Binary codes from some 2-(64, 28, 12) designs and their orbit matrices.

L. Chikamai [*] and B. G. Rodrigues [†]
School of Mathematical Sciences
University of KwaZulu-Natal
Durban 4041, South Africa

Jamshid Moori [‡]
School of Mathematical Sciences
North-West University (Mafikeng)
Mmabatho 2735, South Africa

Abstract

It is known that there are at least 8784 non-isomorphic designs with parameters 2-(64, 28, 12) whose derived 2-(28, 12, 11) designs are quasi-symmetric. In this paper we examine the binary codes related to a class of non-isomorphic designs with these parameters and invariant under the Frobenius group of order 21 for which the derived 2-(28, 12, 11) designs are not quasi-symmetric. We show that up to equivalence there are 30 non-isomorphic binary codes obtained from them. Moreover, we classify the self-orthogonal doubly-even codes of length 13 obtained from the non-fixed parts of orbit matrices of these 2-(64, 28, 12) designs under an action of an automorphism group of order four having 12 fixed points. The subcodes of codimension 1 and minimum weight 8 in these codes are all optimal single weight codes.

[*] NRF scholarship is acknowledged. This work is part of the first author's PhD.
[†] Support of the NRF through incentive grant is acknowledged.
[‡] NRF incentive and competitive grants are acknowledged.

1 Introduction

According to [10] (see also [17, Table II.1, p. 38]) there are at least 8784 designs with parameters 2-$(64, 28, 12)$ whose derived 2-$(28, 12, 11)$ designs are quasi-symmetric. An undertaking to classify the codes of such designs is made unfeasible by this overwhelming number. However, it was proved by Jungnickel and Tonchev in [15] that there exist four non-isomorphic symmetric 2-$(64, 28, 12)$ designs characterized by the symmetric difference property and minimality of their 2-ranks. Moreover, these designs have large full automorphism groups, and also large 2-subgroups. In particular, the orders of the full automorphism groups are divisible by 2^6, and their derived 2-$(28, 12, 11)$ quasi-symmetric designs give rise to four inequivalent $[28, 7, 12]_2$ codes. More recently Crnković and Pavčević in [7], constructed a class of 46 non-isomorphic 2-$(64, 28, 12)$ designs for which 2^6 is not a divisor of the order of their full automorphism groups and have in addition shown that none of the derived designs (with parameters 2-$(28, 12, 11)$) is quasi-symmetric, thus proving that the said designs are non-isomorphic to those with the same parameters constructed in [10, 15, 19]. In an earlier paper [3] (see also [4]) using modular representation theoretic methods we examined the structure of a $[28, 7, 12]_2$ code invariant under the symplectic group $S_6(2)$. The supports of the codewords of minimum weight 12 in that code give rise to a 2-$(28, 12, 11)$ quasi-symmetric design which is a derived design of the unique point-primitive and flag-transitive 2-$(64, 28, 12)$ design with automorphism group isomorphic to $2^6{:}S_6(2)$(this is one of the four non-isomorphic designs with these parameters constructed in [10, 15, 19]). That study led us to announce the investigation of the binary codes of the class of 46 non-isomorphic 2-$(64, 28, 12)$ designs described above. Hence, in this paper we examine codes defined by the binary row span of the incidence matrices of the 46 non-isomorphic 2-$(64, 28, 12)$-designs obtained in [7] and deduce through computations with Magma [1], the following main result:

Theorem 1 *Let $\mathfrak{D}$ be any of the* 2-$(64, 28, 12)$ *designs given in [7], and C the binary code spanned by the row of the incidence matrix of $\mathfrak{D}$. Then*
(i) *C is a self-orthogonal, self-complementary and doubly-even code;*
(ii) *the 2-rank of $\mathfrak{D}$ is either 26 or 27;*
(iii) *if the 2-rank of $\mathfrak{D}$ is 26, then the minimum weight of C is 12 or 16, and the minimum weight of $C^{\perp}$ is 8;*
(iv) *if the 2-rank of $\mathfrak{D}$ is 27, then the minimum weight of C is 8, and the minimum weight of $C^{\perp}$ is 4, 6 or 8;*
(v) *the automorphism group of C is isomorphic to* $\mathrm{Frob}_{21}, \mathrm{Frob}_{21}\times 2$, $\mathrm{Frob}_{21}\times D_8$, $\mathrm{Frob}_{42}\times 2$, $(\mathrm{Frob}_{42}\times 2){:}2$ *or* $(\mathrm{Frob}_{21}\times D_8){:}2$.

An active area of research in coding theory is the classification of self-orthogonal codes of small length or dimension, see for example [13, 21, 20]. Several methods and techniques are used for this purpose, among which the method of orbit matrices (see Section 4 for a brief discussion on this method). In the present paper, using the method of orbit matrices as presented in [9] we completely enumerate and classify the self-orthogonal codes of length 13 (Theorem 7) defined by the action of an automorphism of order 4 on the non-fixed parts of the orbit matrices obtained from the 2-(64, 28, 12) designs in discussion. We establish some properties of the codes and the nature of some classes of codewords and observe that the subcodes of codimension 1 are all single weight optimal codes. The proof of Theorem 1 follows from a series of lemmas and propositions given in Section 3.

The paper is organized as follows: after a brief description of our terminology and some background, in Sections 3 and 4 we outline the construction of the codes and present our results.

2 Terminology and notation

We assume that the reader is familiar with some basic notions and elementary facts from strongly regular graphs, design and coding theory. Our notation for designs and codes are standard. For the structure of groups we follow the Atlas [6] notation. The groups $G \cdot H$, $G{:}H$, and $G^{\cdot}H$ denote a general extension, a split extension and a non-split extension respectively. 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 together incident with precisely λ blocks. The **complement** of $\mathcal{D}$ is the structure $\tilde{\mathcal{D}} = (\mathcal{P}, \mathcal{B}, \tilde{\mathcal{I}})$, where $\tilde{\mathcal{I}} = \mathcal{P} \times \mathcal{B} - \mathcal{I}$. The **dual** structure of $\mathcal{D}$ is $\mathcal{D}^t = (\mathcal{B}, \mathcal{P}, \mathcal{I}^t)$, where $(\mathcal{B}, \mathcal{P}) \in \mathcal{I}^t$ if and only if $(\mathcal{P}, \mathcal{B}) \in \mathcal{I}$. Thus the transpose of an incidence matrix for $\mathcal{D}$ is an incidence matrix for $\mathcal{D}^t$. The design is **symmetric** if it has the same number of points and blocks. In a 2-(v, k, λ) design every point is incident with exactly $r = \dfrac{\lambda(v-1)}{k-1}$ blocks, and r is called the **replication number** of a design. The number $n = r - \lambda$ is called the **order** of a 2-(v, k, λ) design. Given a symmetric 2-(v, k, λ) design $\mathcal{D}$, a **residual** design of $\mathcal{D}$ is the design obtained by deleting a block of $\mathcal{D}$ and retaining those points not incident with the block. A residual design at any block of $\mathcal{D}$ is a 2-$(v - k, k - \lambda, \lambda)$ design. A **derived** design of $\mathcal{D}$ with respect to a block is the design obtained by deleting a block and retaining those points incident with the block. A derived design of $\mathcal{D}$ with respect to a block is a 2-$(k, \lambda, \lambda - 1)$ design. The numbers that occur as the size of the intersection of two distinct blocks are the **intersection numbers** of the design. A t-(v, k, λ) design is called **self-orthogonal** if the intersection numbers have the same parity as the block size. An automorphism of a design $\mathcal{D}$ is a permutation on $\mathcal{P}$ which sends blocks to blocks. The set of all automorphisms of $\mathcal{D}$ forms its full automorphism group denoted by Aut$\mathcal{D}$.

The **code C_F of the design $\mathcal{D}$** over the finite field F is the space spanned by the incidence vectors of the blocks over F. If the point set of $\mathcal{D}$ is denoted by $\mathcal{P}$ and the block set by $\mathcal{B}$, and if $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $\mathcal{Q}$ by $v^{\mathcal{Q}}$. Thus $C_F = \langle v^B \mid B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F. All our codes will be **linear codes**, i.e. subspaces of the ambient vector space. If a code C over a field of order q is of length n, dimension k, and minimum weight d, then we write $[n, k, d]_q$ to show this information. A code has minimum distance d if and only if every $d - 1$ columns in a parity check matrix are linearly independent. The **support**, Supp(v), of a vector v is the set of coordinate positions where the entry in v is non-zero. So $|\text{Supp}(v)| = \text{wt}(v)$, where wt$(v)$ is the weight of v. An $[n, k]$ linear code C is said to be a **best known linear $[n, k]$ code** if C has the highest minimum weight among all known $[n, k]$ linear codes. An $[n, k]$ linear code C is said to be an **optimal linear** $[n, k]$ code if the minimum weight of C achieves the theoretical upper bound on the minimum weight of $[n, k]$ linear codes. The weight enumerator of C is defined as $W_C(x) = \sum_{i=0}^{n} A_i x^i$, where A_i denotes the number of codewords of weight i in C. The **dual** code $C^{\perp}$ is the orthogonal complement under the standard inner product $(\cdot, \cdot)$, i.e. $C^{\perp} = \{v \in F^n | (v, c) = 0 \text{ for all } c \in C\}$. The all-one vector will be denoted by $\mathbf{1}$, and is the constant vector of weight the length of the code and has all entries equal to 1. A code C is **self-orthogonal** if $C \subseteq C^{\perp}$ and it is **self-complementary** if it contains the all-one vector. A binary code C is **doubly-even** if all codewords of C have weight divisible by four. A binary code is even if all its codewords have even weight. An **automorphism** of a code is any permutation of the coordinate positions that maps codewords to codewords and will be denoted Aut(C).

Crnković and Pavčević [7] proved the following:

Result 1 *(***Crnković & Pavčević***) There are 46 non-isomorphic symmetric* 2-(64, 28, 12) *designs with the Frobenius group of order 21 as an automorphism group; these are given in [7].*

3 The binary codes from 2-(64, 28, 12) designs

If A is an incidence matrix of a 2-(v, k, λ) design and $\text{rank}_p(A) < v - 1$, then it is well known that this code is interesting only when p divides $r - \lambda$, the order of the design (see [20, Theorem 1.86]) and p is a prime. Now, let $\mathfrak{D}$ denote a 2-(64, 28, 12) design, since the order of each design is 16, only the binary codes will be of interest for characterization purposes. In the following lemma we collect a number of properties of the code C of a design $\mathfrak{D}$ that will be of use in the sequel.

Lemma 2 *Let C be the binary code of a symmetric* 2-(64, 28, 12) *design $\mathfrak{D}$. Then*
(i) *C is self-orthogonal and doubly-even;*
(ii) *C is self-complementary;*
(iii) *$C^{\perp}$ is an even and self-complementary code with minimum weight at least 4;*
(iv) *unless $\mathfrak{D}$ is a design with the symmetric difference property, the derived designs are not quasi-symmetric.*

Proof: For $i \neq j$ consider B_i and B_j two distinct blocks in each $\mathfrak{D}$. Since $|B_i \cap B_j| = 12 \equiv 0 \pmod 2$ and $k = 28 \equiv 0 \pmod 2$, we have that $\mathfrak{D}$ is a self-orthogonal design. Hence the block-point incidence matrix of $\mathfrak{D}$ spans a self-orthogonal code of length 64, and since the spanning vectors have weight divisible by four it follows that C is doubly-even. Since the blocks of $\mathfrak{D}$ are of even size, we have that $\mathbf{1}$ meets evenly every vector of C, so $\mathbf{1} \in C^{\perp}$. Hence $C^{\perp}$ is self-complementary. Moreover, since $\mathfrak{D}$ satisfies $r \equiv \lambda \pmod 4$ we have from [5, Theorem 3(i)] that $\mathbf{1} \in C$, and consequently C is self-complementary, and all weights in $C^{\perp}$ are even. Set $d^{\perp} = d(C^{\perp})$ to be the minimum weight of $C^{\perp}$. From $C^{\perp}$ singly-even we obtain that $d^{\perp} \equiv 0 \pmod 2$. Moreover, since $C \neq 0$ and for $\mathfrak{D}$ we have $r \neq 2\lambda$, we deduce from [18, Lemma 5] that $d^{\perp} \geq 4$. ■

It is known that there are at least 8784 designs with parameters 2-(64, 28, 12) whose derived 2-(28, 12, 11) designs are quasi-symmetric, [17, Table II.1, p. 38]. A definite listing of the codes, their properties and automorphism groups obtained from the designs with these parameters would be a hopeless task. Thus, in view of its association with [3], and the novelty of the class of 46 designs with this parameter set obtained in [7] in what follows we examine the properties of the codes defined by the binary row span of the adjacency matrices of this class of designs. For that let $\mathfrak{D}_i$ where $1 \leq i \leq 46$ denote any of the 46 symmetric 2-(64, 28, 12) designs given in Result 1 (see also [7]). For each $\mathfrak{D}_i$ using Magma [1, 2] we constructed the corresponding codes (dual codes included). It has been established [7, Theorem 2, Theorem 6] that the 2-rank of a design $\mathfrak{D}_i$ is either 26 or 27 , see also Table 1. In Propositions 3 and 4, we examine the codes according to their dimensions and make some observations about their basic properties, in particular the minimum weight, the nature of the minimum words, and the structure of the automorphism groups.

Proposition 3 *If the 2-rank of $\mathfrak{D}_i$ is 26, then the minimum weight of C is 12, except for $i = 6$ when the minimum weight is 16. Furthermore, the minimum weight of $C^{\perp}$ is 8, in all cases.*

Proof: With the notation as in Lemma 2, we first show $d^{\perp} = 8$. Notice from Lemma 2(iii) that we need to show that $d^{\perp}$ is neither 4 nor 6. Suppose $d^{\perp} \in \{4, 6\}$, then by [12, Theorem 8.4] any 3 (resp. 5) columns of a parity check matrix H of $C^{\perp}$ are linearly independent, but some 4 (resp. 6) columns are linearly dependent. In each case we verified that this is not possible. Hence $d^{\perp} \geq 8$. Moreover, direct calculations for each code show that the weights of the rows of a generator matrix equals 8; thus $d^{\perp} \leq 8$, and the result follows. Now, we examine the minimum weight d of C. By Lemma 2(i) we have that C is doubly-even, so all codewords of C have weight divisible by four, so that $d \geq 4$. But $C \subseteq C^{\perp}$ excludes the possibility of weight 4 codewords in C and we have that $d \geq 8$. However, and once again the earlier argument of the parity check matrix shows that there are no codewords of weight 8 in C. Thus $d(C) = 12$. For the exceptional case when $i = 6$ we used Magma to ascertain the result. ■

Proposition 4 *If the 2-rank of $\mathfrak{D}_i$ is 27, then the minimum weight of C is 8, and the total number of codewords of minimum weight in C equals 1, unless $i = 23$, when there are 29 codewords of minimum weight. The minimum weight of $C^{\perp}$ is 8, unless $i = 8, 9$, in which cases the minimum weight is 4, or $i = 7, 10, 11$, for which the minimum weight is 6.*

Proof: We start by showing that $d^{\perp}$ is as stated. Suppose first that $i \in \{8, 9\}$. From Lemma 2(iii), observe that $d^{\perp} \geq 4$. Now, direct calculations for each case show that the weights of the rows of the generator matrix equals 4; thus $d^{\perp} \leq 4$, and so the result. Next consider $i \in \{7, 10, 11\}$. Recall that $d^{\perp} \geq 4$. Now, suppose that $d^{\perp} = 4$ and argue as follows to get a contradiction. Let p be a fixed point in the support S of a non-zero codeword $w \in C^{\perp}$ of weight $s = d^{\perp}$ and p_l be the number of blocks of the design $\mathfrak{D}$ passing through p and meeting S in l points. A counting argument gives

$$\sum_{l=1}^{k} p_l = r, \ \sum_{l=2}^{k}(l-1)p_l = (s-1)\lambda. \tag{1}$$

From Equation (1) we obtain

$$\sum_{l=3}^{k}(l-2)p_l = (s-1)\lambda - r, \tag{2}$$

and Equations (1) and (2) imply that $p_2 = r - \sum_{l=3}^{k} p_l \geq r - \sum_{l=3}^{k}(l-2)p_l = r - [(s-1)\lambda - r] = 2r - (s-1)\lambda$. Hence we have $p_2 \geq 56 - 36 = 20$ for any point of S. Now, consider the entries of w. Let $S = \{q_l \,|\, 1 \leq l \leq 4\}$. Notice that every block meeting S in two points and passing through q_1 must pass through another point, say q_4, but there are only three points remaining once q_1 is chosen; thus not all 20 blocks which meet S in two points can pass through q_4; thus we have a contradiction. So that $d \geq 6$. Since the weights of the rows of the generator matrix for $C^{\perp}$ equals 6, we obtain $d^{\perp} \leq 6$, and so the assertion follows. Finally, for $i \notin \{7, 8, 9, 10, 11\}$ we have from the earlier cases that $d^{\perp} > 6$, and since $C^{\perp}$ is single-even we obtain that $d^{\perp} \geq 8$. A judicious examination of the weights of the rows of the generator matrix in each case gives $d = 8$. ■

Lemma 5 *The automorphism group of C is isomorphic to either* Frob_{21}, $\mathrm{Frob}_{21} \times 2$, $\mathrm{Frob}_{21} \times D_8$, $\mathrm{Frob}_{42} \times 2$, $(\mathrm{Frob}_{42} \times 2){:}2$ *or* $(\mathrm{Frob}_{21} \times D_8){:}2$.

Proof: It follows from [7, Theorem 3, Theorem 5] that if $\mathfrak{D}$ is any of the 46 non-isomorphic 2-(64, 28, 12) designs whose codes are presented in Table 1, then $\mathrm{Aut}(\mathfrak{D})$ is $\mathrm{Frob}_{21}, \mathrm{Frob}_{21} \times 2$, $\mathrm{Frob}_{42} \times 2$ or $\mathrm{Frob}_{21} \times D_8$. Furthermore, since the rows of each $\mathfrak{D}$ span the code it is evident that $\mathrm{Aut}(\mathfrak{D}) \subseteq \mathrm{Aut}(C)$. In addition, computations with Magma (see Table 1 below) give $|\mathrm{Aut}(\mathfrak{D})| = |\mathrm{Aut}(C)|$ in all cases, except for $i \in \{41, 45, 46\}$. So we have that $\mathrm{Aut}(\mathfrak{D}) = \mathrm{Aut}(C)$. Now, consider $i \in \{41, 45, 46\}$. Notice first that in all cases $[\mathrm{Aut}(C) : \mathrm{Aut}(\mathfrak{D})] = 2$ so that $\mathrm{Aut}(C) = \mathrm{Aut}(\mathfrak{D}){\cdot}2$. In each case we use Magma to ascertain the claims of the lemma. For $i = 41$, computations with Magma show that $\mathrm{Aut}(C)$ contains two normal subgroups, say N and H of orders 21 and 2 respectively, such that $N \cong \mathrm{Frob}_{21}$ and $H \cong \mathbb{Z}_2$. Since $N \cap H = \{1_{\mathrm{Aut}(C)}\}$ and $|\mathrm{Aut}(C)| = |N \cdot H| = 42$ we deduce that $\mathrm{Aut}(C) \cong \mathrm{Frob}_{21} \times 2$ and the result follows. Finally, for $i = 45$ we have that $\mathrm{Aut}(C) \cong (\mathrm{Frob}_{42} \times 2){:}2$, and for $i = 46$ we obtain $\mathrm{Aut}(C) \cong (\mathrm{Frob}_{21} \times D_8){:}2$. ■

Since the all-one vector is always in the code (as the sum of the rows of the incidence matrix), the number of codewords of any weight w equals the number of words of weight $64-w$. Moreover, all weights are $\equiv 0 \pmod 4$. Therefore only weights up to 32 are listed. In Table 1 the first column represents the ordering of the code corresponding to a design (the codes are ordered according to their dimensions), the second column represents the dimension of the code, the third and fourth columns are the orders of the automorphism group of the design and of the code respectively, and the remaining columns list the number of codewords of a given weight w in C. In Table 1 we present only the representatives of classes of mutually equivalent codes. The sets of mutually equivalent codes that contain more than one code are $\{2,3\}$, $\{14,18,31,33\}$, $\{15,34\}$, $\{17,30\}$, $\{23,24\}$, $\{25,35\}$, $\{26,28,36,38\}$, $\{27,29,37,39\}$, $\{40,43,44\}$.

$\mathfrak{D}_i$	dim	$\lvert\mathrm{Aut}(\mathfrak{D}_i)\rvert$	$\lvert\mathrm{Aut}(C_i)\rvert$	0	8	12	16	20	24	28	32
1	26	21	21	1		98	6888	284858	3652880	16266468	26686478
2	26	21	21	1		77	7154	283465	3656968	16258922	26695690
4	26	21	21	1		63	7294	282835	3658648	16255982	26699218
5	26	21	21	1		112	6804	285040	3652768	16266272	26686870
6	26	21	21	1			7588	282688	3656800	16261568	26691574
7	26	21	21	1		7	7434	283675	3653608	16267742	26683930
8	26	21	21	1		7	7294	284795	3649688	16275582	26674130
9	26	21	21	1		77	7126	283689	3656184	16260490	26693730
10	26	42	42	1		7	7434	283675	3653608	16267742	26683930
11	26	42	42	1		98	7224	282170	3662288	16247652	26709998
12	26	84	84	1		21	7070	286097	3645656	16283226	26664722
13	26	168	168	1		105	6678	286293	3648120	16275778	2667491
14	27	21	21	1	1	161	13916	570381	7300951	32544850	53357206
15	27	21	21	1	1	168	14070	568904	7306383	32533776	53371122
16	27	21	21	1	1	168	14238	567560	7311087	32524368	53382882
17	27	21	21	1	1	140	14350	567644	7309743	32527896	53378178
19	27	21	21	1	1	217	13692	570213	7303639	32537794	53366614
20	27	21	21	1	1	210	15218	569002	7280735	32616068	53255258
21	27	21	21	1	1	217	18060	606949	7225230	32450882	53615030
22	27	21	21	1	1	238	18354	603862	7236831	32427068	53645018
23	27	21	21	1	29	658	14714	564970	7289667	32612484	53252682
25	27	21	21	1	1	126	14322	568358	7306719	32534364	53369946
26	27	21	21	1	1	28	14686	568876	7301231	32548280	53351522
27	27	21	21	1	1	35	14392	570983	7294119	32562294	53334078
32	27	21	21	1	1	168	14238	567560	7311087	32524368	53382882
40	27	42	42	1	1	112	14238	569520	7302127	32543968	53357794
41	27	21	42	1	1	14	14994	566902	7307615	32535932	53366810
42	27	21	21	1	1	28	14630	569324	7299663	32551416	53347602
45	27	84	168	1	1	42	14266	571746	7291711	32566900	53328394
46	27	168	336	1	1	210	13482	572138	7296639	32552004	53348778

Table 1: Weight distributions of the binary codes from (64, 28, 12) designs

Since $1 \in C$, it follows that C is also the code of the complementary 2-$(64, 36, 20)$ design. Moreover, since the codes with the same weight distribution were in all instances equivalent, we can thus state the following

Proposition 6 *The binary codes of the 46 non-isomorphic* $(64, 28, 12)$ *designs obtained in [7] can be distinguished by their automorphism groups or by the weight distributions. Up to equivalence there are 30 non-isomorphic binary self-orthogonal codes of length 64 obtained from these designs.*

Remark 1 The binary codes of the residual and derived designs are in all cases the even weight codes with parameters $[36, 25, 2]_2$ and $[28, 25, 2]_2$ respectively.

4 Binary codes from orbit matrices of the 2-$(64, 28, 12)$ designs

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a 2-(v, k, λ) design and $G \leq \mathrm{Aut}(\mathcal{D})$. We denote the G-orbits of points by $\mathcal{P}_1, \ldots, \mathcal{P}_n$, G-orbits of blocks by $\mathcal{B}_1, \ldots, \mathcal{B}_m$, and put $|\mathcal{P}_j| = \omega_j$, $|\mathcal{B}_i| = \Omega_i$, $1 \leq j \leq n$, $1 \leq i \leq m$. Further, we denote by γ_{ij} the number of points of $\mathcal{P}_j$ incident with a representative of the block orbit $\mathcal{B}_i$. For those numbers the following equalities hold (see [8]):

$$\sum_{j=1}^{n} \gamma_{ij} = k \tag{3}$$

$$\sum_{i=1}^{m} \frac{\Omega_i}{\omega_j} \gamma_{ij} \gamma_{is} = \lambda \omega_s + \delta_{js} \cdot (r - \lambda). \tag{4}$$

Definition 1 *A* $(m \times n)$*-matrix* $M = (\gamma_{ij})$ *with entries satisfying conditions* (3) *and* (4) *is called an orbit matrix for the parameters* (v, k, λ) *and orbit lengths distributions* $(\omega_1, \ldots, \omega_n)$, $(\Omega_1, \ldots, \Omega_m)$.

Orbit matrices are often used in the construction of designs with a presumed automorphism group. Construction of designs admitting an action of a presumed automorphism group consists of the two basic steps that follow (see [14]):

1. Construction of orbit matrices for the given automorphism group,
2. Construction of block designs for the orbit matrices obtained in this way. This step is often called an indexing of orbit matrices.

Remark 2 Note that given an orbit matrix M the rows and columns that correspond to non-fixed blocks and non-fixed points form a submatrix called the non-fixed part of the orbit matrix M.

The following theorem quoted from [9] which is a generalization of a result of Harada and Tonchev [11] gives a construction of self-orthogonal codes from the non-fixed parts of orbit matrices of symmetric 2-designs.

Result 2 *[9, Theorem 4] Let G be an automorphism group of a symmetric (v, k, λ) design $\mathcal{D}$. If G is a cyclic group of prime order p and $p|(r-\lambda)$, then the rows of the non-fixed part of the orbit matrix generate a self-orthogonal code of length $\frac{v-f}{p}$ over $\mathbb{F}_p$, where f is the number of fixed points.*

Note that in Result 2 the matrix M does not have to be an orbit matrix induced by an automorphism group, it suffices that M is an orbit matrix satisfying Definition 1. In what follows we determine self-orthogonal codes obtained from the non-fixed parts of the orbit matrices of 2-$(64, 28, 12)$ designs that satisfy Equations (3) and (4). This is regardless of whether or not these matrices are obtained from an action of a group on a design.

5 An automorphism of order 4 acting with 12 fixed points on 2-$(64, 28, 12)$ designs

The following result gives bounds for the number of fixed points of an automorphism of a symmetric design (see [16]).

Result 3 *Suppose that a nonidentity automorphism α of a nontrivial symmetric (v, k, λ) design fixes $f(\alpha)$ points. Then $f(\alpha) \leq v - 2n$ and $f(\alpha) \leq \frac{\lambda v}{k-\sqrt{n}}$. Moreover, if equality holds in either inequality, α must be an involution and every non-fixed block contains exactly λ fixed points.*

In the sequel, we apply Result 2 to classify self-orthogonal codes constructed from orbit matrices of the 2-$(64, 28, 12)$ designs in discussion and admitting $\mathbb{Z}_4$ as an automorphism. Solving Equations (3) and (4) we get up to isomorphism 368 orbit matrices for $\mathbb{Z}_4$ acting on a symmetric 2-$(64, 28, 12)$ design with twelve fixed points and thirteen orbits of order 4. Below we give a representative matrix as used in our computations to construct the codes. The block matrix in the bottom right part of this matrix constitutes the non-fixed part of the orbit matrix. The reader would have noticed that this forms a 13×13 matrix, hence the length of the codes examined in Theorem 7 below.

M	1	1	1	1	1	1	1	1	1	1	1	1	4	4	4	4	4	4	4	4	4	4	4	4	4
1	1	1	1	1	0	0	0	0	0	0	0	0	4	4	4	4	4	4	0	0	0	0	0	0	0
1	1	1	1	1	0	0	0	0	0	0	0	0	4	4	0	0	0	0	4	4	4	4	0	0	0
1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	4	4	0	0	4	4	0	0	4	4	0
1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	4	4	0	0	4	4	4	4	0
1	0	0	0	0	1	1	1	1	0	0	0	0	4	4	4	0	0	0	0	0	4	0	4	4	0
1	0	0	0	0	1	1	1	1	0	0	0	0	4	0	0	4	4	0	4	0	0	4	4	0	0
1	0	0	0	0	1	1	1	1	0	0	0	0	0	4	0	4	0	4	0	4	0	4	0	4	0
1	0	0	0	0	1	1	1	1	0	0	0	0	0	0	4	0	4	4	4	4	4	0	0	0	0
1	0	0	0	0	0	0	0	0	1	1	1	1	4	0	4	0	4	0	0	4	0	4	0	4	0
1	0	0	0	0	0	0	0	0	1	1	1	1	4	0	0	4	0	4	4	0	4	0	0	4	0
1	0	0	0	0	0	0	0	0	1	1	1	1	0	4	4	0	0	4	4	0	0	4	4	0	0
1	0	0	0	0	0	0	0	0	1	1	1	1	0	4	0	4	4	0	0	4	4	0	4	0	0
4	1	1	0	0	1	1	0	0	1	1	0	0	2	2	1	1	2	2	2	2	1	1	2	2	2
4	1	1	0	0	1	0	1	0	0	0	1	1	2	1	2	2	1	2	1	2	2	2	2	1	2
4	1	0	1	0	1	0	0	1	1	0	1	0	1	2	2	2	2	1	2	1	2	2	1	2	2
4	1	0	1	0	0	1	1	0	0	1	0	1	1	2	2	2	1	2	2	1	2	2	1	2	2
4	1	0	0	1	0	1	0	1	1	0	0	1	2	1	2	1	2	2	1	2	2	2	2	1	2
4	1	0	0	1	0	0	1	1	0	1	1	0	2	2	1	2	2	1	2	2	1	1	2	2	2
4	0	1	1	0	0	1	0	1	0	1	1	0	2	1	2	2	1	2	1	2	2	2	2	1	2
4	0	1	1	0	0	0	1	1	1	0	0	1	2	2	1	1	2	2	2	2	1	1	2	2	2
4	0	1	0	1	1	0	0	1	0	1	0	1	1	2	2	2	2	1	2	1	2	2	1	2	2
4	0	1	0	1	0	1	1	0	1	0	1	0	1	2	2	2	2	1	2	1	2	2	1	2	2
4	0	0	1	1	1	1	0	0	0	0	1	1	2	2	1	1	2	2	2	2	1	1	2	2	2
4	0	0	1	1	1	0	1	0	1	1	0	0	2	1	2	2	1	2	1	2	2	2	2	1	2
4	0	0	0	0	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2	2	2	4

The non-fixed parts of the orbit matrices span up to equivalence a unique class of binary self-orthogonal doubly-even codes of length 13. A representative of this class is given by a code with parameters $[13,3,4]_2$ and weight enumerator $A(x) = 1 + 3x^4 + 3x^8 + x^{12}$. The automorphism group of this code has order 82944 and is of shape $[(D_8 \times D_8){:}2] \times D_8{:}(3^3{:}3)$.

We thus have the following

Theorem 7 *Let M be any of the 368 orbit matrices for the symmetric* 2-$(64, 28, 12)$ *designs under an action of an automorphism of order 4 with twelve fixed points. The non-fixed parts of M span up to equivalence a single class of binary self-orthogonal doubly-even* $[13,3,4]_2$ *codes of length 13. Moreover, the subcodes of codimension 1 spanned by codewords of weight 8 are optimal doubly-even* $[13,2,8]_2$ *codes with weight enumerator* $A(x) = 1 + 3x^8$.

References

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp.*, 24, 3/4:235–265, 1997.

[2] J. Cannon, A. Steel, and G. White. Linear codes over finite fields. In J. Cannon and W. Bosma, editors, *Handbook of Magma Functions*, pages 3951–4023. Computational Algebra Group, Department of Mathematics, University of Sydney, 2008. V2.15, http://magma.maths.usyd.edu.au/magma.

[3] L. Chikamai, J. Moori and B. G. Rodrigues. 2-modular representations of the alternating group A_8 as binary codes. *Glas. Mat. Ser. III.* **47**(67) (2012), no 2, 225 - 252.

[4] L. Chikamai. *Linear codes obtained from 2-modular representations of some finite simple groups*, PhD thesis, University of KwaZulu-Natal, Durban, 2013.

[5] A. R. Calderbank and P. Frankl. Binary codes and quasi-symmetric designs. *Discrete Math,* **83** (1990), 201–204.

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

[7] D. Crnković and M. O. Pavčević. Some new designs with parameters $(64, 28, 12)$. *Discrete Math,* **237** (2001), 109–118.

[8] D. Crnković, S. Rukavina. Construction of block designs admitting an abelian automorphism group. *Metrika.*, 62, no. 2-3 (2005), 175–183.

[9] D. Crnković, B. G. Rodrigues, S. Rukavina and L. Simčić. Ternary codes from the strongly regular $(45, 12, 3, 3)$ graphs and orbit matrices of 2-$(45, 12, 3)$ designs. *Discrete Math,* **312** (2012), 3000–3010.

[10] Y. Ding, S. Houghten, C. Lam, S. Smith, L. Thiel and V D Tonchev. Quasi-symmetric 2-$(28, 12, 11)$ designs with an automorphism of order 7. *J. Combin. Des.*, **6** (3) (1998), 213–223.

[11] M. Harada and V. D. Tonchev. Self-orthogonal codes from symmetric designs with fixed-point-free automorphisms. *Discrete Math.*, **264** (2003), no. 1-3, 81–90.

[12] R. Hill. *A First Course in Coding Theory.* Oxford Applied Mathematics and Computing Science Series. Oxford: Oxford University Press, 1986.

[13] W. C. Huffman. Automorphisms of codes with application to extremal doubly-even codes of lenght 48. *IEEE Trans. Inform. Theory,* **28** (1982), no. 3, 511–521.

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

[15] D. Jungnickel and V. D. Tonchev. On symmetric and quasi-symmetric designs with the symmetric difference property and their codes. *J. Combin. Theory Ser. A.* **59** (1992), no. 1, 40–50.

[16] E. Lander. *Symmetric Designs: An Algebraic Approach*, Cambridge University Press, Cambridge, 1983.

[17] R. Mathon and A. Rosa. 2-(v, k, λ) *designs of small order*, in: Handbook of Combinatorial Designs, 2^{nd} ed. (C.J. Colbourn and J.H. Dinitz, Eds.), Chapman and Hall/CRC, Boca Raton, 2007, 25–58.

[18] G. McGuire and H. N. Ward. Characterization of certain minimal rank designs. *J. Combin. Theory Ser. A.* **83** (1998), 42–56.

[19] C. Parker, E. Spence and V. D. Tonchev. Designs with the symmetric difference property on 64 points and their groups. *J. Combin. Theory Ser. A.* **67** (1994), 23–43.

[20] V. D. Tonchev. *Codes*, in: Handbook of Combinatorial Designs, 2^{nd} ed. (C. J. Colbourn and J. H. Dinitz, Eds.), Chapman and Hall/CRC, Boca Raton, 2007, 667–702.