{F}_q$.

4.1. *If $a \neq 0$, $d \neq 0$, and $a = d$, then*
   (a) *the matrix $[M, xI_b]$ for $x^2 + ba \neq 0$, and*
   (b) *the matrix $[M, xI_b, y\mathbf{1}]$ for $x^2 + by^2 + ba \neq 0$*
   generate an LCD code over the field $\mathbb{F}_q$.

4.2. *If $a \neq 0$, $d \neq 0$, and $a \neq d$, then*
   (a) *the matrix M if rows of M are linearly independent, and for $a + (b-1)d \neq 0$,*
   (b) *the matrix $[M, xI_b]$ for $x^2 + a - d \neq 0$ and $x^2 + a + (b-1)d \neq 0$,*
   (c) *the matrix $[M, y\mathbf{1}]$ if rows of M are linearly independent and for $by^2 + a + (b-1)d \neq 0$,*
   (d) *the matrix $[M, xI_b, y\mathbf{1}]$ for $x^2 + a - d \neq 0$ and $x^2 + by^2 + a + (b-1)d \neq 0$,*
   generate an LCD code over the field $\mathbb{F}_q$.

Remark 3.5. Notice that, if the rows of M are not linearly independent, we can use a maximal linearly independent set of incidence vectors as rows of a matrix M', and expand such matric in order to generate a p-ary LCD code.

Examples. Recall that each t-design with $t \geq 1$ is also 1-design. As a result we deduce the following.

1. Let $\mathcal{D}$ be a symmetric (v, k, λ) design and let M be its incidence matrix. Then, the following hold:
   (a) if the rows of M are linearly independent, k is odd, and λ is even, M and M^T generate a binary LCD $[v, v]$-code;
   (b) if the rows of M are linearly independent, k is even, and λ is odd, then both $[M, \mathbf{1}]$ and $[M^T, \mathbf{1}]$ generate a binary LCD $[v+1, v]$-code;
   (c) if k and λ are even, then $[M, I_v]$ and $[M^T, I_v]$ generate a binary LCD $[2v, v]$-code;
   (d) if k and λ are odd, then $[M, I_v, \mathbf{1}]$ and $[M^T, I_v, \mathbf{1}]$ generate a binary LCD $[2v+1, v]$-code.

2. Let $\mathcal{D}$ be a 2-(v,k,λ) design and let M be its incidence matrix. Let r be the replication number of the design $\mathcal{D}$, i.e. the number of blocks containing a given point. The dual design of $\mathcal{D}$ is a 1-design with block size r, intersection numbers equal to λ, and incidence matrix M^T. Then, the following assertions hold:
   (a) if the rows of M are linearly independent, r is odd, and λ is even, then M^T generates a binary LCD $[b,v]$-code;
   (b) if the rows of M are linearly independent, r is even, and λ is odd, then $[M^T,\mathbf{1}]$ generates a binary LCD $[b+1,v]$-code;
   (c) if r and λ are even, then $[M^T,I_v]$ generates a binary LCD $[b+v,v]$-code;
   (d) if r and λ are odd, then $[M^T,I_v,\mathbf{1}]$ generates a binary LCD $[b+v+1,v]$-code.
3. Let $\mathcal{G}$ be a strongly regular graph with parameters (v,k,λ,μ) and let A be its adjacency matrix. Then, A is the incidence matrix of a 1-(v,k,k) design with intersection numbers λ and μ. Then, the following holds:
   (a) if the rows of A are linearly independent, k is odd, and λ and μ are even, then A generates a binary LCD $[v,v]$-code;
   (b) if the rows of A are linearly independent, k is even, and λ and μ are odd, then $[A,\mathbf{1}]$ generates a binary LCD $[v+1,v]$-code;
   (c) if k, λ and μ are even, then $[A,I_v]$ generates a binary LCD $[2v,v]$-code;
   (d) if k, λ and μ are odd, then $[A,I_v,\mathbf{1}]$ generates a binary LCD $[2v+1,v]$-code.

3.2. **LCD codes from orbit matrices of weakly p-self-orthogonal designs.** Let $\mathcal{D}$ be a 1-design with nontrivial automorphism group G. For every prime number p that divides $|G|$, there is a cyclic group $P<G$ isomorphic to Z_p. Then, P acts on the set of points and the set of blocks of the design $\mathcal{D}$ in orbits of length 1 and p, and one can define an orbit matrix of the design for this action. In this section, we introduce methods for constructing LCD codes using orbit matrices and submatrices of orbit matrices of weakly p-self-orthogonal designs.

3.2.1. *Orbit matrices of a 1-design.*

Remark 3.6. Let $\mathcal{D}$ be a 1-(v,k,r) design, and let $G\leq Aut(\mathcal{D})$ be an automorphism group of the design. Let $v_1=|\mathcal{V}_1|,\ldots,v_n=|\mathcal{V}_n|$ be the sizes of point orbits and $b_1=|\mathcal{B}_1|,\ldots,b_m=|\mathcal{B}_m|$ be the sizes of block orbits under the action of the group G. Note that each block from a block orbit $\mathcal{B}_i$ is incident with the same number of points from an orbit $\mathcal{V}_j$, for any i,j. We define an orbit matrix under the action of G as an $m\times n$ matrix

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \ldots & a_{m,n} \end{bmatrix},$$

where $a_{i,j}$ is the number of points of an orbit $\mathcal{V}_j$ incident with a representative of the block orbit $\mathcal{B}_i$.

Now, it can be deduced from [15] that the orbit matrix is well-defined and that $k=\sum_{j=1}^{n}a_{i,j}$, and for $x\in\mathcal{B}_s$, by counting the incidence pairs (P,x') such that $x'\in\mathcal{B}_t$ and P is incident with the block x, we obtain $\sum_{x'\in\mathcal{B}_t}|x\cap x'|=\sum_{j=1}^{n}\frac{b_t}{v_j}a_{s,j}a_{t,j}$.

Remark 3.7. Let $\mathcal{D}$ be a 1-(v,k,r) design such that $k \equiv a \mod p$ and $|B_i \cap B_j| \equiv d \mod p$, for all $i,j \in \{1,\dots,b\}$, $i \neq j$, where B_i and B_j are two blocks of the design $\mathcal{D}$. Let $G \leq Aut(\mathcal{D})$ be an automorphism group of the design which acts on $\mathcal{D}$ with n point orbits of length w and block orbits of lengths $b_1, b_2, \dots, b_m$, and let O be the orbit matrix of the design $\mathcal{D}$ under the action of the group G. From Remark 3.6, for $x \in \mathcal{B}_s$ and $s \neq t$, one deduces $\frac{b_t}{w}O[s]O[t] = \sum_{j=1}^{n} \frac{b_t}{w} a_{s,j}a_{t,j} = \sum_{x' \in \mathcal{B}_t} |x \cap x'|$ so that $\frac{b_t}{w}O[s]O[t] \equiv b_t d \mod p$.

Now, for $x \in \mathcal{B}_s$ and $s = t$, we obtain $\frac{b_t}{w}O[s]O[s] = \sum_{x' \in \mathcal{B}_s} |x \cap x'| = |x \cap x| + \sum_{x' \in \mathcal{B}_s,\ x \neq x'} |x \cap x'|$ so that $\frac{b_s}{w}O[s]O[s] \equiv a + (b_s - 1)d \mod p$.

Let $\mathcal{D}$ be a 1-(v,k,r) design, and let $G \leq Aut(\mathcal{D})$ be an automorphism group of $\mathcal{D}$ acting with f_1 fixed points and n point orbits of length q, and with f_2 fixed blocks and m block orbits of length q. We define the matrices OM_1 and OM_2 to be, respectively, the matrices

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,f_1} \\ a_{2,1} & a_{2,2} & \dots & a_{2,f_1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{f_2,1} & a_{f_2,2} & \dots & a_{f_2,f_1} \end{bmatrix} \text{ and } \begin{bmatrix} a_{f_2+1,f_1+1} & a_{f_2+1,f_1+2} & \dots & a_{f_2+1,f_1+n} \\ a_{f_2+2,f_1+1} & a_{f_2+2,f_1+2} & \dots & a_{f_2+2,f_1+n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{f_2+m,f_1+1} & a_{f_2+m,f_1+2} & \dots & a_{f_2+m,f_1+n} \end{bmatrix},$$

where the columns $1, 2, \dots, f_1$ correspond to the fixed points, and the rows $1, 2, \dots, f_2$ correspond to the fixed blocks.

Remark 3.8. (a) If B_1 and B_2 are blocks fixed under the action of group G on the design, then B_1, B_2, and $B_1 \cap B_2$ are unions of some G-orbits of the point set.

(b) Let $\mathcal{B}_t$ and $\mathcal{B}_s$ be block orbits of size q under the action of the group G on the design. It follows from Remark 3.6 that

$$\sum_{x' \in \mathcal{B}_t} |x \cap x'| = \sum_{j=1}^{f_1} \frac{b_t}{v_j} a_{s,j}a_{t,j} + \sum_{j=f_1+1}^{f_1+n} \frac{b_t}{v_j} a_{s,j}a_{t,j} = q\sum_{j=1}^{f_1} a_{s,j}a_{t,j} + \sum_{j=f_1+1}^{f_1+n} a_{s,j}a_{t,j}.$$

3.2.2. *LCD codes from the orbit matrix of weakly p-self-orthogonal designs for a fix-point-free action.* As immediate consequence of the results presented in the preceding sections, we obtain the following theorems which outline the construction of LCD codes from orbit matrices.

Theorem 3.9. *Let $q = p^l$ be a prime power and let $\mathbb{F}_q$ be the finite field of order q. Let $\mathcal{D}$ be a 1-(v,k,λ) design such that $k \equiv a \mod p$ and $|B_i \cap B_j| \equiv d \mod p$, $\forall i,j \in \{1,\dots,b\}, i \neq j$, where B_i, B_j are blocks of the design $\mathcal{D}$. Let $G \leq Aut(\mathcal{D})$ be an automorphism group of the design $\mathcal{D}$ acting on the set of points of $\mathcal{D}$ with n orbits of length w, and acting on the set of blocks of $\mathcal{D}$ with m orbits of length w. Let O be the $m \times n$ orbit matrix under the action of the group G. Let x and y be non-zero elements of the field $\mathbb{F}_q$.*

1. *If $a = d$, then the following statements holds:*
   (a) *if $x^2 + mwd \neq 0$, then the linear code over $\mathbb{F}_q$ generated by the matrix $[O_p, xI_m]$ is an LCD code;*
   (b) *if $x^2 + my^2 + mwd \neq 0$, then the linear code over $\mathbb{F}_q$ generated by the matrix $[O_p, xI_m, y\mathbf{1}]$ is an LCD code.*
2. *If $a \neq d$, then the following statements holds:*
   (a) *if $d - a - mwd \neq 0$ and if the rows of O_p are linearly independent, then the linear code over $\mathbb{F}_q$ generated by the matrix O_p is an LCD code;*

(b) *if* $x^2 - d + a \neq 0$ *and* $x^2 + mwd - d + a \neq 0$, *the linear code over* $\mathbb{F}_q$ *generated by the matrix* $[O_p, xI_m]$ *is an LCD code;*

(c) *if* $mwd + my^2 - d + a \neq 0$ *and if the rows of* O_p *are linearly independent, then the linear code over* $\mathbb{F}_q$ *generated by the matrix* $[O_p, y\mathbf{1}]$ *is an LCD code;*

(d) *if* $x^2 - d + a \neq 0$ *and* $x^2 + mwd + my^2 - d + a \neq 0$, *then the linear code over* $\mathbb{F}_q$ *generated by the matrix* $[O_p, xI_m, y\mathbf{1}]$ *is an LCD code.*

Proof. 1. Using Remark 3.7, we obtain that $\forall s, t \in \{1, \dots m\},\ s \neq t, O_p[s]O_p[t] = wd$ and $O_p[s]O_p[s] = wd$. Using Lemma 3.1, it follows that

$$\det([O_p, xI_m][O_p, xI_m]^T) = \begin{vmatrix} wd + x^2 & wd & \dots & wd \\ wd & wd + x^2 & \dots & wd \\ \vdots & \vdots & \ddots & \vdots \\ wd & wd & \dots & wd + x^2 \end{vmatrix} = x^{2m-2}(x^2 + mwd),$$

$$\det([O_p, xI_m, y\mathbf{1}][O_p, xI_m, y\mathbf{1}]^T) = \begin{vmatrix} wd + x^2 + y^2 & wd + y^2 & \dots & wd + y^2 \\ wd + y^2 & wd + x^2 + y^2 & \dots & wd + y^2 \\ \vdots & \vdots & \ddots & \vdots \\ wd + y^2 & wd + y^2 & \dots & wd + x^2 + y^2 \end{vmatrix} = x^{2m-2}(x^2 + my^2 + mwd).$$

2. Using Remark 3.7, we obtain that $\forall s, t \in \{1, \dots m\},\ s \neq t,\ O_p[s]O_p[t] = wd$ and $O_p[s]O_p[s] = a + (w-1)d$. Using Lemma 3.1, it follows that

$$\det(O_p O_p^T) = \begin{vmatrix} a + (w-1)d & wd & \dots & wd \\ wd & a + (w-1)d & \dots & wd \\ \vdots & \vdots & \ddots & \vdots \\ wd & wd & \dots & a + (w-1)d \end{vmatrix} = (a - d)^{m-1}(a - d + mwd),$$

$$\det([O_p, xI_m][O_p, xI_m]^T) = \begin{vmatrix} a + (w-1)d + x^2 & wd & \dots & wd \\ wd & a + (w-1)d + x^2 & \dots & wd \\ \vdots & \vdots & \ddots & \vdots \\ wd & wd & \dots & a + (w-1)d + x^2 \end{vmatrix} = (a - d + x^2)^{m-1}(a - d + x^2 + mwd),$$

$$\det([O_p, y\mathbf{1}][O_p, y\mathbf{1}]^T) = \begin{vmatrix} a + (w-1)d + y^2 & wd + y^2 & \dots & wd + y^2 \\ wd + y^2 & a + (w-1)d + y^2 & \dots & wd + y^2 \\ \vdots & \vdots & \ddots & \vdots \\ wd + y^2 & wd + y^2 & \dots & a + (w-1)d + y^2 \end{vmatrix} = (a - d)^{m-1}(a - d + mwd + my^2),$$

$$\det([O_p, xI_m, y\mathbf{1}][O_p, xI_m, y\mathbf{1}]^T)$$

$$= \begin{vmatrix} a+(w-1)d+x^2+y^2 & wd+y^2 & \dots & wd+y^2 \\ wd+y^2 & a+(w-1)d+x^2+y^2 & \dots & wd+y^2 \\ \vdots & \vdots & \ddots & \vdots \\ wd+y^2 & wd+y^2 & \dots & a+(w-1)d+x^2+y^2 \end{vmatrix}$$

$$= (a-d+x^2)^{m-1}(a-d+x^2+my^2+mwd).$$

□

3.2.3. *LCD codes from submatrices of the orbit matrix of weakly p-self-orthogonal designs for an action with fixed points.*

Theorem 3.10. *Let $q = p^l$ be a prime power and let $\mathbb{F}_q$ be the finite field of order q. Let $\mathcal{D}$ be a 1-(v,k,λ) design such that $k \equiv a \mod p$ and $|B_i \cap B_j| \equiv d \mod p$, $\forall i,j \in \{1,\dots,b\}, i \neq j$, where B_i, B_j are blocks of the design $\mathcal{D}$. Let $G \leq Aut(\mathcal{D})$ be an automorphism group of the design $\mathcal{D}$ that acts on the set of points of $\mathcal{D}$ with f_1 fixed points and n orbits of length p^α, $1 \leq \alpha \leq l$, and acts on the set of blocks of $\mathcal{D}$ with f_2 fixed blocks and m orbits of length p^α. Let x and y be non-zero elements of the field $\mathbb{F}_q$.*

1. *If $a = d$, then the following statements hold:*
   - *OM1)* (a) *if $x^2 + f_1 a \neq 0$, then the linear code over $\mathbb{F}_q$ generated by the matrix $[OM_{1_p}, xI_{f_1}]$ is an LCD code;*
     (b) *if $x^2 + f_1 y^2 + f_1 a \neq 0$, the linear code over $\mathbb{F}_q$ generated by the matrix $[OM_{1_p}, xI_{f_1}, y\mathbf{1}]$ is an LCD code.*
   - *OM2)* (a) *A linear code over $\mathbb{F}_q$ generated by the matrix $[OM_{2_p}, xI_m]$ is an LCD code;*
     (b) *for $x^2 + my^2 \neq 0$, the linear code over $\mathbb{F}_q$ generated by the matrix $[OM_{2_p}, xI_m, y\mathbf{1}]$ is an LCD code.*
2. *If $a \neq d$, then the following statements hold:*
   - *OM1)* (a) *if the rows of the matrix OM_{1_p} are linearly independent, then the linear code over $\mathbb{F}_q$ generated by the matrix OM_{1_p} is an LCD code;*
     (b) *for $x^2 + a \neq 0$, the linear code over $\mathbb{F}_q$ generated by the matrix $[OM_{1_p}, xI_{f_1}]$ is an LCD code;*
     (c) *if the rows of the matrix OM_{1_p} are linearly independent and $a + f_1 y^2 \neq 0$, then the linear code over $\mathbb{F}_q$ generated by the matrix $[OM_{1_p}, y\mathbf{1}]$ is an LCD code;*
     (d) *if $x^2 + a \neq 0$ and $x^2 + f_1 y^2 + f_1 a \neq 0$, then the linear code over $\mathbb{F}_q$ generated by the matrix $[OM_{1_p}, xI_{f_1}, y\mathbf{1}]$ is an LCD code.*
   - *OM2)* (a) *if the rows of the matrix OM_{2_p} are linearly independent, then the linear code over $\mathbb{F}_q$ generated by the matrix OM_{2_p} is an LCD code;*
     (b) *if $x^2 + a - d \neq 0$, then the linear code over $\mathbb{F}_q$ generated by the matrix $[OM_{2_p}, xI_m]$ is an LCD code;*
     (c) *if the rows of the matrix OM_{2_p} are linearly independent and $a - d + my^2 \neq 0$, then the linear code over $\mathbb{F}_q$ generated by the matrix $[OM_{2_p}, y\mathbf{1}]$ is an LCD code;*
     (d) *if $x^2 + a - d \neq 0$ and $x^2 + my^2 + a - d \neq 0$, then the linear code over $\mathbb{F}_q$ generated by the matrix $[OM_{2_p}, xI_m, y\mathbf{1}]$ is an LCD code.*

Proof. 1. Let $a = d$.

OM1) Since $k \equiv a \mod p$, each block contains $p\beta + a$ fixed points for some non-negative integer β, and since $|B_i \cap B_j| \equiv a \mod p$, for all $i,j \in$

$\{1,\dots,b\}$, $i \neq j$, the intersection of each two distinct blocks contains $p\gamma + a$ fixed points for some non-negative integer γ,
Using Remark 3.8, we obtain $OM_{1_p}[s]OM_{1_p}[s] = a$ and $OM_{1_p}[s]OM_{1_p}[t] = a$ for every $s,t \in \{1,\dots,f_1\}$, $s \neq t$. Furthermore, Lemma 3.1 shows that

$$\det(OM_{1_p}OM_{1_p}^T) = \begin{vmatrix} a & a & \dots & a \\ a & a & \dots & a \\ \vdots & \vdots & \ddots & \vdots \\ a & a & \dots & a \end{vmatrix}_{f_1\times f_1} = 0.$$

$$\det([OM_{1_p}, xI_{f_1}][OM_{1_p}, xI_{f_1}]^T) = \begin{vmatrix} x^2+a & a & \dots & a \\ a & x^2+a & \dots & a \\ \vdots & \vdots & \ddots & \vdots \\ a & a & \dots & x^2+a \end{vmatrix}_{f_1\times f_1}$$
$$= (x^2)^{f_1-1}(x^2+f_1a)$$

$$\det([OM_{1_p}, y\mathbf{1}][OM_{1_p}, y\mathbf{1}]^T) = \begin{vmatrix} a+y^2 & a+y^2 & \dots & a+y^2 \\ a+y^2 & a+y^2 & \dots & a+y^2 \\ \vdots & \vdots & \ddots & \vdots \\ a+y^2 & a+y^2 & \dots & a+y^2 \end{vmatrix}_{f_1\times f_1} = 0,$$

and

$$\det([OM_{1_p}, xI_{f_1}, y\mathbf{1}][OM_{1_p}, xI_{f_1}, y\mathbf{1}]^T)$$
$$= \begin{vmatrix} a+x^2+y^2 & a+y^2 & \dots & a+y^2 \\ a+y^2 & a+x^2+y^2 & \dots & a+y^2 \\ \vdots & \vdots & \ddots & \vdots \\ a+y^2 & a+y^2 & \dots & a+x^2+y^2 \end{vmatrix}_{f_1\times f_1}$$
$$= x^{2f_1-2}(x^2+f_1y^2+f_1a).$$

$OM2$) For $s \neq t$, since $\mathcal{B}_t$ is an orbit of length p^α, by Remark 3.8 we obtain $\sum_{x'\in\mathcal{B}_t}|x\cap x'| \equiv p^\alpha a \equiv 0 \mod p$, and for $s = t$ we have $\sum_{x'\in\mathcal{B}_s}|x\cap x'| = |x\cap x| + \sum_{x'\in\mathcal{B}_s,\ x\neq x'}|x\cap x'| \equiv a + (p^\alpha - 1)a \equiv 0 \mod p$. Hence, $OM_{2p}[s]OM_{2p}[s] = 0$ for every $s \in \{1,\dots,m\}$.
Now, using Lemma 3.1, we show that

$$\det(OM_{2p}{OM_{2p}}^T) = \begin{vmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{vmatrix}_{m\times m} = 0$$

$$\det([OM_{2p}, xI_m][OM_{2p}, xI_m]^T) = \begin{vmatrix} x^2 & 0 & \dots & 0 \\ 0 & x^2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & x^2 \end{vmatrix}_{m\times m} = x^{2m}$$

$$\det([OM_{2_p}, y\mathbf{1}][OM_{2_p}, y\mathbf{1}]^T) = \begin{vmatrix} y^2 & y^2 & \dots & y^2 \\ y^2 & y^2 & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & y^2 \end{vmatrix}_{m\times m} = 0,$$

and

$$\det([OM_{2_p}, xI_m, y\mathbf{1}][OM_{2_p}, xI_m, y\mathbf{1}]^T) = \begin{vmatrix} x^2+y^2 & y^2 & \dots & y^2 \\ y^2 & x^2+y^2 & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & x^2+y^2 \end{vmatrix}_{m\times m} = x^{2m-2}(x^2+my^2).$$

2. Let $a \neq d$.

   $OM1$) Since $k \equiv a \mod p$, each block contains $p\beta + a$ fixed points for some non-negative integer β, and since $|B_i \cap B_j| \equiv d \mod p$, for all $i, j \in \{1, \dots, b\}$, $i \neq j$, the intersection of any two distinct blocks contains $p\gamma + d$ fixed points for some non-negative integer γ.
   Using Remark 3.8, we obtain $OM_{1_p}[s]OM_{1_p}[s] = a$ and $OM_{1_p}[s]OM_{1_p}[t] = d$, for every $s, t \in \{1, \dots, f_1\}$, $s \neq t$.

   $OM2$) For $s \neq t$, since $\mathcal{B}_t$ is an orbit of length p^α, by Remark 3.8 we obtain $\sum_{x'\in\mathcal{B}_t} |x \cap x'| \equiv p^\alpha d \equiv 0 \mod p$, and for $s = t$ we have $\sum_{x'\in\mathcal{B}_s} |x \cap x'| = |x \cap x| + \sum_{x'\in\mathcal{B}_s,\ x\neq x'} |x \cap x'| \equiv a + (p^\alpha - 1)d \equiv a - d \mod p$. Thus, we have $OM_{2_p}[s]OM_{2_p}[s] = a - d$ and $OM_{2_p}[s]OM_{2_p}[t] = 0$ for all $s, t \in \{1, \dots, m\}$, $s \neq t$.
   Finally, using Lemma 3.1 once more, we show that

$$\det(OM_{2_p}{OM_{2_p}}^T) = \begin{vmatrix} a-d & 0 & \dots & 0 \\ 0 & a-d & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a-d \end{vmatrix}_{m\times m} = (a-d)^m$$

$$\det([OM_{2_p}, xI_m][OM_{2_p}, xI_m]^T) = \begin{vmatrix} x^2+a-d & 0 & \dots & 0 \\ 0 & x^2+a-d & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & x^2+a-d \end{vmatrix}_{m\times m} = (x^2+a-d)^m$$

$$\det([OM_{2_p}, y\mathbf{1}][OM_{2_p}, y\mathbf{1}]^T) = \begin{vmatrix} y^2+a-d & y^2 & \dots & y^2 \\ y^2 & y^2+a-d & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & y^2+a-d \end{vmatrix}_{m\times m} = (a-d)^{m-1}(a-d+my^2),$$

and

$$\det([OM_{2_p}, xI_m, y\mathbf{1}][OM_{2_p}, xI_m, y\mathbf{1}]^T)$$

$$= \begin{vmatrix} x^2+y^2+a-d & y^2 & \dots & y^2 \\ y^2 & x^2+y^2+a-d & \dots & y^2 \\ \vdots & \vdots & \ddots & \vdots \\ y^2 & y^2 & \dots & x^2+y^2+a-d \end{vmatrix}_{m\times m}$$
$$= (x^2+a-d)^{m-1}(x^2+a-d+my^2).$$

□

Remark 3.11. Determining the minimum distance of the codes and weight distribution remains a challenging quest and we keep this as an open question.

4. Examples of LCD codes constructed from weakly p-self-orthogonal 1-designs.

4.1. Some known families of weakly p-self-orthogonal designs and LCD codes.

- Symmetric designs.
  We mention some of the infinite families of symmetric designs which are weakly p-self orthogonal for some prime p. The reader could find more examples of such families in [9, Chapter 6.8.].
  1. Point-hyperplane designs. Recall that such designs have parameters $v = \frac{(q^{m+1}-1)}{q-1}$, $k = \frac{q^m-1}{q-1}$, $\lambda = \frac{q^{m-1}-1}{q-1}$, $q = p^l$ a prime power, and $m \geq 2$. Points and blocks of the designs are points, and hyperplanes of the projective geometry $PG(m,q)$.
     Note that these designs are weakly p-self-orthogonal since $k \equiv 1 \mod p$ and $\lambda \equiv 1 \mod p$.
     For example, the point-hyperplane design of the projective space $PG(3,2)$ is a 2-$(15,7,3)$ weakly self-orthogonal design. By applying Theorem 3.4 (case 4.1.), a $[31,15,4]$ LCD code with automorphism group A_8 can be obtained.
  2. Menon designs.
     The parameters of the design are $v = 4t^2, k = 2t^2 - t$, and $\lambda = t^2 - t$. A design with these parameters exists if and only if there exists a regular Hadamard matrix of order $4t^2$. It is conjectured ([9]) that these designs exist for all values of t. The incidence matrix of a Menon design is given by $M = \frac{1}{2}(J_{4t^2} - H)$, and H is a regular Hadamard matrix in which the sum of every row is equal to $2t$. In [11], the author gave a construction of Menon designs for p and $2p-1$ prime powers and $p \equiv 3 \mod 4$.
     Note that these designs are p-self-orthogonal for every prime p dividing t.
     For example, if we take matrix H to be the first matrix (labeled 36a) in https://documents.uow.edu.au/~jennie/matrices/H36/36R.html and replace all -1 with 0 we obtain a point-block incidence matrix of a Menon design with 36 points which is 3-self orthogonal. Now, applying Theorem 3.4 (case 1), we obtain $[72,36,6]_3$ and $[73,36,6]_3$ LCD codes.
- Quasi-symmetric designs.
  1. In [3], Blokhuis and Haemers constructed an infinite family of quasi-symmetric 2-$(q^3, q^2(q-1)/2, q(q^3-q^2-2)/4)$ designs with block intersection numbers $q^2(q-2)/4$ and $q^2(q-1)/4$, where q is a power of 2.
     For $q > 2$, these designs are self-orthogonal since $k \equiv 0 \mod 2$ and the block intersection numbers are even.

2. In [24], the authors found many new quasi-symmetric 2-$(28, 12, 11)$ and 2-$(36, 16, 12)$ designs. In [23], one can find a table of known quasi-symmetric designs along with their incidence matrices.
   For example, if we consider the first incidence matrix of a 2-$(28, 12, 11)$ quasi-symmetric design with intersection numbers 4 and 6, we observe that this design is self-orthogonal, and so using Theorem 3.4 (case 1), we obtain a $[91, 63, 3]$ LCD code.

- Strongly regular graphs.
  1. The triangular graph $T(n)$ is a graph whose vertices are 2-element subsets of an n-elements set, two pairs being adjacent if and only if they have an element in common. $T(n)$ is a strongly regular graph with parameters $\left(\binom{n}{2}, 2(n-2), n-2, 4\right)$.
     If $n > 2$ is even, the adjacency matrix of $T(n)$ is the incidence matrix of a self-orthogonal 1-design since $k \equiv 0 \mod 2$ and the block intersection numbers are even.
     For example, $T(4)$ is a strongly regular graph with parameters $(6, 4, 2, 4)$ whose adjacency matrix is an incidence matrix of a 1-$(6, 4, 2)$ self-orthogonal design. Applying Theorem 3.4 (case 1), we obtain a $[9, 6, 2]$ LCD code with automorphism group $Z_2 \times S_4$.

4.2. **LCD codes constructed from weakly self-orthogonal 1-designs invariant under the transitive action of the group A_5.** In this section, we present LCD codes constructed using the method described in Theorem 3.4 from weakly self-orthogonal 1-designs that admit a transitive action of the alternating group A_5. We constructed the 1-designs by applying the following construction introduced in [16].

Theorem 4.1. *Let G be a finite permutation group acting transitively on the sets Ω_1 and Ω_2 of size m and n, respectively. Let $\alpha \in \Omega_1$ and $\Delta_2 = \bigcup_{i=1}^{s} \delta_i G_\alpha$, where $\delta_1, \cdots, \delta_s \in \Omega_2$ are representatives of distinct G_α-orbits. If $\Delta_2 \neq \Omega_2$ and $\mathcal{B} = \{\Delta_2 g : g \in G\}$, then $\mathcal{B}$ is set of blocks of a $1-(n, |\Delta_2|, \frac{|G_\alpha|}{|G_{\Delta_2}|} \sum_{i=1}^{s} |\alpha G_{\delta_i}|)$ design with $\frac{m \cdot |G_\alpha|}{|G_{\Delta_2}|}$ blocks. The group $H \cong G/\bigcap_{x \in \Omega_2} G_x$ acts as an automorphism group on the design transitively on points and blocks of the design. If $\Delta_2 = \Omega_2$, then the set $\mathcal{B}$ consists of one block.*

Recall that any transitive action of a group G on a set Ω is equivalent to the action by left (or right) multiplication of the group G on the set of cosets G/P, where P is a stabiliser of an element of Ω for the given action.

Let G be a group isomorphic to the alternating group A_5. To obtain 1-designs that admit a transitive action of G, we apply Theorem 4.1 as follows:

- Consider faithful transitive action of the group G of degree n, i.e. $n \leq |G|$. Without loss of generality, we define Ω_2 as $\{1, \ldots n\}$. Note that this action of G on Ω_2 is equivalent to the action of G on G/P by multiplication where $P = G_1$ and $n = [G : P]$.
- Consider the subgroup $H < G$, $H \neq \{1_G\}$, and define $\Delta_2 = \bigcup_{i=1}^{s} \delta_i H$ for all combinations of representatives of different H-orbits on Ω_2. Note that in this case $\Omega_1 = G/H$ and G acts transitively on Ω_1 by multiplication. If $P = H$, then $b \leq v$.

Note that by using conjugate subgroups of G, one will obtain isomorphic 1-designs.

Applying the steps described above, we constructed 1-designs from all transitive actions of the permutation group $G \cong A_5$, and for each, up to conjugation, $H < G$, $H \neq \{1_G\}$, and we single out the weakly-self orthogonal designs. We have constructed exactly 182 weakly self-orthogonal 1-designs that are invariant under the action of G. The following table lists weakly self-orthogonal 1-designs from which we constructed optimal and near-optimal LCD codes.

The table contains number of points of the constructed design, i.e. $|\Omega_2|$, subgroup $H < A_5$ used to obtain the base block of the design, parameters of the weakly self-orthogonal 1-design, parameters of the corresponding binary LCD code, and the structure of automorphism group of the code. Minimum distances and automorphism groups of the codes are computed using the computational algebra system MAGMA ([4]). Optimal codes are marked with *, near-optimal codes with **.

n	$H < A_5$	**Design**	C	**Aut**(C)
20	Z_2	1-$(20, 12, 3)$	$[25, 5, 11]*$	$E_{2^4} : (E_{2^4} : S_5)$
20	Z_2	1-$(20, 14, 7)$	$[30, 10, 9] **$ $[31, 10, 10]*$	S_5
20	Z_5	1-$(20, 15, 9)$	$[20, 12, 4]*$ $[21, 12, 4] **$	$Z_2 \times S_5$
12	D_{10}	1-$(12, 10, 5)$	$[18, 6, 6] **$	$(E_{2^5} : A_6) : E_{2^2}$
10	Z_2	1-$(10, 6, 3)$	$[11, 5, 4]*$	S_5
10	Z_2	1-$(10, 5, 3)$	$[10, 6, 3]*$ $[11, 6, 4]*$	S_5

TABLE 1. Optimal and near-optimal binary LCD codes constructed from WSO 1-designs from group A_5

Tables with the parameters of all LCD codes constructed from weakly self-orthogonal 1-designs, as well as all constructed designs can be found here: https://www.math.uniri.hr/~inovak/LCD/

4.3. **Examples of LCD codes constructed from orbit matrices of weakly p-self-orthogonal 1-designs, $p \in \{3, 5\}$.** Using Theorem 4.1, we constructed examples of weakly 3-self-orthogonal designs and weakly 5-self-orthogonal designs from the permutation representation of the group $S_4(9)$ on 1640 points. The orbit matrices of the constructed designs were obtained under the action of the cyclic group of order 5, which acts on the points of the design, i.e. in orbits of length 5. Using Theorem 3.9, we constructed LCD codes over the finite fields of order 3 and 5, with at least one example for each case described in the theorem. Table 2 lists the constructed LCD codes and the corresponding 1-designs.

The following tables are be ordered by five cases of weakly p-self-orthogonal designs as follows:

Case 1. Codes obtained from p-self-orthogonal designs.
Case 2. Codes obtained from weakly p-self-orthogonal designs such that $a = 0$, $d \neq 0$.
Case 3. Codes obtained from weakly p-self-orthogonal designs such that $a \neq 0$, $d = 0$.
Case 4.1 Codes obtained from weakly p-self-orthogonal designs such that $a = d \neq 0$.
Case 4.2 Codes obtained from weakly p-self-orthogonal designs such that $a \neq 0$, $d \neq 0$, $a \neq d$.

Design	C	**Case**
1-$(1640, 729, 729)$	$[657, 328, 2]_3$	1
1-$(1640, 1458, 729)$	$[492, 164, 2]_3$ $[493, 164, 2]_3$	1
1-$(1640, 1638, 819)$	$[329, 164, 1]_3$	2
1-$(1640, 2, 1)$	$[328, 164, 2]_3$ $[329, 164, 3]_3$	3
1-$(1640, 182, 91)$	$[493, 164, 4]_3$	4.1
1-$(1640, 911, 911)$	$[656, 328]_3$	4.1
1-$(1640, 1458, 729)$	$[328, 164, 2]_5$ $[492, 164, 12]_5$ $[493, 164, 12]_5$ $[329, 164, 3]_5$	4.2
1-$(1640, 1638, 819)$	$[493, 164, 3]_5$ $[493, 164, 4]_5$	4.2

TABLE 2. LCD codes obtained from p-self orthogonal designs, $p \in \{3, 5\}$, using Theorem 3.9

Using weakly 3-self-orthogonal 1-designs constructed from the group $S_4(9)$ on 1640 points, we have constructed LCD codes using Theorem 3.10. The orbit matrices of the designs are obtained under the action of a cyclic group of order 3 acting on the points of the designs of lengths 1 and 3. The following table lists the LCD codes constructed using Theorem 3.9 as indicated above. It also presents the corresponding 1-designs, with construction examples given for 4 of the 5 cases of the weakly p-self-orthogonal designs described.

Design	C	Case
1-$(1640, 182, 91)$	$[57, 19, 1]_3$ $[58, 19, 2]_3$ $[1068, 534]_3$ $[1069, 534]_3$	1
1-$(1640, 729, 729)$	$[76, 38, 1]_3$ $[801, 267]_3$ $[802, 267]_3$	1
1-$(1640, 1638, 819)$	$[39, 19, 1]_3$ $[534, 267, 2]_3$ $[535, 267, 3]_3$	2
1-$(1640, 2, 1)$	$[38, 19, 2]_3$ $[534, 267, 2]_3$ $[535, 267, 3]_3$	3
1-$(1640, 182, 91)$	$[58, 19, 2]_3$ $[801, 267]_3$ $[802, 267]_3$	4.1
1-$(1640, 911, 911)$	$[76, 38, 2]_3$ $[77, 38, 2]_3$ $[1068, 534]_3$ $[1069, 534]_3$	4.1

TABLE 3. LCD codes obtained from weakly 3-self orthogonal designs using Theorem 3.9

REFERENCES

[1] E. F. Assmus and J. D. Key, *Designs and their Codes*, Cambridge University Press, Cambridge, 1992.

[2] A. Baartmans, I. Landjev and V. D. Tonchev, On the binary codes of Steiner triple systems, *Des. Codes Cryptogr.*, **8** (1996), 29-43.

[3] A. Blokhuis and W. H. Haemers, An infinite family of quasi-symmetric designs, *Journal of Statistical Planning and Inference*, **95** (2001), 117-119.

[4] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, **24** (1997), 235-265

[5] S. Bouyuklieva, Optimal binary LCD codes, *Des. Codes Cryptogr.*, **89** 2021, 2445–2461.

[6] C. Carlet and S. Guilley, Complementary dual codes for counter-measures to side-channel attacks, *Adv. Math. Commun.*, **10** (2016), 131-150.

[7] C. Carlet, S. Mesnager, C. Tang, Y. Qi and R. Pellikaan, Linear codes over F_q which are equivalent to LCD codes for $q > 3$, *IEEE Trans. Inform. Theory*, **64** (2018), 3010-3017.

[8] N. Chigira, M. Harada and M. Kitazume, Permutationgroups and binary self-orthogonal codes, *J. Algebra*, **309** (2007), 610-621.

[9] C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs*, Second Edition (Discrete Mathematics and Its Applications), Chapman and Hall/CRC (2006).

[10] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *ATLAS of Finite Groups*, Oxford: Oxford University Press, 1985.

[11] D. Crnković, A series of regular Hadamard matrices, *Des. Codes Crypt.*, **39** (2006), 247-251.

[12] D. Crnković, D. Dumičić Danilović and S. Rukavina, On symmetric (78,22,6) designs and relatedself-orthogonal codes, *Util. Math.*, **109** (2018), 227-253.

[13] D. Crnković, R. Egan, B. G. Rodrigues and A. Švob, LCD codes from weighing matrices, *Appl. Algebra Engrg. Comm. Comput.*, **32** (2021), 175-189.

[14] D. Crnković, R. Egan and A. Švob, Constructingself-orthogonal and Hermitian self-orthogonal codes via weighingmatrices and orbit matrices, *Finite Fields Appl.*, **55** (2019), 64-77.

[15] D. Crnković, V. Mikulić Crnković and B. G. Rodrigues, On self-orthogonaldesigns and codes related to Held's simple group, *Adv. Math. Commun.*, **12** (2018), 607-628.

[16] D. Crnković, V. Mikulić Crnković and A. Švob, Onsome transitive combinatorial structures constructed from the unitarygroup $U(3, 3)$, *J. Statist. Plann. Inference*, **144** (2014), 19-40.

[17] D. Crnković and N. Mostarac, Self-dual codes fromorbit matrices and quotient matrices of combinatorial designs, *Discrete Math.*, **341** (2018), 3331-3343.

[18] D. Crnković, B. G. Rodrigues, S. Rukavina and L. Simčić, Self-orthogonal codes from orbit matrices of 2-designs, *Adv. Math. Commun.*, **7** (2013), 161-174.

[19] D. Crnković and S. Rukavina, Self-dual codes fromextended orbit matrices of symmetric designs, *Des. Codes Cryptogr.*, **79** (2016), 113-120.

[20] S. T. Dougherty, J.-L. Kim, B. Ozkaya, L. Sok and P. Solé, The combinatorics of LCD codes: Linear programming bound and orthogonal matrices, *Int. J. Inf. Coding Theory.*, **4** (2017) 116-128.

[21] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, Online available at `http://www.codetables.de`.

[22] M. Harada and V. D. Tonchev, Self-orthogonal codes fromsymmetric designs with fixed-point-free automorphisms, *Discrete Math.*, **264** (2003), 81-90.

[23] V. Krčadinac, Quasi-symmetric designs, `https://web.math.pmf.unizg.hr/~krcko/results/quasisym.html`.

[24] V. Krčadinac and R. Vlahović, New quasi-symmetric designs by the Kramer-Mesner method, *Discrete Math.*, **339** (2016), 2884-2890.

[25] J. L. Massey, Linear codes with complementary duals, *Discrete Math.*, **106/107** (1992), 337-342.

[26] V. Mikulić Crnković and I. Traunkar, Self-orthogonal codes constructed from weakly self-orthogonal designs invariant under an action of M_{11}, *AAECC*, **34** (2023), 139-156.

[27] V. D. Tonchev, Self-orthogonal designs and extremaldoubly-even codes, *Journal of Combinatorial Theory, Series A*, **52** (1989), 197-205.

[28] V. D. Tonchev, Quantum codes from finite geometry andcombinatorial designs, Finite Groups, Vertex Operator Algebras, and Combinatorics, *ResearchInstitute for Mathematical Sciences*, **1656** (2009), 44-54.

Received May 2023; 1st revision January 2024; 2nd revision May 2024; early access September 2024.