*International Journal of Engineering and Mathematical Sciences*
*July – Dec. 2018, Volume 14, Issue – 1, pp.10 – 23.*
*ISSN (Print) – 2319 - 4537, (Online) – 2319 - 4545.*


IJEMS

# Binary Codes from the Projective Symplectic Group $S_8(2)$

***Lydiah Rukaria[1], Lucy Chikamai[2], Ireri Kamuti[3]***
***[1, 2, 3]Mathematics Department***
***[1, 2]Kibabii University***
***[3] Kenyatta University***
***[1, 2] P. O. Box 1699-50200, Bungoma Kenya***
***[3] P. O. Box 43844- 00100, Nairobi Kenya***
***lydiahrukaria@gmail.com[1], lucychikamai@gmail.com[2], kamuti.ireri@ku.ac.ke[3]***

## Abstract

We find all of the binary codes constructed from the primitive permutation representation of the projective symplectic group $S_8(2)$of degree 255. It is shown that in total we have 76 non - trivial and non - isomorphic codes. The properties of the codes with small dimension are given and links with modular representation theory established. Further from the support of the codewords, we construct the 1 and 2 - designs associated to the code and the graphs of the designs.

**Keywords:** Code, group Design, Graph, Automorphism, projective Symplectic group.

## Introduction

Let G be a permutation group, $\Omega$ a finite set and $\mathbb{F}$ a field. The vector space over $\mathbb{F}$ with basis $\Omega$ is considered as an $\mathbb{F}G$ - module. It is often of considerable interest to consider the structure of the permutation module $\mathbb{F}\Omega$ . The G - invariant submodules of $\mathbb{F}\Omega$ can be regarded as linear codes in $\mathbb{F}\Omega$ and one may therefore ask for the weight distribution and the partioning of the code into G - orbits. To a greater extent, this paper fits into a programme outlined in [13], in that we determine binary codes invariant under a prescribed permutation group. In this paper, using a modular representation theoretic approach, we construct from the primitive permutation representation of degree 255 of the simple projective symplectic group $S_8(2)$ irreducible submodules of the permutation module $\mathbb{F}\Omega$ . In the theorem given below, we summarize our results. The specific results relating to the codes and designs held by the supports of the codewords are given as propositions in the sections that follow.

## Theorem 1.1

Let G be the simple projective symplectic group$S_8(2)$. In its natural action as a primitive rank 3 group of degree 255 on the points of the projective space PG(7, 2), a permutation module of dimension 255 invariant under G is formed. The permutation module splits into 80 submodules of which we obtain 76 non - trivial and non isomorphic binary linear codes. Let $\mathcal{D}_{w_m}$be the design held by orbiting the codewords of weight $w_m$ under G in the code $C_{255,r}$.Let M = {127, 128} and N= {119, 120, 136, 137}. Then,

i) The codes [255, 8, 128] and [255, 9, 127] are optimal codes.

ii) The codes [255, 8, 128] and [255, 9, 120] are doubly even and self orthogonal.

iii) The codes [255, 8, 128] and [255, 9, 119] are projective codes whose duals are 1 error correcting codes.

iv) The automorphism group of the codes [255, 8, 128] and [255, 9, 127] is the group $L_8(2)$ and the automorphism group of the codes [255, 9, 119], [255, 9, 120] and [255, 10, 119] is $S_8(2)$.

v) For $m \in M$ the automorphism group of the 1 - design $\mathcal{D}_{w_m}$ is $L_8(2)$.

vi) For $m \in M$ the automorphism group of the 2 – design $\mathcal{D}_{w_m}$ is $L_8(2)$.

vii) For $m \in N$ the automorphism group of the 1 - design $\mathcal{D}_{w_m}$ is $S_8(2)$.

viii) The minimum weight of the code $C_{255,r}$ for i = 1, 2, . . , 5 is the block size of the geometrical 1 – design. Thus a basis of minimum words exists.

The paper is organized as follows: in section 2 we outline our background and notations. In section 3 we describe the methodology applied for obtaining the binary codes. In section 4 we give a brief but complete overview description of the projective symplectic group $S_8(2)$. In section 5 we describe the codes of small dimension of the representation of degree 255. In section 6 we describe the designs held by the codes obtained in section 5 and their respective graphs in section 7.

## Terminology and Notations

We assume that the reader is familiar with some basic notions and elementary facts from design, coding and graph theory. Our notation for groups and codes is standard and it is as in [6] and ATLAS [2]. For the structure of groups and their maximal subgroups we follow the ATLAS [2]. The group G.H, G·Hand G:H denote a general extension, a non- split extension and a split extension respectively. Given a prime p, the symbol pr denotes an abelian group of that order. If G is finite group acting on a finite set Ω, the set $\mathbb{F}_q\Omega$, is the vector space o $\mathbb{F}_q$verwith basis Ω is called an $\mathbb{F}_q$G permutation module if the action of G is extended linearly on Ω. An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$with point set $\mathcal{P}$, block set $\mathcal{B}$and incidence $\mathcal{I} = \mathcal{P} \times \mathcal{B}$ is a t – (v, k, λ) design if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with the k points and every t distinct points in $\mathcal{P}$are together incident with λ blocks. The design $\mathcal{D}$is symmetric if it has the same number of points and blocks. 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 of the design $\mathcal{D}$ over a finite field $\mathbb{F}$ is the space spanned by the incidence vectors of the blocks over $\mathbb{F}_q$. The weight enumerator of C is defined as $\sum_{c\in C} x^{wt(c)}$. If a linear code C over a field of order q is of length n, dimension k and minimum distance d, then we say C is a [n, k, d] q – ary code. The dual or orthogonal code $C^{\perp}$ is the orthogonal under the standard inner product.A code C is self orthogonal if $C \subset C^{\perp}$ and self dual if $C = C^{\perp}$. The hull of a code is the intersection of C and $C^{\perp}$. If $u \in C$ is a codeword, then the support of u is the set of non – zero coordinate positions of u. A two – weight code C is a code which has exactly two non – zero weights. The dual of a two – weight code belongs to the important family of uniformly packed codes. The all one vector will be denoted by 1. It is a constant vector of weight equal to the length of the code whose coordinate entries consist of entirely 1's. A binary code is doubly even if all its code words have weight divisible by four. Two linear codes are isomorphic if they can be obtained from one another by permuting the coordinate positions. An automorphism of a code is any permutation of the coordinate positions that maps code words to code words and is denoted by Aut (C).

Terminology for graphs is standard and our graphs are undirected. The valency of a vertex is the number of edges incident with the vertex, the girth of a graph is the number of edges in the smallest cycle of the graph and the diameter of a graph is the length of the longest path in the graph. In a regular graph, all the vertices have the same valence. A regular graph is strongly regular of type $n, k, \lambda, \mu$ if it has n vertices, valence k, and if any two adjacent vertices are together adjacent to $\lambda$ vertices, while any two non adjacent vertices are together adjacent to $\mu$vertices.

## Preliminary Results

Our interest is to find all the G - invariant codes from the primitive permutation representation of degree 255. In so doing we consider the permutation module obtained from the action of the group on the cosets of its maximal sub modules. Given a permutation group G acting on a set $\Omega$, over a finite field$\mathbb{F}$, the vector space over $\mathbb{F}$ with basis $\Omega$ is considered as an $\mathbb{F}G-$ module. The G - invariant sub modules of $\mathbb{F}\Omega$ are the linear codes in $\mathbb{F}\Omega$. This approach provides the determination of all binary codes invariant under a given group G more directly since we obtain an explicit basis of the code. We have developed a series of computer programs in MAGMA to search for modules under the group and also used the recursive searches in MEAT-AXE to help determine the irreducibility of the module, subsequently obtaining a chain of maximal sub modules which constitute the binary codes invariant under G. An in-depth use of the database of irreducible faithful representations available in MAGMA and Wilson's webpage together with the Brauer character tables and the ATLAS of finite groups is widely used. Once the isomorphic copies are eliminated, a lattice of sub modules is obtained. This in a way answers to the problem of enumeration and classification.

Given a representation $\vartheta : G \to GL(n, \mathbb{F})$, $V = \mathbb{F}^n$ is converted into an $\mathbb{F}G$ – module by

$\left(\sum_{g \in G} \alpha_g g\right).v := \sum_{g \in G} \alpha_g g\,\vartheta(g)(v),\ v \in V$[29]

From the definition of linear codes as subspaces of $\mathbb{F}^n$ for a finite field $\mathbb{F}$, it follows that linear codes are simply $\mathbb{F}G-$ submodules. Hence for any permutation group G, the G – invariant codes are exactly the $\mathbb{F}G-$ submodules of $\mathbb{F}^n$. For a field$\mathbb{F}$, the representations of G correspond to the finite dimensional $\mathbb{F}G-$ modules.

Lemma 3.1 [9, 16]

Let G be a finite group and $\Omega$ a finite G – set. Then the FG – sub modules of $\mathbb{F}\,\Omega$ are the G – invariant codes. That is, the G – invariant subspaces of $\mathbb{F}\,\Omega$.

In this paper, we have used lemma 3.1 to construct codes and associated combinatorial structures for the representations of degree 255.

## The Projective Symplectic Group

The linear, unitary, symplectic and orthogonal groups generalize the familiar classical groups, whose description involves heavy use of the properties of finite fields. The general linear group $GL_n(q)$ is made up of all the $n \times n$ matrices with entries in $F_q$ that have non-zero determinant. $GL_n(q)$is the group of all linear automorphisms of an n dimensional vector space over $F_q$. The special linear group $SL_n(q)$ is the subgroup of all $n \times n$ matrices with determinant 1.For an even number the symplectic group $Sp_{2n}(q)$ is defined as the group of all elements of $GL_n(q)$ that preserve a nonsingular form

f(x,y). Any such matrix has determinant 1 so that the general and the special symplectic groups coincide.

Let $J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$. The symplectic group of rank n over F is defined to be; $Sp_n(q) = \{g \in M_{2n}(F) : g^t Jg = J\}$. It is evident that $Sp_{2n}(q)$ is a subgroup of $GL_{2n}(q)$. Given that m = 2n, the projective symplectic group of order m in a finite field $\mathbb{F}_q$ is denoted by $S_m(q)$, which is the standard ATLAS notation. This is the notation used throughout this work.

Let G be the projective symplectic group$S_8(2)$. The order of G is $47377612800 = 2^{16}.3^5.5^2.7.17$. Using ATLAS G has 11 distinct primitive representations of degree 120, 136, 255, 2295, 5355, 5440, 11475, 13056, 24192, 45696 and 19353600.

The representations and orbit lengths of G are shown in Table 1. The first column gives the maximal subgroups as given by the ATLAS [2], the second column shows the degree (the number of cosets of the point stabilizer), the third indicates the number of orbits and the last column gives the size of the orbits of the point stabilizer.

**Maximal subgroups of $S_8(2)$**

| Maximal subgroups | Degree | Number | Orbit Lengths |
|---|---|---|---|
| $O_8^-(2):2$ | 120 | 2 | 1, 119 |
| $O_8^+(2):2$ | 136 | 2 | 1, 135 |
| $2^7:S_6(2)$ | 255 | 3 | 1, 126, 128 |
| $2^{10}:A_8$ | 2295 | 5 | 1, 30, 280, 960, 1024 |
| $2^{3+8}:(S_3 \times S_6)$ | 5355 | 6 | 1, 90, 96, 240, 2048, 2880 |
| $S_3 \times S_6(2)$ | 5440 | 5 | 1, 189, 336, 1890, 3024 |
| $2^{6+6}:(S_3 \times L_3(2))$ | 11475 | 7 | 1, 42, 56, 896, 1008, 4096, 5376 |
| $S_{10}$ | 13065 | 5 | 1, 210, 1575, 5600, 5670 |
| $S_4(4):2$ | 24192 | 8 | 1, 85, 136, 850, 1360, 3400, 8160, 10200 |
| $(S_6 \times S_6):2$ | 45696 | 9 | 1, 200, 225, 1350, 3600, 3600, 4320, 16200, 16200 |

Table 1 Maximal subgroups of $S_8(2)$ of degree $\leq 45696$

## The Codes

The stabilizer of a point of the action of $S_8(2)$ on the set of points of the projective space PG (7, 2) is the group $2^7:S_6(2)$ which is maximal in G. The elements being permuted by G are points of the projective space PG (7, 2). We get a permutation representation of degree 255. From table 1, $S_8(2)$ acts primitively as a rank - 3 group of degree 255 on the cosets of $2^7:S_6(2)$with orbits of lengths 1, 126 and 128. By lemma 3.1 we form a permutation module of dimension 255 invariant under G and its subsequent sub modules. The permutation module splits into absolutely irreducible constituents of dimension 1, 8, 16, 26 and 48 with multiplicities 7, 4, 1, 4 and 2 respectively. Working recursively and

filtering out isomorphic copies of maximal sub modules, we find that the permutation module has a total of 80 sub modules of dimensions 0, 1, 8, 9, 10, 35, 36, 37, 44, 45, 84, 85, 86, 92, 93, 94, 118, 119, 120, 121, 134, 135, 136, 137, 161, 162, 163, 169, 170, 171, 210, 211, 218, 219, 220, 245, 246, 247, 254 and 255. The lattice of the sub modules is shown in figure 1. From this we obtain in total 76 non - trivial binary codes of length 255 whose dimensions are 8, 9, 10, 35, 36, 37, 44, 45, 84, 85, 86, 92, 93, 94, 118, 119, 120, 121, 134, 135, 136, 137, 161, 162, 163, 169, 170, 171, 210, 211, 218, 219, 220, 245, 246 and 247 summarized in table 2.

| Dimension | # | Dimension | # | Dimension | # |
|---|---|---|---|---|---|
| 8 | 1 | 93 | 3 | 163 | 1 |
| 9 | 3 | 94 | 1 | 169 | 1 |
| 10 | 1 | 118 | 1 | 170 | 3 |
| 35 | 1 | 119 | 7 | 171 | 1 |
| 36 | 3 | 120 | 7 | 210 | 1 |
| 37 | 1 | 121 | 1 | 211 | 1 |
| 44 | 1 | 134 | 1 | 218 | 1 |
| 45 | 1 | 135 | 7 | 219 | 3 |
| 84 | 1 | 136 | 7 | 220 | 1 |
| 85 | 3 | 137 | 1 | 245 | 1 |
| 86 | 1 | 161 | 1 | 246 | 3 |
| 92 | 1 | 162 | 3 | 247 | 1 |

Table 2: Dimensions of the 76 non – trivial and non – isomorphic codes

### The Binary linear codes $C_{255,i}$

The permutation module breaks into 80 sub modules which gives us 76 non-trivial and non – isomorphic codes whose dimensions are shown in the table 2.

| Code | Parameters | Dual Code Parameters |
|---|---|---|
| $C_{255,1}$ | $[255, 8, 128]_2$ | $[255, 247, 3]_2$ |
| $C_{255,2}$ | $[255, 9, 119]_2$ | $[255, 246, 3]_2$ |
| $C_{255,3}$ | $[255, 9, 127]_2$ | $[255, 246, 4]_2$ |
| $C_{255,4}$ | $[255, 9, 120]_2$ | $[255, 246, 3]_2$ |
| $C_{255,5}$ | $[255, 10, 119]_2$ | $[255, 245, 4]_2$ |

Table 3: Parameters of codes with small dimension in the 255 representation

For any permutation representations of degree n, we denote the constructed codes by $C_{n,1}, C_{n,2}, \dots, C_{n,r}$ if r codes are obtained and by $C_n$ if we only have one code up to isomorphism.

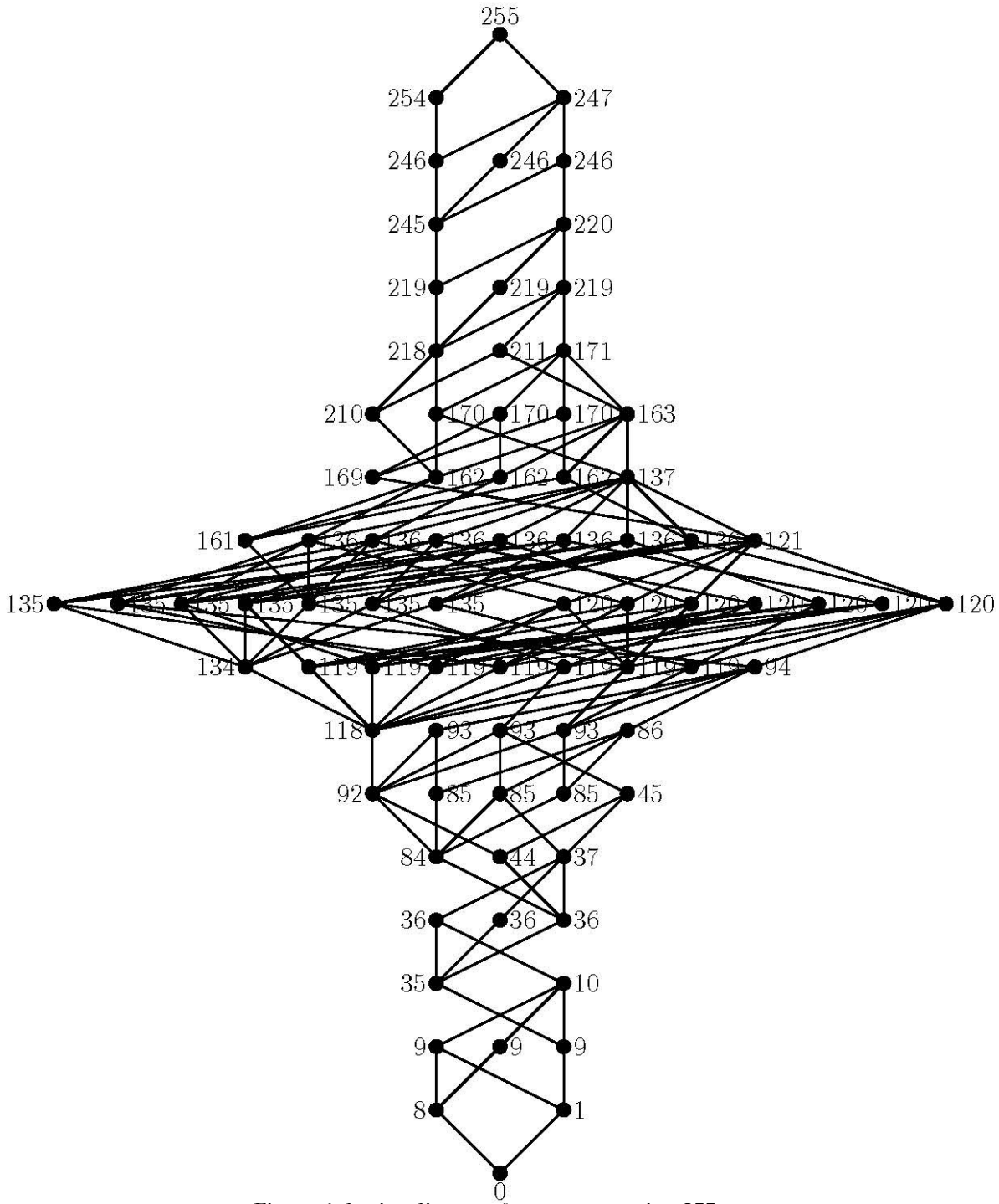


Figure 1: lattice diagram for representation 255

In this section we discuss the first five codes with small dimension shown in the table 3. Due to computational limitations, we could only get the weight distribution of the 5 codes.The weight distribution is shown in table 4.

| Nane | Dim | 0 | 119 | 120 | 127 | 128 | 135 | 136 | 255 |
|---|---|---|---|---|---|---|---|---|---|
| $C_{255,1}$ | 8 | 1 | | | | 255 | | | |
| $C_{255,2}$ | 9 | 1 | | 136 | | 255 | | | |
| $C_{255,3}$ | 9 | 1 | 120 | 136 | | 255 | 136 | 120 | |
| $C_{255,4}$ | 9 | 1 | | | 255 | 255 | | | 1 |
| $C_{255,5}$ | 10 | 1 | 120 | 136 | 255 | 255 | 136 | 120 | 1 |

Table 4: Weight distribution of some codes

**Proposition 6.1**

Let G be a permutation module of degree 255 with an irreducible submodule of dimension 8. Then the *following hold:*

i) The code $\mathrm{C}_{255,1}$ is a $[255, 8, 128]_2$ optimal, self orthogonal, doubly even and projective code. Its dual $\mathrm{C}_{255,1}^{\perp}$ is a $[255, 247, 3]_2$ code.
ii) $\mathrm{Aut}(\mathrm{C}_{255,1}) = \mathrm{L}_8(2)$

**Proof**

i) Computations by MAGMA shows the hull of $C_{255,1}$ has dimension 8 which is precisely the dimension of the code. This implies that $C \subset C^{\perp}$ this shows that the code is self orthogonal. The code $C_{255,1}$ is a one weight code whose weight enumerator is$1 + 255x^{128}$. Since $128 \equiv 0\ mod\ 4$, the code is clearly doubly even. $C^{\perp}$has minimum weight 3, therefore the code is projective. The optimality of the code is given by MAGMA and also from Grassl online tables.

ii) The code $C_{255,1}$ is spanned by its minimum weight codewords and these form the blocks of a symmetric $1-(255, 128, 128)$ design, we have that $Aut(D) \leq Aut\,(C_{255,1})$. By the fundamental theorem of projective geometry, the automorphism group of D is $P\Gamma L_8(2)$ and the order $|Aut(D)| = 2^{28}.3^5.5^2.7^2.17.31.127 = |Aut\,(C_{255,1})|$. Therefore $Aut\,(C_{255,1})$ = $P\Gamma L_8(2)$. Let $\bar{G}$ be the automorphism group of the code. By construction, all codes have $S_8(2) \leq \bar{G}$. The composition series for $\bar{G}$ found using MAGMA is $1_{\bar{G}} \trianglelefteq N \trianglelefteq \bar{G}$which is actually a chief series for $\bar{G}$. Hence N is a non abelian chief factor of $\bar{G}$. The order of N is the same as the$|L_8(2)|$. Therefore$N \cong L_8(2)$. Hence the automorphism group of the code $C_{255,1}$ is $L_8(2)$.

**Remarks**

i) The codewords with minimum weight in $C_{255,1}$ represent the points in the projective space PG (7, 2). The stabilizer of a point of the action of G on the points of the projective space is a group isomorphic to the group $2^7{:}S_6(2)$with index 255.
ii) The code$C_{255,1}$ has 255 codewords with minimum weight. Since $C_{255,1}$ is a [255, 8, 128] code, the words of minimum weight generate the code.

**Proposition 6.2** The code $\mathrm{C}_{255,2}$ is a $[255, 9, 119]_2$ projectivecode. The dual code $\mathrm{C}_{255.2}^{\perp}$ is a $|255, 246, 3|_2$ code. The automorphism group of the code $\mathrm{C}_{255,2}$ is $\mathrm{S}_8(2)$.

**Proof**

Let $\bar{G}$ be the automorphism group of the code. $\bar{G}$ is of order $2^{16}.3^5.5^2.7.17$.. The composition series for $\bar{G}$ found using MAGMA is $1_{\bar{G}} \trianglelefteq N \trianglelefteq \bar{G}$which is actually a chief series for $\bar{G}$. Hence N is a non abelian chief factor of $\bar{G}$. The order of N is the same as the$|S_8(2)|$. Therefore $N \cong S_8(2)$. Hence the automorphism group of the code $C_{255,2}$ is $S_8(2)$.

**Remarks**

i) Given a linear code of length 255 and dimension 9, the best known linear code upper boundary with these parameters has minimum distance 127 and lower boundary minimum distance 127. Therefore from MAGMA the code $C_{255,2}$ is a new code.
ii) The weight enumerator of $C_{255,2}$ is $1 + 120x^{119} + 255x^{128} + 136x^{135}$.Thus$C_{255,2}$, has 120 codewords with minimum weight while its dual has 5440 code words with minimum weight. The group $G = S_8(2)$ acts on the cosets of $O_8^-(2):2$ with orbits of length 1 and 119. From table 4.1 and the ATLAS, the elements being permuted by G are copies of $O_8^-(2)$. The number of codewords with minimum weight for the code $C_{255,2}$ is equal to the number of cosets of the point stabilizer for this group action. The dual code $C_{255.2}^{\perp}$ has 5440 codewords with minimum weight. The group $G = S_8(2)$ acts on the cosets of $S_3 \times S_6(2)$ with orbits of length 1,189, 336, 1890 and 3024. From ATLAS, the elements being permuted by G are the non isotropic lines. The number of codewords with minimum weight for the dual code $C_{255.2}^{\perp}$ is equal to the number of cosets of the point stabilizer for this group action.

**Proposition 6.3**

The code $C_{255,3}$ is a $[255, 9, 127]_2$ optimal projective code and its dual $C_{255,3}^{\perp}$ is a $[255, 246, 4]_2$ even and projective code. The automorphism group of the code $C_{255,3}$ is $L_8(2)$.

**Proof**

The optimality of the code is given by MAGMA and also from Grassl online tables. The code and its dual have minimum weights greater than 3, hence projective. Let $\bar{G}$ be the automorphism group of the code. $\bar{G}$ is of order $2^{28}.3^5.5^2.7^2.17.31.127$. The composition series for $\bar{G}$ found using MAGMA is $1_{\bar{G}} \trianglelefteq N \trianglelefteq \bar{G}$which is actually a chief series for $\bar{G}$. Hence N is a non abelian chief factor of $\bar{G}$. The order of N is the same as the$|L_8(2)|$. Therefore $N \cong L_8(2)$. Hence the automorphism group of the code $C_{255,3}$ is $L_8(2)$. From MAGMA, all the weights of the codewords of the dual code are of even weight, and therefore the dual is even.

**Remark**

The weight enumerator of the code $C_{255,3}$ is $1 + 255x^{127} + 255x^{128} + x^{255}$ and has 255 code words with minimum weight. The number of codewords with minimum weight is precisely the number of points in the projective space PG (7, 2). $G = S_8(2)$ acts primitively on the points of PG (7,2).

**Proposition 6.4**

The code $C_{255,4}$ is a $[255, 9, 120]_2$ self orthogonal, doubly even and projective code and its dual $C_{255,4}^{\perp}$ is a $[255, 246, 3]_2$ code. The automorphism group of the code $C_{255,4}$ is $S_8(2)$.

**Proof**

The weight enumerator for the code $C_{255,4}$ is $1 + 136x^{120} + 255x^{128} + 120x^{136}$. Clearly all the weights of the code words are congruent to $0 \equiv \text{mod } 4$. Hence the code is doubly even and self orthogonal.The proof of the automorphism is exactly as it is in the proof of proposition 6.2.2.

**Remark**

The code $C_{255,4}$ has 136 codewords with minimum weight. The codewords of minimum weight represent copies of $O_8^+(2)$ , which is the plus hyper plane in the orthogonal space. The dual code $C_{255.2}^{\perp}$ has 5355 codewords with minimum weight. The group $G = S_8(2)$ acts on the cosets of $2^{3+8}{:}(S_3 \times S_6)$ with orbits of length 1, 90, 96, 240, 2048, 2880. From ATLAS, the elements being permuted by G are the 10795 isotropic lines of PG (7, 2). The number of codewords with minimum weight for the dual code $C_{255.2}^{\perp}$ is equal to the number of cosets of the point stabilizer for this group action.

**Proposition 6.5**

The code $C_{255,5}$ is a $[255, 10, 119]_2$ code. The dual $C_{255,5}^{\perp}$ is a $[255, 245, 4]_2$ code. The automorphism group of the code $C_{255,5}$ is $S_8(2)$.

**Proof**

Similar arguments as in the proof of proposition 6.2.2 can apply here.

**Remarks**

The code $C_{255,5}$ has 120 codewords with minimum weight. The weight enumerator for the code $C_{255,5}$ is$1 + 120x^{119} + 136x^{120} + 255x^{127} + 255x^{128} + 136x^{135} + 120x^{136} + x^{255}$. The codewords with minimum weight represent copies of $O_8^-(2)$ which is the affine hyperplane in the orthogonal space. The code words with weight 120 and 135 represent copies of $O_8^+(2)$which is the quadratic form hyper plane in the orthogonal space. The codewords with weight 127 and 128 represent the points in the projective space PG (2, 7).

**Designs**

Coding theory has been used to extend designs. In [16] Kennedy extended designs held by vectors of a code. A binary vector u of weight w is said to determine a block of w points corresponding to the support of u. In this case, we say that the vectors of a fixed weight w in a binary code of length n, hold a t – design if the blocks determined by these vectors are the t blocks of a t – design on n points [15]. This means that every set of t coordinate positions occurs as non- zero positions for exactly λ vectors of weight w. The knowledge of the number of vectors of each weight existing in a code is vital in the determination of whether or not the supports of these vectors could form a design. For the Galois field $\mathbb{F}_2$, the supports are in a one to one correspondence with the code words. The Assmus – Mattson theorem establishes the connection between codes and designs, in that codes of certain weight in a $q-$ary code hold a design and that we can determine the number of codes of such weight [22]. The theorem provides conditions on the weight enumerators of a code and its dual that are sufficient to

ensure that support of the minimum weight codes and other codes, yield a t – design, where t is a positive integer less than the minimum weight.

Most designs arise as supports of codewords of a given weight in a code.

We denote the designs by $D_{255,i}\ for\ i = 1,2,\dots,5$ associated with the code $C_{255,i}$ in the same range. Let W be a set of codewords of non – zero weight in $C_{255,i}\ where\ i = 1, 2, \dots, 5$. From the weight distributions of the five codes, we found all the 1 - designs held by the supports of the codewords and also the 2 - designs in cases where they existed.

**Designs held by the support of the codewords in $C_{255,i}$ for i = 1, 2, . . . , 5**

Let $w_m$ be a codeword of non – zero weight in $C_{255,1}$ fori= 1, 2,. . . , 5. We determine the structure of the stabilizer of $w_m$inAut(C), denoted by $\mathrm{Aut}(C)_{w_m}$ and form the designs $D_{w_m}$ from the orbits. We examine the action of $\mathrm{Aut}(C) = L_8(2)$or $\mathrm{Aut}(C) = S_8(2)$on the set $W_m$ of non trivial codewords of C and describe their nature. Let M = {119, 120, 127, 128, 135, 136}, for codes $C_{255,i}$and fori $= 1, 2, \dots, 5$. For $m \in M$we define $W_m = \{w_m \in C_{255,i\,|wt\,(w_m)=m}\}$. For $w_m \in W_m$, we take the image of the support of $w_m$ under the action of $G = S_8(2)$or $G = L_8(2)$ to form the blocks of the $t-(255, m, k_m)$designs $\mathcal{D} = \mathcal{D}_{w_m}$where $k_m = |(w_m)^G| \times \frac{m}{255}$and show that Aut (C ) acts primitively on$\mathcal{D}_{w_m}$. In lemma 7.1, we show that for all $m \in M$, the stabilizer $\mathrm{Aut}(C)_{w_m}$where $H < \mathrm{Aut}(C)$is a maximal subgroup of Aut (C ).

**Lemma 7.1**

*Let $C_{255,1}$ for i= 1, 2,. . . , 5.and $0 \neq w \in C$. Then $Aut\,(C)_w$ is a maximal subgroup of Aut (C). Also, the design D obtained by orbiting the images of the support of any non – trivial codeword in C is primitive.*

**Proof :** All the codes $C_{255,i}$ for i= 1, 2,. . . , 5.have either $S_8(2)$ or $L_8(2)$ as the automorphism group. We consider the action of these two groups on the codewords of weight $m \in M$ separately.

**Case I:** Suppose $\mathrm{Aut}(C) = S_8(2)$which we denote by$\overline{G}$. Let C be the codes $C_{255,i}$ for i= 2, 4, 5 and M = {119, 120, 127, 128, 135, 136}. In all cases of $m \in M$, $W_m$ is invariant under the action of G. Therefore each $W_m$ is a single orbit under this action and so $\overline{G}$is transitive on each $W_m$. By the orbit stabilizer theorem, we conclude that$|\overline{G}: \overline{G}_{w_m}| \in$ {119,120,128,135,136}. From table 1 the table of maximal subgroups of$S_8(2)$, $(S_8(2))_{w_m} \in \{O_8^-(2):2,\ O_8^+(2):2,\ 2^7:S_6(2)\}$. Since $S_8(2)$ is transitive on the code coordinates, the code words of $W_m$ form a 1 - design $\mathcal{D}_{w_m}$with the number of blocks being the indices of $(S_8(2))_{w_m}$ in$S_8(2)$. This implies that $S_8(2)$ is transitive on the blocks of $\mathcal{D}_{w_m}$ for each $W_m$. Since $(S_8(2))_{w_m}$is a maximal subgroupof $S_8(2)$for $m \in M$ we conclude that$S_8(2)$ acts primitively on $\mathcal{D}_{w_m}$.

**Case II:** Suppose $\mathrm{Aut}(C) = L_8(2)$. In this case $C_{255,i}$ for i= 1, 3 and M = {119, 120, 127, 128, 135, 136}. For all the choices of $m \in M$, we have$(w_m)^{L_8(2)}$. Thus $W_m$is a single orbit of $L_8(2)$.. Similar arguments as in case I, show that$(L_8(2))_{w_m}$ is a maximal subgroup of $L_8(2)$ and that $L_8(2)$ acts primitively on the designs $\mathcal{D}_{w_m}$. In table 5, the first column represents the codewords of weight m (the sub index of m represents the codes from where the codeword is drawn), the second column shows the parameters of the t - designs $\mathcal{D}_{w_m}$as defined in sub – section 6.1, the third column lists the number of blocks of $\mathcal{D}_{w_m}$ and the fourth column indicates whether or not a design $\mathcal{D}_{w_m}$ is primitive under the action

ofAut(C). This information is useful in giving a geometrical interpretation to the codewords of minimum weight.

We take the supports of the code words of non - zero weights in $C_{255,i}$ and orbit them under the action of $S_8(2)$ to form the blocks of designs $\mathcal{D}_{w_m}$ on which$S_8(2)$ acts primitively on points and blocks. Our results are summarized in table 5.

| m | $\mathcal{D}_{w_m}$ | Number of blocks | Primitive |
|---|---|---|---|
| $119_{3,5}$ | 1 – (255, 119, 56) | 120 | Yes |
| $120_{4,5}$ | 1 – (255, 120, 64) | 136 | Yes |
| $127_{2,5}$ | 1 – (255, 127, 127) | 255 | Yes |
| | 2 – ( 255, 127, 63) | 255 | Yes |
| $128_{2,5}$ | 1 – (255, 128, 128) | 255 | Yes |
| | 2 – (255, 128, 64) | 255 | Yes |
| $135_{3,5}$ | 1 – (255, 135, 72) | 136 | Yes |
| $136_{4,5}$ | 1 – (255, 136, 64) | 120 | Yes |

Table 5: Primitive t – designs invariant under Aut ( C )

**Proposition 7.1**

Let M = {127, 128) and N= {119, 120, 136, 137}. Let $\mathcal{D}_{w_m}$be the design held by the codewords of weight m. Then the following hold:

i) Form $\in$ M the automorphism group of the 1 - design $\mathcal{D}_{w_m}$ is $L_8(2)$
ii) Form $\in$ M the automorphism group of the 2 - design $\mathcal{D}_{w_m}$ is $L_8(2)$
iii) Form $\in$ N the automorphism group of the 1 - design $\mathcal{D}_{w_m}$ is $S_8(2)$

**Proof**

i) Let $\mathcal{D}_{w_m}$ be the symmetric 1 - design. By construction $S_8(2) \subseteq$ Aut $(C_{255,i})$and $S_8(2)$ is a primitive group of degree 255. It follows that Aut $(C_{255,i})$is a primitive group of degree 255. Since there are exactly 255 codewords of weight 127 and 128, we use this fact to determine the automorphism group of the design as a set of permutations that preserve the set of the weightof codewords. Let$\bar{G}$ be the automorphism group of the $\mathcal{D}_{w_m}$ 1 - design. Using MAGMA, the$|\bar{G}| = 2^{28}.3^5.5^2.7^2.17.31.127$. The composition series for $\bar{G}$ is $1_{\bar{G}} \trianglelefteq N \trianglelefteq \bar{G}$which is actually a chief series for $\bar{G}$. Hence N is a non abelian chief factor of $\bar{G}$. The order of N is the same as the$|L_8(2)|$. Therefore $N \cong L_8(2)$. Therefore $\bar{G} = L_8(2)$.
ii) We consider the action of Aut $(C_{255,i}) = L_8(2)$for i = 1, 3. G acts 2 - transitively on the set of coordinates of $C_{255,i}$ and the support of a codeword of any fixed non zero weight in $C_{255,i}$will yield a 2 - design. Since $C_{255,i}$ is spanned by the codewords of weight 128 and 127 respectively, and these codewords form the blocks of a symmetric 2 - (255, 127, 63) and 2 -(255, 128, 64) designs $\mathcal{D}_{w_m}$ we have that Aut $(\mathcal{D}_{w_m}) \subseteq$ Aut $(C_{255,5})$. By the fundamental theorem of projective geometry, the automorphism group of the designs is $P\Gamma L_8(2)$ and by order $|\text{Aut}(\mathcal{D}_{w_m})| = 2^{28}.3^5.5^2.7^2.17.31.127 = |\text{Aut}(C_{255,5}).|$ Therefore $|\text{Aut}(\mathcal{D}_{w_m})| = |P\Gamma L_8(2)|$. The composition series forAut $(\mathcal{D}_{w_m})$ shows that it is a simple group and by the classification of simple groups we get that Aut $(\mathcal{D}_{w_m}) = L_8(2)$.

iii) Similar arguments hold as in the proof of i) in proposition 6.3.1

**Remarks**

i) The codewords of minimum weight in $C_{255,1}$represent the points of the projective space PG (7, 2) or the isotropic points of the orthogonal space. They also represent the blocks of the 1 - (255, 128, 128) symmetric design and the 2 - (255, 128, 64) designs of the points and hyperplanes of PG (7, 2). Thus the minimum weight codewords are the incident vectors of the blocks of the designs $\mathcal{D}$and hence spanning vectors of the code. $S_8(2)$acts primitively as a rank – 3 group on the points of the projective space PG (7, 2) and the stabilizer of a point is $2^7{:}\,S_6(2)$ which is maximal in $S_8(2)$. The primitive action of $S_8(2)$ on $2^7{:}\,S_6(2)$ gives three orbits of length 1, 126 and 128. The codewords of minimum weight in $C_{255,1}$ represent the index of this coset action. That is, $[S_8(2) : 2^7{:}\,S_6(2)] = 255$.

ii) NB: there are 255 codewords with minimum weight 128 in$C_{255,1}$. In $C_{255,i}$ for fori = 2, 3, 4, 5 there are 255 codewords with weight 128 and thus represent the blocks of the same designs.

iii) Codewords of weight 127 (which is minimum weight in $C_{255,2}$) represent the blocks of the 1 - (255, 127, 127) symmetric design and 2 - (255, 127, 63) design. Codewords of weight 119 (which is minimum in $C_{255,3}$ and $C_{255,5}$) represent the blocks of the 1 - (255, 119, 56) design. Codewords of weight 120 (which is minimum in $C_{255,4}$) represent the blocks of the 1 - (255, 120, 64) design. Codewords of weight 135 represent the blocks of the 1 - (255, 135, 72) design and codewords of weight 136 represent the blocks of the 1 - (255, 136, 64) design.

iv) The symplectic group $S_8(2)$acts as a primitive rank-3 group of degree 255 on the points of the projective space PG (7, 2). The orbits of the stabilizer of a point α are of length 1, 126 and 128. The point α together with the points of the orbit of length 126 form a hyperplane which is the image of the absolute point α under the symplectic polarity [14]. The symmetric 1 - (255, 128, 128) design $\mathcal{D}$ formed by orbiting the orbit of length 128 is the complement of the design of points and hyperplanes obtained by taking the union of the other 2 orbits. The union of the orbit of length 1 and length 126 give a 2 - (255, 126, 126) symmetric design and its complement is also a 2 - (255, 128, 64) design.

v) By the fundamental theorem of projective geometry, the automorphism group of the design of the points and planes and hence the complementary design is the full projective semi linear group $P\Gamma L_8(2)$

vi) Let G be the simple symplectic group$S_n(q), n > 4$ and q any prime power, acting as a rank – 3 group of degree $\frac{q^n-1}{q-1}$and let $\mathcal{D}$ be the 1 - $\left(\frac{q^n-1}{q-1}, q^{n-1}, q^{n-1}\right)$symmetric design. Then $\mathcal{D}$ is a symmetric 2 – design with automorphism group $P\Gamma L_8(2)$which properly contains the automorphism group of $S_n(q)$ and Aut $(\mathcal{D}) \lneq$ Aut (G) [14].

vii) By taking the action on the symmetric design of points and hyperplanes of the PG(7,2) space or its complementary design, the symplectic group$S_8(2)$in its natural primitive rank – 3 action on the points of the projective space PG(7,2) does not satisfy the conjecture of Key and Moori (section 7 in [11]). For the sake of completeness of this paper, we state the conjecture here: "any design $\mathcal{D}$obtained from a primitive permutation representation of a simple group G will have the automorphism group Aut (G)as its full automorphism group unless the design is isomorphic to another one constructed in the same way in which case the automorphism group of the design will be a proper subgroup of Aut (G)containing G".

**Graphs of the design $D_{255,i}$**

All the graphs of the designs are regular and the vertices are primitive on the points of the blocks. In table 6, the first column represents the supports of codewords w in $C_{255,i}$ orbited under the action of $S_8(2)$to form the blocks of the designs$\mathcal{D}_{w_m}$, the second column gives the number of vertices of the graph , the third column lists the number of edges of the graph and the fourth column shows the valency of the graph. From a $C_{255,1}$code $[255, 8, 128]_2$ with 255 codewords with minimum weight, we get a symmetric 1 – design 1 – (255, 128, 128) with 255 blocks which holds the graph $\Gamma = (255, 128, 64, 64)$. This graph is a symplectic graph $\Gamma = (2^{2m} - 1, 2^{2m-1}, 2^{2m-2}, 2^{2m-2})$, $m = 4$. This graph is a known strongly regular graph with spectrum$[128]^1, [8]^{119}, [-8]^{135}$. The complement of this graph is also a strongly regular graph $\bar{\Gamma} = (255, 126, 61, 63)$ with spectrum $[126]^1, [7]^{135}, [-9]^{119}$.

| w | Vertices (V) | Edges (E) | Valency |
|---|---|---|---|
| 119 | 120 | 7140 | 119 |
| 120 | 136 | 9180 | 135 |
| 127 | 255 | 32385 | 254 |
| 128 | 255 | 32385 | 254 |
| 135 | 136 | 9180 | 135 |
| 136 | 120 | 7140 | 119 |

Table 6: Parameters of the graph $\Gamma = (V, E)$

## References


1. E. Artin (1957). Geometric Algebra, Wiley Interscience, New York.
2. E. F Assmus, Jr and J. D. Key (1992). Designs and their codes, Cambridge University Press, Cambridge tracts in mathematics, Vol 103
3. W. Bosma, J. Cannon, C. Playoust (1997). The Magma algebra system 1, the user language. Journal of symbolic computations 24, no. 3-4, 235 – 265.
4. N.L. Biggs, A. T. White (1979). Permutation groups and combinatorial structures,Cambridge University press, London Mathematical society, Lecture notes series 33.
5. R. Calderbank, W. M. Kantor (1986).The geometry of two weight codes. London Mathematics, Soc. 18, 97 – 122.
6. Y. M. Chee, H. M. Kiah and P. Purkayatsha, (2013). Matrix Codes and Multitone Frequency Shift Keying for Power Line Communications, IEEE International Symposium of Information Theory, 2870 – 2874.
7. Chikamai L.W (2012).Linear codes obtained from 2 – modular representations of some finite simple groups. PhD Thesis, University of KwaZulu – Natal.
8. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson (1985). Atlas of finite groups, Oxford University Press, Oxford.
9. D. Crnkovic, S. Rukavina (2004). On Symmetric (71, 35, 17) designs. Math. Maced, 51 – 50.
10. Dean Crnkovic, SanjaRukavina, LoredanaSimcic (2013). Binary doubly – even self – dual codes of length 72 with large automorphism groups. Mathematical communications 18, 297 – 308.
11. P. Delsarte (1972). Weight of linear codes and strongly regular normed spaces. Discrete Mathematics 3, 47 – 64.
12. P. Dembowski (1968). Finite geometries, Springer -Verlag.

13. Georges Ferdinand R – Radohery (2014), Designs and codes from certain finite simple groups, Msc Thesis, North – West University.
14. M. Grassl(2007). Bounds on the minimum distance of linear codes and quantum codes. Available online athttp://www.codetables.de
15. D. Jungnickel, A. Pot, K. W. Smith (2007). Difference sets. Handbook of combinatorial designs, 2nd Edition, 419 – 435.
16. G. T Kennedy, V. Pless (1995).A coding theoretic approach to extending designs. Discrete Maths, 142, 155 – 168.
17. J . D Key (1998). Codes and finite geometries. Congress Num. 131, 85 – 89.
18. J. D. Key, J. Moori (2002). Designs, codes and graphs from the Janko groups J1 and J2. Journal of Combinatorial Mathematics and combinatorial computing 40, 143 – 153.
19. G. F. R. Radoheny (2013). Designs and codes from certain Finite simple groups. Master's thesis, North west University.
20. Rauhi I. Elkhatib (2012). The Maximal Subgroups of the Symplectic Group PsP8(2), Journal of Systems and Software, Vol 2, No. 3.
21. B.G. Rodriguez (1999). On the theory and examples of group extensions, MastersThesis, University of Natal, Pietermaritzburg.
22. B. G. Rodriguez (2003), Codes of designs and graphs from finite simple groups. PhD thesis, University of Natal, Pietermaritzburg.
23. B. G. Rodriguez (2008). Self – orthogonal designs and codes from the symplectic groups S4(3) and S4.(4). Science direct, Discrete Mathematics, 1941 – 1950.
24. B. G. Rodriguez (2018). A projective two – weight code related to the simple group Co_1 of Conway.
25. J. J. Rotman (1994). An Introduction to the Theory of Groups. Springer
26. D. Seipe (2009). Investigation of binary self dual codes invariant under simple groups, Masters Thesis, The University of Arizona.
27. C. Shannon (1948).A mathematical theory of communication. Bell system, Tech Journal 27, 379 – 423.
28. D. E. Taylor (1992). The geometry of classical groups, Sigma series in pure mathematics, Vol 9, Heldermann -Verlag, Berlin.
29. Tendai M. M. Shumba (2014). On the existence of self dual codes invariant under permutation groups. Masters Thesis, University of KwaZulu – Natal.
30. J. D. Key, J. Moori (2008). "Correction to: "Designs, codes and graphs from the Janko groups J1 and J2 ". Journal of Combinatorial Mathematics and combinatorial computing, 64, 143 -153.
31. J. D. Key, J. Moori and B. G. Rodriguez (2003), On some designs and codes from primitive representations of some finite simple groups. Journal of Combinatorial mathematics and combinatorial computations 45, 3 – 19.