



www.combinatorics.ir

Transactions on Combinatorics

ISSN (print): 2251-8657, ISSN (on-line): 2251-8665

Vol. 3 No. 1 (2014), pp. 15-28.

© 2014 University of Isfahan



www.ui.ac.ir

SOME DESIGNS AND CODES FROM $L_2(q)$

J. MOORI AND G. F. RANDRIAFANOMEZANTSOA-RADOHERY*

Communicated by Alireza Abdollahi

ABSTRACT. For $q \in \{7, 8, 9, 11, 13, 16\}$, we consider the primitive actions of $L_2(q)$ and use Key-Moori Method 1 as described in [Codes, designs and graphs from the Janko groups J_1 and J_2 , *J. Combin. Math. Combin. Comput.*, **40** (2002) 143–159., Correction to: “Codes, designs and graphs from the Janko groups J_1 and J_2 ” [J. Combin. Math. Combin. Comput. **40** (2002) 143–159], *J. Combin. Math. Combin. Comput.*, **64** (2008) 153.] to construct designs from the orbits of the point stabilisers and from any union of these orbits. We also use Key-Moori Method 2 (see *Information security, coding theory and related combinatorics*, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., IOS Amsterdam, **29** (2011) 202–230.) to determine the designs from the maximal subgroups and the conjugacy classes of elements of these groups. The incidence matrices of these designs are then used to generate associated binary codes. The full automorphisms of these designs and codes are also determined.

1. Introduction

The structure of a group is deeply entangled with the structure of the objects that they preserve, to some extent we can even say that those objects exist inside the groups themselves. That idea is comforted by the joint works of J. D. Key and J. Moori [5, 6, 8] in which they have developed two methods to construct an incidence structure on the conjugacy classes of a maximal subgroup of a primitive group and an incidence structure on the conjugacy classes of elements of a primitive group. In these methods the primitive group will be an automorphism group of these incidence structures.

In [3, 4] M. R. Darafsheh et al. used only the first method of Key and Moori and constructed 1-designs from the individual non-trivial orbits (that is not from the unions) of the point stabilisers of $L_2(q)$ ($q \in \{8, 9, 11, 13, 16\}$) in their primitive representations. Here, for the same values of q , we

MSC(2010): Primary: 05B05; Secondary: 20D05, 20D06, 94B05.

Keywords: Designs, codes, projective special linear groups, maximal subgroups, conjugacy classes.

Received: 13 May 2013, Accepted: 05 December 2013.

*Corresponding author.

consider all the possible unions of the orbits of the point stabilisers of $L_2(q)$ in some of its primitive representations to construct further additional designs by using Key-Moori Method 1. We also use Key-Moori Method 2 (see [8]) to determine the designs from the maximal subgroups and the conjugacy classes of elements of these groups. These are completely new designs which were not covered in [3, 4]. For each of the designs, constructed by Method 1 or 2, we look at the associated binary code and the structures of the automorphism groups of the design and the code. We note here that in [3, 4] none of the codes were investigated.

The terminology and notation that we use are listed in Section 2. The two methods of Key and Moori are given in Section 3. In Section 4 we construct, all symmetric 1-designs with 28 and 36 points on which $L_2(8)$ acts primitively and all symmetric 1-designs with 15, 55 and 78 points on which $L_2(9)$, $L_2(11)$ and $L_2(13)$ act primitively, respectively. In this section we also construct all symmetric 1-designs with 68 and 120 points on which $L_2(16)$ acts primitively. In this section, finally, we determine all the non-isomorphic binary codes obtained from these designs. In Section 5 we construct all the designs and codes obtained by applying the second method of Key and Moori on $L_2(q)$ for $q \in \{7, 8, 9, 11, 13, 16\}$.

2. Terminologies and notations

For the structure of groups and their maximal subgroups we follow the ATLAS notation [2]. The group $G:H$ denotes a split extension. For a prime p , p^n denotes the elementary abelian group of order p^n . Suppose that G is a finite group acting on a finite set Ω , the action of G on Ω gives a permutation representation π with corresponding permutation character χ_π denoted by $\chi(G|\Omega)$. For a subgroup M of G , if Ω is the set of all conjugates of M in G , then we denote $\chi(G|\Omega)$ by χ_M .

An incidence structure is a triple $I = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, \mathcal{P} is called the point set, \mathcal{B} is called the block set and \mathcal{I} is an incidence relation between \mathcal{P} and \mathcal{B} . A **t-design** or more precisely a **t-(v, k, λ) design** is an incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ such that $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points and every t distinct points are together incident with precisely λ blocks. We will say that the design is **symmetric** if it has the same number of points and blocks. Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a t -(v, k, λ) design with b blocks and let the points be labeled $\{p_1, p_2, \dots, p_v\}$ and the blocks $\{B_1, B_2, \dots, B_b\}$. The **incidence matrix** of \mathcal{D} is a $v \times b$ matrix $D = (d_{ij})$ ($1 \leq i \leq v, 1 \leq j \leq b$) such that $d_{ij} = 1$ if $(x_i, B_j) \in \mathcal{I}$ and $d_{ij} = 0$ otherwise. Two designs \mathcal{D}_1 and \mathcal{D}_2 are isomorphic if there is an incidence-preserving bijection sending the point set of \mathcal{D}_1 to the point set \mathcal{D}_2 and sending the block set of \mathcal{D}_1 to the block set of \mathcal{D}_2 , the automorphism of a design \mathcal{D} is an isomorphism from \mathcal{D} to \mathcal{D} .

If q is a prime power and $F = \mathbb{F}_q$ the finite field of order q , then a **q-ary linear block code** C of length n and dimension k is a subspace of dimension k of the n -dimensional subspace F^n . The elements of C are called **codewords**. In this work all codes are linear block codes. The **dual** code C^\perp of a code C is its orthogonal space with respect to the standard inner product of F^n . The **hull** of a code C is the intersection $C \cap C^\perp$. We endow the vector space F^n with the Hamming distance defined by $d(x, y) = |\{i | x_i \neq y_i\}|$ for $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n) \in F^n$. The **weight** of a code word x is defined by $w(x) = d(x, \mathbf{0})$. The all one vector will be denoted by \mathbf{j} , and is the constant vector of weight the length of the code. The minimum weight d of a code C is defined by $d = \min_{x \in C, x \neq \mathbf{0}} w(x)$.

A $[\mathbf{n}, \mathbf{k}, \mathbf{d}]_q$ code C is a q -ary linear block code of length n , dimension k and minimum weight d . The weight distribution of a code C is the sequence $(A_i)_{i=0}^n$, where A_i is the number of codewords of weight i . The polynomial $A(x) = \sum_{i=0}^n A_i x^i$ is the weight enumerator of C . The code C_F of the t -design \mathcal{D} over F is the space spanned by the rows of the incidence matrix of \mathcal{D} over the field F . The length of C_F is the size of the point set of \mathcal{D} and the dimension of C_F is the rank of the incidence matrix of \mathcal{D} over F . Two codes with the same length and dimension are said to be isomorphic if one can be obtained from the other by permuting the coordinate positions. The automorphism group of C_F is an isomorphism from C_F to C_F .

3. Preliminary results

The designs and codes in this work will be constructed using the following methods described in [6] and [8] :

Method 3.1 (Key-Moori Method 1). *Let G be a finite primitive permutation group acting on the set Ω of size n . Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer G_α of α . If $\mathcal{B} = \{\Delta^g : g \in G\}$, then Ω and \mathcal{B} are the point set and the block set of a symmetric 1 - $(n, |\Delta|, |\Delta|)$ design, with G acting as an automorphism group on this structure, primitive on the points and blocks of the design.*

Proof. For the proof we refer to [6]. □

Theorem 3.2. *Let G be a primitive group acting on a set X of size n . Let Δ be a union of some orbits of the stabiliser including the orbit of size one. If $\mathcal{B} = \{\Delta^g : g \in G\}$, then $\mathcal{D} = (X, \mathcal{B})$ is a symmetric 1 - $(n, |\Delta|, |\Delta|)$ design, with G acting as an automorphism group, primitive on points and blocks of the design. Moreover, the blocks of any symmetric 1 -design with an automorphism group G acting primitively on points can be constructed as union of orbits of the G -stabiliser.*

Proof. If $\Delta \subset X$ is an union of orbits of the stabiliser G_x , then Δ is G_x invariant and $G_x \leq G_\Delta$. By the maximality of G_x , $G_\Delta = G$ or $G_\Delta = G_x$. The first case is impossible since $\Delta \subset X$. Thus $G_\Delta = G_x$ and the design \mathcal{D} has $[G : G_x] = |X| = n$ blocks.

For the proof of the second part of the result we refer to [5, Lemma 2]. □

Method 3.3 (Key-Moori Method 2). *Let G be a finite simple group, M a maximal subgroup of G and nX a conjugacy class of elements of order n in G such that $M \cap nX \neq \emptyset$. Let $\mathcal{B} = \{(M \cap nX)^y | y \in G\}$ and $\mathcal{P} = nX$. Then we have a 1 - $(|nX|, |M \cap nX|, \chi_M(g))$ design \mathcal{D} , where $g \in nX$. The group G acts as an automorphism group on \mathcal{D} , primitive on blocks and transitive (not necessarily) on points of \mathcal{D} .*

Proof. We can find the detailed proof in [8, Theorem 12]. □

Remark 3.4. *In Method 3.3, the number of blocks of the design \mathcal{D} is $b = [G:M]$ and it is symmetric if and only if $|M| = |C_G(g)|$.*

The following results deal with the automorphism group of the designs and codes constructed from Method 3.1.

Result 3.5. *Let \mathcal{D} be a symmetric 1-design obtained by taking all the images under G of a non-trivial orbit Δ of the point stabilizer in any of G 's primitive representations, and on which G acts primitively on points and blocks. Then*

- (i) *the automorphism group of \mathcal{D} contains G .*
- (ii) *If C is a linear code of \mathcal{D} over a finite field \mathbb{F}_q , then the automorphism group of \mathcal{D} is contained in the automorphism group of C .*

Proof. We refer to [9]. □

The following results deal with the automorphism group and the parameters of some designs and codes constructed from Method 3.3.

Result 3.6. (1) *If $\lambda = 1$ and b is the number of blocks of \mathcal{D} then \mathcal{D} is a $1-(|nX|, k, 1)$ design. We have $Aut(\mathcal{D}) = S_k^b : S_b$ and for all prime p , the code C of the design is a $[|nX|, b, k]_p$ code with $Aut(C) = Aut(\mathcal{D})$.*

- (2) *For $G = L_2(q)$, let M be the stabilizer of a point in the natural action of degree $q + 1$ on the set Ω . Let $M = G_1$. Suppose $g \in nX \subseteq G$ is an element fixing exactly one point, and without loss of generality, assume $g \in M$. Then the replication number for the associated design is $r = \lambda = 1$. We also have*

- (i) *If q is odd then $|g^G| = \frac{1}{2}(q^2 - 1)$, $|M \cap g^G| = \frac{1}{2}(q - 1)$, and \mathcal{D} is a $1-(\frac{1}{2}(q^2 - 1), \frac{1}{2}(q - 1), 1)$ designs with $q + 1$ blocks and*

$$Aut(\mathcal{D}) = S_{\frac{1}{2}(q-1)} \wr S_{q+1} = (S_{\frac{1}{2}(q-1)})^{q+1} : S_{q+1}.$$

For all p , $C = C_p(\mathcal{D}) = [\frac{1}{2}(q^2 - 1), q + 1, \frac{1}{2}(q - 1)]_p$, with $Aut(\mathcal{D}) = Aut(C)$.

- (ii) *If q is even then $|g^G| = (q^2 - 1)$, $|M \cap g^G| = (q - 1)$, and \mathcal{D} is a $1-((q^2 - 1), (q - 1), 1)$ design with $q + 1$ blocks and*

$$Aut(\mathcal{D}) = S_{(q-1)} \wr S_{q+1} = (S_{(q-1)})^{q+1} : S_{q+1}.$$

For all p , $C = C_p(\mathcal{D}) = [(q^2 - 1), q + 1, (q - 1)]_p$, with $Aut(\mathcal{D}) = Aut(C)$.

Now if we suppose that $g \in nX \subseteq G$ is an element fixing exactly two points, and without loss of generality, assume $g \in M = G_1$ and that $g \in G_2$. Then the replication number for the associated design is $r = \lambda = 2$. We also have

- (iii) *If g is an involution, so that $q \equiv 1 \pmod{4}$, the design \mathcal{D} is a $1-(\frac{1}{2}q(q + 1), q, 2)$ design with $q + 1$ blocks and $Aut(\mathcal{D}) = S_{q+1}$. Furthermore $C_2(\mathcal{D}) = [\frac{1}{2}q(q + 1), q, q]_2$, $C_p(\mathcal{D}) = [\frac{1}{2}q(q + 1), q, 2q]_p$ if p is an odd prime, and $Aut(C_p(\mathcal{D})) = Aut(\mathcal{D}) = S_{q+1}$ for all p .*
- (iv) *If g is not an involution, the design \mathcal{D} is a $1-(q(q + 1), 2q, 2)$ design with $q + 1$ blocks and $Aut(\mathcal{D}) = 2^{\frac{1}{2}q(q+1)} : S_{q+1}$. Furthermore $C_2(\mathcal{D}) = [q(q + 1), q, 2q]_2$, $C_p(\mathcal{D}) = [q(q + 1), q + 1, 2q]_p$ if p is an odd prime, and $Aut(C_p(\mathcal{D})) = Aut(\mathcal{D}) = 2^{\frac{1}{2}q(q+1)} : S_{q+1}$ for all p .*

Proof. For the proof we refer to [8, Method 2]. □

4. Designs and codes from maximal subgroups

For i, q_i and n_i in Table 1, we applied Method 3.1 to the groups $G = L_2(q_i)$ with Ω the set of all cosets of a maximal subgroup of index n_i . Using MAGMA [1] we considered the primitive representation of degree n_i of $L_2(q_i)$ and we formed the orbits of the point stabilizer. In [3, 4] M.R. Darafsheh et al. used the first method of Key and Moori and constructed 1-designs from the individual non-trivial orbits (that is not from the unions) of $L_2(q_i)$, but here we considered not only the non-trivial orbits but also any of their unions and constructed symmetric 1-designs according to Theorem 3.2. We look at the associated binary codes and the structures of the automorphism groups of the designs and the codes. We note here that in [3, 4] none of these codes were investigated. Table 1 gives the structure of the maximal subgroup of index n_i of $L_2(q_i)$, the number of orbits of the point stabilisers corresponding to the action of $L_2(q_i)$ on the cosets of these maximal subgroups and the lengths of the orbits of the point stabilisers with the number of orbits with that length in parenthesis in case there is more than one such orbits.

i	q_i	n_i	Max. Sub.	rank	length
1	8	28	D_{18}	4	1, 9(3)
2	8	36	D_{14}	5	1, 7(3), 14
3	9	15	S_4	3	1, 8, 6
4	11	55	D_{12}	9	1, 3(2), 6(4), 12(2)
5	13	78	D_{14}	9	1, 7(5), 14(3)
6	16	68	A_5	5	1, 12, 15, 20(2)
7	16	120	D_{34}	8	1, 17(7)

TABLE 1. Orbits of a point-stabiliser of $L_2(q_i)$

If G is a rank- r group, then we should obtain 2^{r-2} designs with block size > 1 and the same number of codes, but some of these structures will be isomorphic. In summary we have the following proposition:

Proposition 4.1. (i) *There exist exactly d_i non isomorphic symmetric 1-designs with n_i points on which $L_2(q_i)$ acts primitively on points and blocks and from these d_i symmetric 1-designs we can generate exactly c_i non isomorphic binary codes. The values of d_i and c_i are given in Table 2a.*

(ii) *δ_{ij} of these d_i designs and γ_{ij} of these c_i codes have automorphism groups isomorphic to A_{ij} as listed in Table 2b.*

Remark 4.2. *In general the number of codes c_i is smaller than the number of designs because two non-isomorphic designs may generate the same code. For instance, for $L_2(16)$ of degree 120 there exist 6 non-isomorphic designs giving the same $[120, 44, 20]_2$ binary code, more precisely 3 of these non-isomorphic designs have the same parameters $1-(120, 52, 52)$ and the other 3 have the parameters $1-(120, 68, 68)$. The block sizes give a partial information about the weight distribution of the corresponding code. The*

(A) Number of designs and codes					(B) Automorphism groups				
i	q_i	n_i	d_i	c_i	j	i	A_{ij}	δ_{ij}	γ_{ij}
1	8	28	6	3	1	1	S_{28}	3	2
2	8	36	14	7	2	1	$L_2(8)$	3	1
3	9	15	6	5	1		$L_2(8)$	8	2
4	11	55	286	31	2	2	S_9	4	3
5	13	78	318	23	3		S_{36}	2	2
6	16	68	22	9	1		S_6	2	0
7	16	120	86	11	2	3	A_8	2	2
					3		S_{15}	2	3
					1		$L_2(11)$	221	4
					2	4	$L_2(11):2$	60	20
					3		S_{11}	3	4
					4		S_{55}	2	3
					1		$L_2(13)$	192	6
					2	5	$L_2(13):2$	124	15
					3		S_{78}	2	2
					1		$L_2(16):2$	9	3
					2	6	$L_2(16):4$	12	4
					3		S_{68}	1	2
					1		$L_2(16)$	49	3
					2		$L_2(16):2$	24	3
					3	7	$L_2(16):4$	8	2
					4		$S_4(4):2$	4	1
					5		S_{120}	1	2

TABLE 2. Designs and codes from $L_2(q_i)$

code has at least 3×120 words of weight 52 and 3×120 words of weight 68. The full weight enumerator of this code is

$$\begin{aligned}
 W(x) = & 1 + 2040x^{20} + 29495x^{24} + 454920x^{28} + 12816045x^{32} + 308806360x^{36} \\
 & + 5956858344x^{40} + 70439478240x^{44} + 467040670200x^{48} + \mathbf{1769618341680x^{52}} \\
 & + 3923105184315x^{56} + 5119220761136x^{60} + 3923105184315x^{64} + \mathbf{1769618341680x^{68}} \\
 & + 467040670200x^{72} + 70439478240x^{76} + 5956858344x^{80} + 308806360x^{84} + 12816045x^{88} \\
 & + 454920x^{92} + 29495x^{96} + 2040x^{100} + x^{120}.
 \end{aligned}$$

For $L_2(16)$ of degrees 68 and 120 ($i = 6, 7$), Table 3 gives $c_6 = 9$ and $c_7 = 11$ non isomorphic codes of length 68 and 120, respectively and one of the representatives of the designs that produced these codes.

The automorphism groups of designs and codes are also given. The second column, 'Block', gives the length of the orbits forming the blocks of the designs.

Degree	Block	Design \mathcal{D}	$\text{Aut}(\mathcal{D})$	Code \mathcal{C}	$\text{Aut}(\mathcal{C})$
68	1 20	1-(68, 21, 21)	$L_2(16):2$	$[68, 52, 5]_2$	$L_2(16):2$
	1 15	1-(68, 16, 16)	$L_2(16):4$	$[68, 17, 16]_2$	$L_2(16):4$
	20(2)	1-(68, 40, 40)	$L_2(16):4$	$[68, 8, 32]_2$	$L_2(16):4$
	1 12 20 15	1-(68, 48, 48)	$L_2(16):2$	$[68, 25, 12]_2$	$L_2(16):2$
	1 12 20	1-(68, 33, 33)	$L_2(16):2$	$[68, 68, 1]_2$	S_{68}
	20	1-(68, 20, 20)	$L_2(16):2$	$[68, 24, 12]_2$	$L_2(16):2$
	12 20(2)	1-(68, 52, 52)	$L_2(16):4$	$[68, 16, 22]_2$	$L_2(16):4$
	1 12 15	1-(68, 28, 28)	$L_2(16):4$	$[68, 9, 28]_2$	$L_2(16):4$
	1 12 15 20(2)	1-(68, 68, 1)	S_{68}	$[68, 1, 68]_2$	S_{68}
120	1 17	1-(120, 18, 18)	$L_2(16)$	$[120, 44, 18]_2$	$L_2(16)$
	17(3)	1-(120, 51, 51)	$L_2(16):2$	$[120, 120, 1]_2$	S_{120}
	1 17	1-(120, 18, 18)	$L_2(16):2$	$[120, 44, 18]_2$	$L_2(16):2$
	1 17(3)	1-(120, 52, 52)	$L_2(16)$	$[120, 44, 24]_2$	$L_2(16)$
	1 17(3)	1-(120, 52, 52)	$L_2(16)$	$[120, 44, 20]_2$	$L_2(16):2$
	17(4)	1-(120, 68, 68)	$L_2(16)$	$[120, 10, 52]_2$	$L_2(16)$
	1 17(5)	1-(120, 86, 86)	$L_2(16):2$	$[120, 36, 18]_2$	$L_2(16):4$
	1 17(3)	1-(120, 52, 52)	$L_2(16)$	$[120, 36, 24]_2$	$L_2(16):4$
	1 17(3)	1-(120, 52, 52)	$L_2(16):2$	$[120, 10, 52]_2$	$L_2(16):2$
	1 17(3)	1-(120, 52, 52)	$S_4(4):2$	$[120, 10, 52]_2$	$S_4(4):2$
	1 17(7)	1-(120, 120, 1)	S_{120}	$[120, 1, 120]_2$	S_{120}

TABLE 3. Designs and codes from $L_2(16)$

4.1. Two 1-(120, 52, 52) non-isomorphic designs and two non-isomorphic $[120, 10, 52]_2$ codes. We consider $L_2(16)$ of degree 120. As we can see from Table 1, there are 7 orbits of length 17. Firstly we take three orbits of length 17 namely the second, the fifth orbit and the eighth orbit (order in MAGMA) and join them with the orbit of length 1 to obtain a block of length 52. Now we apply Method 3.1 to construct a 1-(120,52,52) symmetric design \mathcal{D}_1 . The full automorphism group of \mathcal{D}_1 is the group $S_4(4):2$. From \mathcal{D}_1 we can generate a doubly-even $[120, 10, 52]_2$ code \mathcal{C}_1 with the same automorphism group as \mathcal{D}_1 . The weight enumerator of \mathcal{C}_1 is

$$W(x) = 1 + 120x^{52} + 255x^{56} + 272x^{60} + 255x^{64} + 120x^{68} + x^{120}.$$

The dual of \mathcal{C}_1 is a $[120, 110, 4]_2$ code and $\mathcal{C}_1 \subset \mathcal{C}_1^\perp$.

Secondly we consider the union of the third, the fifth and the sixth orbit with the orbit of length 1. Hence, we obtain another 1-(120, 52, 52) symmetric design \mathcal{D}_2 , non isomorphic to \mathcal{D}_1 , and with the full automorphism group isomorphic to $L_2(16):2$. From \mathcal{D}_2 we can generate a code \mathcal{C}_2 with the same parameters and weight distribution as \mathcal{C}_1 , however \mathcal{C}_1 and \mathcal{C}_2 are non isomorphic. Indeed, the full automorphism group of \mathcal{C}_2 is $L_2(16):2$, which is isomorphic to a subgroup of index 240 of $\text{Aut}(\mathcal{C}_1)$.

5. Designs and codes from maximal subgroups and conjugacy classes of elements

For $q \in \{7, 8, 9, 11, 13, 16\}$ we consider the designs and codes constructed from the groups $L_2(q)$ using Key-Moori Method 2. We discuss in detail the constructions for $L_2(7)$ and for the other groups the results are summarised in Table 10.

The group $L_2(7)$ has 6 conjugacy classes of elements listed in Table 4. Method 3.3 is applied to the maximal subgroups of $L_2(7)$ and its conjugacy classes of elements to construct some non-symmetric 1-designs. The corresponding binary codes are also constructed. The permutation character afforded by the action of $L_2(7)$ on the cosets of its maximal subgroups are listed in Table 5.

nX	# nX	$C_G(g)$	Maximal Centralizer
1A	1	G	Yes
2A	21	D_8	No
3A	56	3	No
4A	42	4	No
7AB	24	7	No

TABLE 4. Conjugacy classes of $L_2(7)$

Max. sub.	Degree	χ_M
S_4	7	$\chi_1 + \chi_4$
7:3	8	$\chi_1 + \chi_5$

TABLE 5. Permutation characters

5.1. $M = S_4, nX = 2A$. We have $\chi_M = \chi_1 + \chi_4$ and hence for g in $2A$

$$b = [G : M] = 7, v = |2A| = 21, k = |M \cap 2A| = 9, \lambda = \chi_M(g) = 1 + 2 = 3.$$

Thus we obtain a non symmetric 1-(21,9,3) design \mathcal{D} with 7 blocks. The group $L_2(7)$ acts primitively on the blocks of \mathcal{D} .

Lemma 5.1. *Two blocks of \mathcal{D} intersect on 3 points and there are exactly 3 blocks containing those 3 points.*

Proof. We consider $A = (a_{ij})_{1 \leq i \leq 21, 1 \leq j \leq 7}$ the incidence matrix of \mathcal{D} with the rows indexed by the 21 points and the columns indexed by the 7 blocks. The block intersection numbers of \mathcal{D} is given by the entries of the symmetric matrix $A^t A$ and using MAGMA we can find that any two distinct blocks of \mathcal{D} intersect exactly on 3 points.

Let be B_1 and B_2 two blocks of \mathcal{D} . The three points of $B_1 \cap B_2$ are denoted by p_1, p_2 and p_3 . Let's consider p_1 , since there are three blocks containing p_1 there is a third block B containing p_1 that is $p_1 \in B \cap B_1$ and $p_1 \in B \cap B_2$. Apart from p_1, p_2 and p_3 we have 6 points $\{p_4, p_5, p_6, p_7, p_8, p_9\}$ inside B_1 which are different from the 6 remaining points $\{p_{10}, p_{11}, p_{12}, p_{13}, p_{14}, p_{15}\}$ of B_2 and 6 other points

$\{p_{16}, p_{17}, p_{18}, p_{19}, p_{20}, p_{21}\}$ which are neither in B_1 nor B_2 . Let's suppose that p_1 and p_2 are not in B , since B intersects B_1 and B_2 on three points, we have to take two points p_4, p_5 from B and p_{10}, p_{11} from B_2 as points of B . To complete B we have to take 4 other points $p_{16}, p_{17}, p_{18}, p_{19}$ which are not inside B_1 or B_2 . Thus we have $\binom{6}{2}^3 > 7$ possibilities for B which is absurd. Hence the two other points in $B \cap B_1$ and $B \cap B_2$ must be p_2 and p_3 and the three blocks containing p_1 are B, B_1 and B_2 . The same arguments apply to p_2 and p_3 , hence $B \cap B_1 \cap B_2 = \{p_1, p_2, p_3\}$ and B_1, B_2 and B are the only blocks containing these three points. \square

Lemma 5.2. *2A is the disjoint union of seven 3-subsets and each block of \mathcal{D} is a union of three of them.*

Proof. By the previous lemma two blocks B_i and B_j intersect exactly on three points and apart from those two blocks there is only a third block B_k containing those three points together and these 3 blocks are the only blocks containing each of these 3 points. We denote by P_{ijk} that set of three points, we have :

- B_1, B_2 and a third block B_3 intersect on P_{123} ; B_1, B_4 and a third block B_5 intersect on P_{145} and $P_{145} \cap P_{123} = \emptyset$; B_1 and the two last blocks B_6 and B_7 intersect on P_{167} . Thus $B_1 = P_{123} \cup P_{145} \cup P_{167}$.
- $B_2 \cap B_1$ and $B_2 \cap B_3$ is P_{123} , $B_2 \cap B_4$ is contained inside B_5 or B_6 or B_7 , it can not be contained inside B_5 since $B_4 \cap B_5$ is P_{145} and it remains two choices B_6 or B_7 , we take B_6 as the third block and $B_2 \cap B_4 \cap B_6$ is P_{246} ; the intersection of B_2 with B_5 is contained inside B_7 and $B_2 \cap B_5 \cap B_7$ is P_{257} . Thus $B_2 = P_{123} \cup P_{246} \cup P_{257}$.
- $B_3 \cap B_1 = B_3 \cap B_2 = P_{123}$, $B_3 \cap B_4 = B_3 \cap B_7 = P_{347}$, $B_3 \cap B_5 = B_3 \cap B_6 = P_{356}$ and $B_3 = P_{123} \cup P_{347} \cup P_{356}$.
- $B_4 \cap B_1 = B_4 \cap B_5 = P_{145}$, $B_4 \cap B_2 = B_4 \cap B_6 = P_{246}$, $B_4 \cap B_3 = B_4 \cap B_7 = P_{347}$ and $B_4 = P_{145} \cup P_{246} \cup P_{347}$.
- $B_5 \cap B_1 = B_5 \cap B_4 = P_{145}$, $B_5 \cap B_2 = B_5 \cap B_7 = P_{257}$, $B_5 \cap B_3 = B_5 \cap B_6 = P_{356}$ and $B_5 = P_{145} \cup P_{257} \cup P_{356}$.
- $B_6 \cap B_1 = B_6 \cap B_7 = P_{167}$, $B_6 \cap B_2 = B_6 \cap B_4 = P_{246}$, $B_6 \cap B_3 = B_6 \cap B_5 = P_{356}$ and $B_6 = P_{167} \cup P_{246} \cup P_{356}$.
- $B_7 \cap B_1 = B_7 \cap B_6 = P_{167}$, $B_7 \cap B_2 = B_7 \cap B_5 = P_{257}$, $B_7 \cap B_3 = B_7 \cap B_4 = P_{347}$ and $B_7 = P_{167} \cup P_{257} \cup P_{347}$.

Observe that $2A = P_{123} \cup P_{145} \cup P_{167} \cup P_{246} \cup P_{257} \cup P_{347} \cup P_{356}$. \square

Proposition 5.3. *2A is the disjoint union of 7 subsets of size 3 which are the points of a 2-(7,3,1) design and $Aut(\mathcal{D}) = S_3^7:L_2(7)$.*

Proof. The first part of the proposition is proved by the previous lemma. For the second part, if we consider the point set $\mathcal{P} = \{P_{123}, P_{145}, P_{167}, P_{246}, P_{257}, P_{347}, P_{356}\}$ and the block set

$$\mathcal{B} = \{(P_{123}, P_{145}, P_{167}), (P_{123}, P_{246}, P_{257}), (P_{123}, P_{347}, P_{356}), (P_{145}, P_{246}, P_{347}), \\ (P_{145}, P_{257}, P_{356}), (P_{167}, P_{246}, P_{356}), (P_{167}, P_{257}, P_{347})\},$$

then $(\mathcal{P}, \mathcal{B})$ is a 2-(7,3,1) design. □

Computation with MAGMA shows that the binary code C of the design \mathcal{D} is a $[21, 4, 9]_2$ code. The weight enumerator of C is $W(x) = 1 + 7x^9 + 7x^{12} + x^{21}$. Further computation gives that $|\text{Aut}(C)| = |\text{Aut}(\mathcal{D})|$, thus we have $\text{Aut}(C) \cong \text{Aut}(\mathcal{D}) \cong S_3^7:L_2(7)$. The dual C^\perp of C is a $[21, 17, 2]_2$ code and $\text{Hull}(C)$ is a $[21, 3, 12]_2$ code.

5.2. $M = S_4, nX \in \{3A, 4A\}$. We have $\chi_M = \chi_1 + \chi_4$ and for $g \in 3A$ or $4A$, $\lambda = \chi_M(g) = 1$. Hence the parameters of the designs and the codes are completely determined by Result 3.6 (1). In both cases $b = [G : M] = 7$.

- For $nX = 3A$, $v = |3A| = 56$ and $k = |M \cap 3A| = 8$. Hence we obtain a non-symmetric 1-(56, 8, 1) design \mathcal{D} with 7 blocks and with $\text{Aut}(\mathcal{D}) = S_8^7:S_7$. The binary code of \mathcal{D} is a $[56, 7, 8]_2$ doubly even code C with $\text{Aut}(C) \cong \text{Aut}(\mathcal{D})$ and with the weight enumerator

$$W(x) = 1 + 7x^8 + 21x^{16} + 35x^{24} + 35x^{32} + 21x^{40} + 7x^{48} + x^{56}.$$

We have $C^\perp = [56, 49, 2]_2$ and $\text{Hull}(C) = C$.

- For $nX = 4A$, $v = |4A| = 42$ and $k = |M \cap 3A| = 6$. Hence we obtain a non-symmetric 1-(42,6,1) design \mathcal{D} with 7 blocks and with $\text{Aut}(\mathcal{D}) = S_6^7:S_7$. The binary code of \mathcal{D} is a $[42, 7, 6]_2$ code C with $\text{Aut}(C) \cong \text{Aut}(\mathcal{D})$ and with the weight enumerator

$$W(x) = 1 + 7x^6 + 21x^{12} + 35x^{18} + 35x^{24} + 21x^{30} + 7x^{36} + x^{42}.$$

5.3. $M = 7:3, nX \in \{3A, 7A\}$. First we notice that M is a maximal subgroup of index $7 + 1$ of $L_2(7)$.

- Now a $g \in 3A$ is an element of order 3 having cycle type 1^23^2 and g fixes exactly two points. So by Result 3.6 2.iv, we obtain a 1-(56, 14, 2) design \mathcal{D} with 8 blocks and $\text{Aut}(\mathcal{D}) \cong 2^{28}:S_8$. The binary code of \mathcal{D} is a $[56, 7, 14]_2$ code with $\text{Aut}(C) \cong \text{Aut}(\mathcal{D})$. The weight enumerator of C is

$$W(x) = 1 + 8x^{14} + 28x^{24} + 56x^{30} + 35x^{32}.$$

- A $g \in 7A$ is an element of order 7 having cycle type 1^17^1 and g fixes exactly one point. Thus by Result 3.6 1.i we obtain a 1-(24, 3, 1) design \mathcal{D} with 8 blocks and with $\text{Aut}(\mathcal{D}) \cong S_3^8:S_8$. The code of \mathcal{D} is a $[24, 8, 3]_2$ code C with $\text{Aut}(C) \cong \text{Aut}(\mathcal{D})$. The weight enumerator of C is

$$W(x) = 1 + 8x^3 + 28x^6 + 56x^9 + 70x^{12} + 56x^{15} + 28x^{18} + 8x^{21} + x^{24}.$$

Max. sub.	Index	nX	Design (\mathcal{D})	Code (C)	Aut(\mathcal{D})	Aut(C)
S_4	7	2A	1-(21,9,3)	$[21, 4, 9]_2$	$S_3^7:L_2(7)$	$S_3^7:L_2(7)$
		3A	1-(56, 8, 1)	$[56, 7, 8]_2$	$S_8^7:S_7$	$S_8^7:S_7$
		4A	1-(42, 6, 1)	$[42, 7, 6]_2$	$S_6^7:S_7$	$S_6^7:S_7$
7:3	8	3A	1-(56, 14, 2)	$[56, 7, 14]_2$	$2^{28}:S_8$	$2^{28}:S_8$
		7A	1-(24, 3, 1)	$[24, 8, 3]_2$	$S_3^8:S_8$	$S_3^8:S_8$

TABLE 6. Codes and designs from $L_2(7)$ using Key-Moori Method 2.

5.4. **Observations.** Proposition 5.3 reflects a common property to the designs constructed from Method 3.3. That method gives us a $1-(v, k, \lambda)$ design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$, that is every point belongs to exactly λ blocks. Here we follow the recent work in a forthcoming paper by T. Le and J. Moori (see [7]). If we consider a point x and if we denote by I_x the intersection of the λ blocks containing x , then $n = |I_x|$ is the same for any point of \mathcal{P} . Moreover if $y \in I_x$, then $I_x = I_y$. If we define on \mathcal{P} the equivalence relation \sim by $y \sim x \Leftrightarrow y \in I_x$, then the number of equivalence classes corresponding to \sim is $v' = v/n$. If $[x]$ is a class of \sim , then $\mathcal{P}' = \{[x_1], \dots, [x_{v'}]\}$ is the point set of a $1-(v', k', \lambda)$ design \mathcal{D}' with $k' = k/n$; $S_n^{v'} \trianglelefteq \text{Aut}(\mathcal{D})$ and $\text{Aut}(\mathcal{D}) / S_n^{v'} \simeq \text{Aut}(\mathcal{D}')$. Table 7 gives a summary of the value of the parameter $n = |I_x|$ and the design \mathcal{D}' corresponding to each design \mathcal{D} in Table 6, we have used MAGMA to compute n and to construct \mathcal{D}' directly from \mathcal{D} .

In Table 8 we can also notice that if $C' = [m', p, d']_2$ is the code from \mathcal{D}' then the code from \mathcal{D} is $C = [m, p, d]_2$ with $m = m'n$ and $d = d'n$.

$1-(v, k, \lambda)$ design \mathcal{D}	$ I_x $	$1-(v', k', \lambda)$ design \mathcal{D}'	Aut(\mathcal{D}')	Aut(\mathcal{D}) $\simeq S_n^{v'}:\text{Aut}(\mathcal{D}')$
1-(21, 9, 3)	3	1-(7, 3, 3)	$L_2(7)$	$S_3^7:L_2(7)$
1-(56, 8, 1)	8	1-(7, 1, 1)	S_7	$S_8^7:S_7$
1-(42, 6, 1)	6	1-(7, 1, 1)	S_7	$S_6^7:S_7$
1-(56, 14, 2)	2	1-(28, 7, 2)	S_8	$2^{28}:S_8$
1-(24, 3, 1)	3	1-(8, 1, 1)	S_8	$S_3^8:S_8$

TABLE 7. Designs from the conjugacy classes of $L_2(7)$

\mathcal{D}	n	\mathcal{D}'	code(C')	code(C)	Aut(C')	Aut(C)
1-(21, 9, 3)	3	1-(7, 3, 3)	$[7, 4, 3]_2$	$[21, 4, 9]_2$	$L_2(7)$	$S_3^7:L_2(7)$
1-(56, 8, 1)	8	1-(7, 1, 1)	$[7, 7, 1]_2$	$[56, 7, 8]_2$	S_7	$S_8^7:S_7$
1-(42, 6, 1)	6	1-(7, 1, 1)	$[7, 7, 1]_2$	$[42, 7, 6]_2$	S_7	$S_6^7:S_7$
1-(56, 14, 2)	2	1-(28, 7, 2)	$[28, 7, 7]_2$	$[56, 7, 14]_2$	S_8	$2^{28}:S_8$
1-(24, 3, 1)	3	1-(8, 1, 1)	$[8, 8, 1]_2$	$[24, 8, 3]_2$	S_8	$S_3^8:S_8$

TABLE 8

TABLE 9. Conjugacy classes of $L_2(q)$

q	nX	$ nX $	$C_G(g)$	Max Centralizer
8	2A	63	2^3	False
	3A	56	9	False
	7ABC	72	7	False
	9ABC	56	9	False
9	2A	45	D_8	False
	3AB	40	9	False
	4A	90	4	False
	5AB	72	5	False
11	2A	55	D_{12}	True
	3A	110	6	False
	5AB	132	5	False
	6A	110	6	False
	11AB	60	11	False
13	2A	63	2^3	False
	3A	56	9	False
	7ABC	72	7	False
	9ABC	56	9	False
16	2A	255	2^4	False
	3A	272	15	False
	5AB	272	15	False
	15ABCD	272	15	False
	17ABCDEFGH	240	17	False

TABLE 10. Codes and designs from $L_2(q)$ using Key-Moori Method 2.

q	Max	nX	Design \mathcal{D}	$\text{Aut}(\mathcal{D})$	Code \mathcal{C}	$\text{Aut}(\mathcal{C})$
8	D_{18}	2A	1-(63,9,4)	$L_2(8):3$	$[63, 19, 9]_2$	$L_2(8):3$
		3A	1-(56, 2, 1)	$2^{28}:S_{28}$	$[56, 28, 2]_2$	$2^{28}:S_{28}$
		9A	1-(56, 2, 1)	$2^{28}:S_{28}$	$[56, 28, 2]_2$	$2^{28}:S_{28}$
	$2^3:7$	2A	1-(63, 7, 1)	$(S_7)^9:S_9$	$[63, 9, 7]_2$	$(S_7)^9:S_9$
		7A	1-(72, 16, 2)	$2^{36}:S_9$	$[72, 8, 16]_2$	$2^{36}:S_9$
	D_{14}	2A	1-(63, 7, 4)	$L_2(8):3$	$[63, 27, 7]_2$	$L_2(8):3$
7A		1-(72, 2, 1)	$2^{36}:S_{36}$	$[72, 36, 2]_2$	$2^{36}:S_{36}$	
9	A_5	2A	1-(45, 15, 2)	$(S_3)^{15}:S_6$	$[45, 5, 15]_2$	$(S_3)^{15}:S_6$
		3A	1-(40, 20, 3)	$2^{20}:S_6$	$[40, 6, 16]_2$	$2^{20}:S_6$
		5A	1-(72, 12, 1)	$(S_{12})^6:S_6$	$[72, 6, 12]_2$	$(S_{12})^6:S_6$
	$3^2:4$	2A	1-(45, 9, 2)	S_{10}	$[45, 9, 9]_2$	S_{10}
		3A	1-(40, 4, 1)	$(S_4)^{10}:S_{10}$	$[40, 10, 4]_2$	$(S_4)^{10}:S_{10}$
		4A	1-(90, 18, 2)	$2^{45}:S_{10}$	$[90, 9, 18]_2$	$2^{45}:S_{10}$
	S_4	2A	1-(45, 9, 3)	$(S_3)^{15}:S_6$	$[45, 10, 9]_2$	$6^{15}:S_6$

Continued on next page

Table 10 – continued from previous page

q	Max	nX	Design \mathcal{D}	$\text{Aut}(\mathcal{D})$	Code \mathcal{C}	$\text{Aut}(\mathcal{C})$	
		3A	1-(40, 8, 3)	$2^{20}:S_6$	$[40, 10, 8]_2$	$2^{20}:S_6$	
		4A	1-(90, 6, 1)	$(S_6)^{15}:S_6$	$[90, 15, 6]_2$	$(S_6)^{15}:S_6$	
11	11:5	5A	1-(132, 22, 2)	$2^{66}:S_{12}$	$[132, 11, 22]_2$	$2^{66}:S_{12}$	
		11A	1-(60, 5, 1)	$(S_5)^{12}:S_{12}$	$[60, 12, 5]_2$	$(S_5)^{12}:S_{12}$	
	A_5	2A	1-(55, 15, 3)	$L_2(11)$	$[55, 11, 15]_2$	$L_2(11):2$	
		3A	1-(110, 20, 2)	$2^{55}:S_{11}$	$[110, 10, 20]_2$	$2^{55}:S_{11}$	
		5A	1-(132, 12, 1)	$(S_{12})^{11}:S_{11}$	$[132, 11, 12]_2$	$(S_{12})^{11}:S_{11}$	
	D_{12}	2A	1-(55, 7, 7)	$L_2(11):2$	$[55, 35, 4]_2$	$L_2(11):2$	
		3A	1-(110, 2, 1)	$2^{55}:S_{55}$	$[110, 55, 2]_2$	$2^{55}:S_{55}$	
	13	13:6	2A	1-(91, 13, 2)	S_{14}	$[91, 13, 13]$	S_{14}
3A			1-(182, 26, 2)	$2^{91}:S_{14}$	$[182, 13, 26]_2$	$2^{91}:S_{14}$	
6A			1-(182, 26, 2)	$2^{91}:S_{14}$	$[182, 13, 26]_2$	$2^{91}:S_{14}$	
13A			1-(84, 6, 1)	$(S_6)^{14}:S_{14}$	$[84, 14, 6]_2$	$(S_6)^{14}:S_{14}$	
A_4		2A	1-(91, 3, 3)	$L_2(13):2$	$[91, 77, 3]_2$	$L_2(13):2$	
		3A	1-(182, 8, 4)	$2^{91}:(L_2(13):2)$	$[182, 62, 8]_2$	$2^{91}:(L_2(13):2)$	
D_{12}		2A	1-(91, 3, 3)	$L_2(13):2$	$[91, 77, 3]_2$	$L_2(13):2$	
		3A	1-(182, 8, 4)	$2^{91}:(L_2(13):2)$	$[182, 62, 8]_2$	$2^{91}:(L_2(13):2)$	
		2B	1-(91, 7, 7)	$L_2(13):2$	$[91, 63, 6]_2$	$L_2(13):2$	
		3B	1-(182, 2, 1)	$2^{91}:S_{91}$	$[182, 91, 2]$	$2^{91}:S_{91}$	
16		$2^4:15$	2A	1-(255, 15, 1)	$(S_{15})^{17}S_{17}$	$[255, 17, 15]_2$	$(S_{15})^{17}S_{17}$
			3A	1-(272, 32, 2)	$2^{136}:S_{17}$	$[272, 16, 32]_2$	$2^{136}:S_{17}$
	5A		1-(272, 32, 2)	$2^{136}:S_{17}$	$[272, 16, 32]_2$	$2^{136}:S_{17}$	
	15A		1-(272, 32, 2)	$2^{136}:S_{17}$	$[272, 16, 32]_2$	$2^{136}:S_{17}$	
	A_5	2A	1-(255, 15, 4)	$(S_3)^{85}:(L_2(16):4)$	$[255, 65, 17]_2$	$(S_3)^{85}:(L_2(16):4)$	
		3A	1-(272, 20, 5)	$(S_3)^{85}:(L_2(16):4)$	$[272, 44, 20]_2$	$(S_3)^{85}:(L_2(16):4)$	
		5A	1-(272, 12, 3)	$(S_3)^{85}:(L_2(16):4)$	$[272, 60, 12]_2$	$(S_3)^{85}:(L_2(16):4)$	
	D_{34}	2A	1-(255, 17, 8)	$L_2(16):4$	$[255, 65, 17]_2$	$L_2(16):4$	
		17A	1-(240, 2, 1)	$2^{120}:S_{120}$	$[240, 120, 2]_2$	$2^{120}:S_{120}$	
	D_{30}	2A	1-(255, 15, 8)	$L_2(16):4$	$[255, 81, 15]_2$	$L_2(16):4$	
		3A	1-(272, 2, 1)	$2^{136}:S_{136}$	$[272, 136, 2]_2$	$2^{136}:S_{136}$	
		5A	1-(272, 2, 1)	$2^{136}:S_{136}$	$[272, 136, 2]_2$	$2^{136}:S_{136}$	
15A		1-(272, 2, 1)	$2^{136}:S_{136}$	$[272, 136, 2]_2$	$2^{136}:S_{136}$		

Acknowledgment

The authors thank the NRF, North-West University (Mafikeng) and AIMS (South Africa) for their supports. The referee is also acknowledged for the invaluable comments.

REFERENCES

[1] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, **24** no. 3-4 (1997) 235–265.

- [2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Eynsham, 1985.
- [3] M. R. Darafsheh, A. R. Ashrafi and M. Khademi, Some designs related to group actions, *Ars Combin.*, **86** 2008 65–75.
- [4] M. R. Darafsheh, A. Iranmanesh and R. Kahkeshani, Some designs and codes invariant under the groups S_9 and A_8 , *Des. Codes Cryptogr.*, **51** no. 2 (2009) 211–223.
- [5] J. D. Key and J. Moori, Codes, designs and graphs from the Janko groups J_1 and J_2 , *J. Combin. Math. Combin. Comput.*, **40** (2002) 143–159.
- [6] J. D. Key and J. Moori, Correction to: “Codes, designs and graphs from the Janko groups J_1 and J_2 ” [J. Combin. Math. Combin. Comput. **40** (2002) 143–159], *J. Combin. Math. Combin. Comput.*, **64** (2008) 153.
- [7] T. Le and J. Moori, On the automorphisms of designs constructed from finite simple groups, Submitted, 2013.
- [8] J. Moori, Finite groups, designs and codes, In *Information security, coding theory and related combinatorics*, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., IOS Amsterdam, **29** 2011 202–230.
- [9] B. G. Rodrigues, *Codes of Designs and Graphs from Finite Simple Groups*, PhD thesis, University of Natal, 2002.

J. Moori

Department of Mathematics, North-West University, P. O. Box 2375, Mafikeng, South Africa

Email: jamshid.moori@nwu.ac.za

G. F. Randriafanomezantsoa-Radohery

Department of Mathematics, North-West University, P. O. Box 2375, Mafikeng, South Africa

Email: georges@aims.ac.za