BINARY CODES FROM THE GROUP $\text{PSU}_2(16)$

Ali ZAGHIYAN$^1$, Ahmad MAJLESI$^2$, Reza KAHKESHANI$^3$, Hossein SHABANI$^4$

We examine all of the binary codes constructed from the primitive permutation representations of the group $\text{PSU}_2(16)$ of degrees 68 and 136. It is shown that the groups $\text{PSU}_2(16):4$ and $S_7$ are full automorphism groups of the constructed binary codes.

Keywords: Design, code, automorphism group, projective special unitary group.
MSC2000: 05E15, 05E20, 05B05.

1. Introduction

In [1,2], Key and Moori considered the primitive actions of the Janko groups $J_1$ and $J_2$ and constructed designs, codes and graphs with $J_1$ and $J_2$ as a group of automorphisms. Together with Rodrigues, they extended the results of [1] by applying the same method to the groups $\text{PSp}_6(q)$, $A_6 \cong \text{PSL}_2(9)$ and $A_9$ in [3]. Their aim was to construct designs $D$ from the action of a group $G$ such that $\text{Aut}(D)$ and $\text{Aut}(G)$ have no containment relationship. In [4], the authors considered the design $D$ and binary code $C$ constructed from the action of the McLaughlin group on 275 points and proved that $\text{Aut}(C) = \text{Aut}(D) = \text{McL}:2$. Also, they examined some designs and their binary codes constructed from the primitive permutation representation of degree 2300 of the sporadic simple group $\text{Co}_2$ [5].

Motivated by the method used in [1,2], M. R. Darafsheh et al. considered all of the primitive actions of the groups $\text{PSL}_2(q)$, $q = 11, 13, 16, 17, 19$ and 23 and found the parameters of all the designs and determined their automorphism groups [6]. These results were extended in [7] to the groups $\text{PSL}_2(q)$, $q = 8, 25, 27, 29, 31$ and 32 and in [8] to the groups $\text{PSL}_2(q)$, $q = 37, 41, 43, 47$ and 49. Therefore, the authors completed the construction of 1-designs using the primitive actions of the groups $\text{PSL}_2(q)$, $q$ a prime power less than 50. Moreover, a certain 1-design $D$ from the group $\text{PSL}_2(q)$, $q$ a power of 2, are found such that $\text{Aut}(D) \cong S_{q+1}$ [9]. In following, M. R. Darafsheh et al. constructed the binary

---

$^1$ Assist. Prof., Dept. of Mathematics, University of Technology Esfahan, Esfahan 83145-115, Iran
$^2$ Assist. Prof., Dept. of Mathematics, University of Technology Esfahan, Esfahan 83145-115, Iran
$^3$ Assist. Prof., Dept. of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan 87317 - 51167, Iran, e-mail: kahkeshanireza@kashanu.ac.ir
$^4$ Ph.D. Student, Dept. of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan 87317 - 51167, Iran
codes for all of the designs obtained from the groups $PSL_2(8)$ and $PSL_2(9)$ and found the parameters and determined their automorphism groups [10]. They extended these results to the groups $PSL_2(11)$ and $PSL_2(13)$ in [11] and [12], respectively.

In this paper, we consider all the primitive representations of the group $PSU_2(16)$ of degrees 68, 120 and 136 and construct the binary codes for all the obtained designs. It is shown that the full automorphism groups of the constructed non–trivial codes are $PSU_2(16);4$ and $S_{17}$.

2. Background and notation

Our notation will be standard and it is as in [13], [14] and ATLAS [15]. For the structure of groups and their maximal subgroups, we follow the ATLAS notation. The groups $G.H$, $G:H$ and $G·H$ denote a general extension, a split extension and a non-split extension, respectively. For a prime $p$, $p^0$ denotes the elementary abelian group of order $p^0$.

Let $S = (P,B,I)$ be a finite incidence structure which consists of two disjoint finite sets $P$ and $B$ and a subset $I$ of $P \times B$. The members of $P$ and $B$ are called points and blocks, respectively. It is sometimes convenient to identify a block of $S$ with the set of points incidence with it, and we may write $p \in B$ instead of $(p,B) \in I$. The dual of $S$ is $S' = (B,P,I)$, where $(p,B) \in I$ if and only if $(B,p) \in I'$. The incidence matrix of $S$ is a $|B| \times |P|$ matrix $A$ whose rows are labeled by blocks in $B$, whose columns are labeled by points in $P$ and the entry $(B,p)$ is equal to 1 if $p$ is incidence with $B$ and zero otherwise. Thus the incidence matrix of $S'$ is $A'$, the transpose of $A$. Two structures $S = (P,B,I)$ and $S' = (P',B',I')$ are isomorphic and we write $S \cong S'$ if there is a one to one correspondence $\theta : P \rightarrow P'$ such that $(p,B) \in I$ if and only if $(\theta(p),\theta(B)) \in I'$ for any $p \in P$ and $B \in B$. The structure $S$ is called self–dual if $S \cong S'$. An isomorphism of $S$ onto itself is called an automorphism of $S$ and the set of all the such automorphisms is the group $Aut(S)$. The incidence structure $D = (P,B,I)$ is a $t-(v,k,\lambda)$ design if $|P| = v$, $|B| = k$ for each $B \in B$, and every $t$ points of $P$ is incident with precisely $\lambda$ blocks of $B$. The design $D$ is symmetric if $v = b$, where $|B| = b$. The number of blocks through any set of $s$ points is denoted by $\lambda_s$. It is easy to deduce that $\lambda_s$ is independent of the set, $\lambda_s = \binom{v-s}{t-s} \binom{k-s}{t-s}$ and $D$ is also a $s-(v,k,\lambda_s)$ design if $s \leq t$. $D$ is called trivial if every subset of $P$ with cardinality $k$ is a block of $B$, i.e. $b = \binom{v}{k}$. If $D$ is a $t-(v,k,\lambda)$ design then $D'$ is a design with $b$ points such that the size of every block is $\lambda_1$. The code $C$ of the design $D = (P,B)$ over the finite field $F$
Binary codes from the group $PSU_2(16)$

is the subspace of $F^P$, the full vector space of functions from $P$ to $F$, spanned by the incidence vectors of the blocks over $F$. The orthogonal subspace of $C$ under the standard inner product is the dual code $C^\perp$ and the hull of $C$ is $C \cap C^\perp$. If a linear code over a field of order $q$ is of the length $n$, the dimension $k$ and the minimum distance $d$, then we write $[n,k,d]_q$ to represent this information. The elements of $C$ are called codewords. The support of a codeword $c \in C$ is the set of non-zero coordinate positions of $c$ and the weight of $c$ is the cardinality of this set. The all-one vector which is a vector all of whose coordinate entries are 1 will be denoted by $j$. A binary code, that is a code over $F_2$, with all weights divisible by 2 or 4 is called even or doubly even, respectively. Two linear codes of the same length and over the same field are equivalent if each can be obtained from the other by permuting the coordinate positions and multiplying each coordinate position by a non-zero field element. They are isomorphic if they can be obtained from one another by permuting the coordinate positions. An automorphism of $C$ is any permutation of the coordinate positions that maps codewords to codewords. The set of all the automorphisms of $C$ is a group, denoted by $Aut(C)$.

Let $F_q$ denote the Galois field with $q = p^n$ elements, where $p$ is a prime number and $n$ a positive integer. There is a unique (up to isomorphism) degenerate Hermitian space on vector spaces $V$ over $F_q^2$ and analogously a matrix group corresponding to all of isometries of degenerate Hermitian space denoted by $GU_2(q)$, is named the unitary group. Then $SU_2(q) = \{A \in GU_2(q) | \det(A) = 1\}$ is called a special unitary group and the quotient of $SU_2(q)$ by its center is the projective special unitary group, denoted by $PSU_2(q)$.

3. Preliminaries

Our results for the designs are based on the following standard construction:

**Result 3.1.** [1, Proposition 1], [2, Proposition 1] Let $G$ be a finite primitive permutation group acting on the set $\Omega$ of size $n$. Let $\alpha \in \Omega$ and $\{\alpha\} \neq \Delta$ be an orbit of the stabilizer $G_\alpha$ of $\alpha$. If $B := \Delta^G = \{\Delta^g | g \in G\}$ and $E := \{\alpha, \delta\}^G = \{\{\alpha, \delta\}^g | g \in G\}$, for a given $\delta \in \Delta$, then the incidence structure $D = (\Omega, B)$ forms a symmetric $1-(n,|\Delta|,|\Delta|)$ design. Further, if $\Delta$ is a self-paired orbit of $G_\alpha$ then $\Gamma = (\Omega, E)$ is a regular connected graph of valency $|\Delta|$, $D$ is self-dual and $G$ acts as an automorphism group on each of these structures, primitive on vertices of the graph and on points and blocks of the design.
Remark 3.1. [1], If $\Delta$ be any union of orbits of the stabilizer of a point, including the orbit consisting of the single point, then we still get a symmetric 1-design with the group operating.

Theorem 3.2. [4, Theorems 1 and 2], If $D$ is a design constructed from the primitive group $G$ using Result 3.1, and $C$ is its linear code over a finite field $F_q$, then $G \leq Aut(D) \leq Aut(C)$.

Table 1

| Max. | $n$ | No. | $|\Delta|$ | $|Aut(D)|$ | $C$ | $C^\perp$ | $|Aut(C)|$ |
|------|-----|-----|-----------|----------|-----|----------|----------|
| $D_{34}$ | 120 | 8 | 17(1) | 16320 | [120,120,1] | [120,0,\infty] | 120! |
| | | | 17(2) | 8160 | [120,120,1] | [120,0,\infty] | 120! |
| | | | 17(4) | 4080 | [120,120,1] | [120,0,\infty] | 120! |
| $D_{30}$ | 136 | 9 | 15(1) | 16320 | [136,120,3] | [136,16,16] | 17! |
| | | | 15(2) | 8160 | [136,120,3] | [136,16,16] | 17! |
| | | | 15(4) | 4080 | [136,120,3] | [136,16,16] | 17! |
| | | | 30(1) | 17! | [136,16,16] | [136,120,3] | 17! |
| $A_5$ | 68 | 5 | 12(1) | 16320 | [68,24,12] | [68,44,5] | 16320 |
| | | | 15(1) | 16320 | [68,52,5] | [68,16,22] | 16320 |
| | | | 20(2) | 8160 | [68,24,12] | [68,44,5] | 16320 |

4. Binary codes from $PSU_2(16)$

Using Magma [16] and [17, Exercise 3.6.7], we see that $PSU_2(16)$ has four distinct primitive representations of degrees 136, 120, 68 and 17 respectively to the maximal subgroups $D_{30}$, $D_{34}$, $A_5$ and a solvable group of order 240, respectively. For the last representation, the designs are trivial and so, we don't consider it. Our computations are listed in Table 1; the columns are the maximal subgroups 'Max.', the degree '$n$', the number of orbits 'No.', the size of non-trivial orbits '$|\Delta|$' shows $k$ orbits of length $m$), the cardinality of automorphism groups of the designs '$|Aut(D)|$', the parameters of the design's codes '$C$', their dual codes '$C^\perp$' and the cardinality of automorphism group of the codes '$|Aut(C)|$', respectively (see program in Appendix).

For any primitive representation of degree $n$, we denote the constructed designs by $D_{n,1}$, ..., $D_{n,r}$ if $r$ designs are obtained and by $D_n$ if we have only one design, up to isomorphism. Moreover, this notation is used for the obtained codes.

4.1. The representation of degree 120. Using Result 3.1, three designs $D_{120,1}$, $D_{120,2}$ and $D_{120,3}$ from 7 orbits of length 17 are constructed and it is shown that $Aut(D_{136,1}) = PSU_2(16):4$, $Aut(D_{136,2}) = PSU_2(16):2$ and $Aut(D_{136,3}) = PSU_2(16)$.
Computations with Magma show that the binary codes obtained from these designs are the full space $F_2^{120}$.

4.2. The representation of degree 136. Using Result 3.1, three designs $D_{136,1}$, $D_{136,2}$ and $D_{136,3}$ from 7 orbits of length 15 and a design $D_{136,4}$ from one orbit of length 30 are constructed and it is shown that $\text{Aut}(D_{136,1}) = PSU_2(16):4$, $\text{Aut}(D_{136,2}) = PSU_2(16):2$, $\text{Aut}(D_{136,3}) = PSU_2(16)$ and $\text{Aut}(D_{136,4}) = S_{17}$ [6]. Computation with Magma show that the rows of the block–point incidence matrix of these designs span two codes $C_{136,1}$ and $C_{136,2}$ from the orbits of length 15 and 30, respectively.

**Theorem 4.1.** (i) $C_{136,1}$ and $C_{136,2}$ are $[136,120,3]_2$ and $[136,16,16]_2$ codes, respectively.

(ii) $C_{136,1} \perp C_{136,2}$.

(iii) $C_{136,2}$ is an even code and $j \in C_{136,1}$.

(iv) $F_2^{136} = C_{136,1} \oplus C_{136,2}$.

(v) $\text{Aut}(C_{136,1}) \cong S_{17}$.

**Proof.** (i), (ii) They are deduced by Magma.

(iii) Since $D_{136,4}$ is a design with the even block size, the code $C_{136,2}$ spanned by the rows of the incidence matrix of $D_{136,4}$ is an even binary code. Thus $j \in C_{136,1}$ and

$$A_1 := \{ \omega : \omega \in C_{136,1}, \text{wt}(\omega) = l \}$$

$$= \{ \omega + j : \omega \in C_{136,1}, \text{wt}(\omega) = l \}$$

$$= \{ \omega : \omega \in C_{136,1}, \text{wt}(\omega) = 136 - l \}$$

$$= A_{136 - l}.$$

(iv) Magma shows that the dimension of $\text{hull}(C_{136,1})$ is zero. Therefore, $C_{136,1}$ and $C_{136,2}$ are subspaces of $F_2^{136}$ such that $\dim(C_{136,1} + C_{136,2}) = 120 + 16 - 0 = 136$. This implies the assertion.

(v) By Result 3.2, $S_{17} \leq \text{Aut}(C_{136,1})$. On the other hand, Magma shows that $|\text{Aut}(C_{136,1})| = 355687428096000 = 17!$.

Thus, $\text{Aut}(C_{136,1}) = \text{Aut}(C_{136,2}) \cong S_{17}$.

4.3. The representation of degree 68. Using Result 3.1, three designs $D_{68,1}$, $D_{68,2}$ and $D_{68,3}$ from the orbits of length 12, 15 and 20 are constructed and it is shown that $\text{Aut}(D_{68,1}) = \text{Aut}(D_{68,2}) \cong PSU_2(16):4$ and $\text{Aut}(D_{68,3}) \cong PSU_2(16):2$ [6]. By Magma, the rows of the block–point incidence matrix of these designs span two codes $C_{68,1}$ and $C_{68,2}$ from the orbits of length 12 and 15, respectively.
Theorem 4.2. (i) $C_{68,1}$ and $C_{68,2}$ are binary codes with the parameters $[68,24,12]_2$ and $[68,52,5]_2$, respectively.

(ii) $C_{68,1}$ is an even code and $j \in C_{68,2}$.

(iii) $\text{Aut}(C_{68,1}) = \text{Aut}(C_{68,2}) \cong PSU_2(16):4$.

Proof. (i) It is deduced by Magma.

(ii) Since the design $D_{68,1}$ has the even block size, the code $C_{68,1}$ is even and $j \in C_{68,2}$. Computations with Magma show that the binary code $C_{68,2}^\perp$ is even with the parameters $[68,16,22]$ and hence $j \in C_{68,2}$. It is noticeable that $C_{68,1}$ has 12 codewords of minimum weight that are exactly the incidence vectors of the blocks of $D_{68,1}$.

(iii) Let $\text{Aut}(C_{68,1}) = \overline{G}$. By Magma, $|\overline{G}| = 16320$ and there exist the permutations $\alpha_1, \alpha_2, \alpha_3$ with the cycle type $2^{56}1^8$ and $\gamma$ with the cycle type $4^{30}$ such that $\overline{G} = \langle \alpha_1, \alpha_2, \alpha_3, \gamma \rangle$. Let $N = \langle \alpha_1, \alpha_2, \alpha_3 \rangle$. Computations with Magma show that $PSU_2(16) \cong N \rtimes \overline{G}PSU_2(16)$ and $N \cap \langle \gamma \rangle = 1$. This implies that $\overline{G}$ is a split extension of $N$ by $\gamma$ and hence, $\overline{G} \cong PSU_2(16):4$. Now the assertion is followed, since the operator 'eq' in Magma shows that the codes $C_{68,1}$ and $C_{68,2}$ have the same automorphism group (see the generators in Appendix).

5. Conclusions

We constructed and studied the binary codes obtained from all the primitive representations of the group $PSU_2(16)$ of degrees 68 and 136 and proved that the full automorphism groups of the non-trivial codes are $PSU_2(16):4$ and $S_{17}$. Our construction method is based on the result of Key and Moori [1,2]. Generally, using this method and a computer program, we can construct and examine designs and codes from any finite primitive permutation groups.

6. Acknowledgment

The third author is partially supported by the University of Kashan under grant number 233437/1.

Appendix

Magma version 2.10 of May 2003 was used.

//The program, where $g = PSU(2,16)$ and $m$ is one of the maximal subgroups
a1,a2,a3:=CosetAction(g,m);
st:=Stabilizer(a2,1);
orbs:=Orbits(st);
"no of orbits","#orbs;
v:=Index(a2,st);
"degree",v;
lo:=[#orbs[j]:j in [1..#orbs]];
"seq of orbit length","lo;
for j:=2 to #lo do
"orbs no","j","of length","#orbs[j];
blox:=Setseq(orbs[j]^a2);
des:=Design<1,v|blox>;
autdes:=AutomorphismGroup(des);
"aut des of order",Order(autdes);
lc:=LinearCode(des,GF(2));
du:=Dual(lc);
dim:=Dimension(lc);
dimd:=Dimension(du);
"Code:",Length(lc),dim,MinimumDistance(lc);
"Dual:",Length(du),dimd,MinimumDistance(du);
"dim hull="",Dimension(lc meet du);
if not(dim,dimd) subset [0,1,v,v-1]) then
autcod:=PermutationGroup(lc);
"aut cod of order",Order(autcod);
end if;
end for;
//omiting the trivial designs and the natural representations

Generators

$\alpha_1 = \left(3,91\right)\left(4,23\right)\left(5,57\right)\left(6,100\right)\left(8,119\right)\left(9,62\right)\left(10,102\right)\left(11,38\right)\left(13,84\right)\left(14,79\right)\left(15,103\right)\left(16,24\right)\left(17,67\right)\left(18,73\right)\left(19,68\right)\left(20,104\right)\left(21,45\right)\left(22,25\right)\left(26,106\right)\left(27,72\right)\left(28,113\right)\left(29,55\right)\left(30,37\right)\left(31,105\right)\left(32,34\right)\left(33,35\right)\left(36,107\right)\left(40,53\right)\left(41,80\right)\left(42,54\right)\left(43,46\right)\left(44,75\right)\left(47,117\right)\left(48,64\right)\left(49,93\right)\left(50,90\right)\left(51,66\right)\left(52,78\right)\left(56,82\right)\left(58,61\right)\left(59,88\right)\left(60,110\right)\left(63,115\right)\left(65,109\right)\left(69,92\right)\left(70,94\right)\left(71,98\right)\left(76,118\right)\left(77,120\right)\left(81,96\right)\left(83,101\right)\left(86,87\right)\left(89,97\right)\left(95,116\right)\left(99,112\right)\left(111,114\right);

$\alpha_2 = \left(2,18\right)\left(3,19\right)\left(4,97\right)\left(5,56\right)\left(6,37\right)\left(7,65\right)\left(8,109\right)\left(9,96\right)\left(10,75\right)\left(11,74\right)\left(12,106\right)\left(13,81\right)\left(14,31\right)\left(15,69\right)\left(16,104\right)\left(17,52\right)\left(20,119\right)\left(21,114\right)\left(22,116\right)\left(23,115\right)\left(24,91\right)\left(25,26\right)\left(27,48\right)\left(28,118\right)\left(30,62\right)\left(32,99\right)\left(33,55\right)\left(34,67\right)\left(35,82\right)\left(36,94\right)\left(38,44\right)\left(39,66\right)\left(40,70\right)\left(41,42\right)\left(43,101\right)\left(45,110\right)\left(46,111\right)\left(47,79\right)\left(49,63\right)\left(50,78\right)\left(51,53\right)\left(57,107\right)\left(58,120\right)\left(59,80\right)\left(60,64\right)\left(61,93\right)\left(68,76\right)\left(71,73\right)\left(72,87\right)\left(85,86\right)\left(88,103\right)\left(89,98\right)\left(92,102\right)\left(95,112\right)\left(100,105\right)\left(108,117\right);

$\alpha_3 = \left(1,2\right)\left(3,75\right)\left(4,23\right)\left(5,73\right)\left(6,65\right)\left(7,39\right)\left(8,77\right)\left(9,36\right)\left(10,66\right)\left(11,63\right)\left(12,108\right)\left(13,59\right)\left(14,24\right)\left(15,68\right)\left(16,79\right)\left(17,41\right)\left(18,57\right)\left(19,103\right)\left(20,99\right)\left(21,95\right)\left(22,37\right)\left(25,30\right)\left(26,42\right)\left(27,31\right)\left(28,113\right)\left(29,58\right)\left(32,76\right)\left(33,87\right)\left(34,118\right)\left(35,86\right)\left(38,115\right)\left(40,64\right)\left(43,46\right)\left(44,91\right)\left(45,116\right)\left(47,117\right)\left(48,53\right)\left(49,8

REFERENCES


[11]. M. R. Darafsheh, A. Iranmanesh, R. Kahkeshani, “Codes whose automorphism groups are \( S_5 \), \( PSL_2(11) \) or \( PSL_2(11):2 \)”, submitted for publication.


