A self-orthogonal doubly-even code invariant under M^cL

Jamshid Moori*
School of Mathematical Sciences
University of KwaZulu-Natal
Pietermaritzburg 3209
South Africa

B. G. Rodrigues †
School of Mathematical Sciences
University of KwaZulu-Natal
Durban 4041
South Africa

June 22, 2005

Abstract

We examine a design $\mathcal{D}$ and a binary code C constructed from a primitive permutation representation of degree 2025 of the sporadic simple group M^cL. We prove that $\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D}) = M^cL$ and determine the weight distribution of the code and that of its dual. In Section 6 we show that for a word w_i of weight i, where $i \in \{848, 896, 912, 972, 1068, 1100, 1232, 1296\}$ the stabilizer $(M^cL)_{w_i}$ is a maximal subgroup of M^cL. The words of weight 1024 split into two orbits $C_{(1024)_1}$ and $C_{(1024)_2}$ respectively. For $w_i \in C_{(1024)_1}$ we prove that $(M^cL)_{w_i}$ is a maximal subgroup of M^cL.

1 Introduction

The binary codes obtained from the primitive permutation representations of the sporadic simple groups have been examined in [3], [6], [9] and [10].

*Support of NRF and the University of Natal (URF) acknowledged.

†Post-Doctoral research grant of the Ministry of Petroleum (Angola) and the University of of KwaZulu-Natal (URF) acknowledged. The authors also wish to thank the Department of Mathematical Science at Clemson University for the computing facilities.

See [7] for collected results. Here following a similar approach to that of [9] and [10] we construct a 1-(2025, 1232, 1232) self-dual symmetric design $\mathcal{D}$ from a primitive permutation representation of degree 2025 of the sporadic simple group M^cL of McLaughlin [4]. Associated to this design we construct a $[2025, 22, 848]_2$ self-orthogonal doubly-even binary code C which is invariant under the M^cL group. We determine the weight distribution of C and that of $C^\perp$ and show that $\text{Aut}(C) = \text{Aut}(\mathcal{D}) = M^cL$. Also we show that C is the smallest non-trivial $GF(2)$ module on which M^cL acts irreducibly. Let C_i denote the set of all words of C of weight i. In Section 6, we determine the structures of the stabilizers $(M^cL)_{w_i}$, for all nonzero weight i, where w_i is a word of weight i (see Table 3). We show that if $i \in \{848, 896, 912, 972, 1068, 1100, 1232, 1296\}$, $(M^cL)_{w_i}$ is a maximal subgroup of M^cL. Note that the words of weight 1024 split into two orbits, respectively $C_{(1024)_1}$ and $C_{(1024)_2}$. For $w_i \in C_{(1024)_1}$ we show that $(M^cL)_{w_i}$ is a maximal subgroup of M^cL. On the other hand if w_i is such that $i \in \{988, 1004, 1008, (1024)_2, 1052\}$, we describe the structures of $(M^cL)_{w_i}$ for each i and we show that they are not maximal in M^cL. Finally, in Section 6 for each w_i, we take the support of w_i and orbit it under the action of $G = M^cL$ to form the blocks of the $1-(2025, i, k_i)$ designs $\mathcal{D}_{w_i}$ where $k_i = |(w_i)^G| \times \frac{i}{2025}$. Information on these designs is listed in Table 4. We outline our notation in Section 2, and describe the background results and a construction method in Section 3. A brief overview of the simple sporadic group M^cL is given in Section 4. Our results are given in Sections 5 and 6.

2 Terminology and notation

Our notation will be standard, and it is as in [1] and ATLAS [4]. For the structure of groups and their maximal subgroups we follow the ATLAS notation. The groups $G.H$, $G:H$, and $G \cdot H$ denote a general extension, a split extension and a non-split extension respectively. For a prime p, p^n denotes the elementary abelian group of order p^n. We also denote the particular cases of an extraspecial group by p^{1+2n}, p_+^{1+2n} or p_-^{1+2n}.

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. The **dual** structure of $\mathcal{D}$ is $\mathcal{D}^t = (\mathcal{B}, \mathcal{P}, \mathcal{I})$. Thus the transpose of an incidence matrix for $\mathcal{D}$ is an incidence matrix for $\mathcal{D}^t$. We will say that the design is **symmetric** if it has the same number of points and blocks, and **self dual** if it is isomorphic to its dual.

The code C_F of the design $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. We take F to be a prime field

F_p, in which case we write also C_p for C_F, and refer to the dimension of C_p as the **p-rank** of $\mathcal{D}$. In the general case of a 2-design, the prime must divide the order of the design, i.e. $r - \lambda$, where r is the replication number for the design, that is, the number of blocks through a point. If the point set of $\mathcal{D}$ is denoted by $\mathcal{P}$ and the block set by $\mathcal{B}$, and if $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $\mathcal{Q}$ by $v^{\mathcal{Q}}$. Thus $C_F = \langle v^B \mid B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F. For any code C, the **dual** or **orthogonal** code $C^{\perp}$ is the orthogonal under the standard inner product. The **hull** of a design's code over some field is the intersection $C \cap C^{\perp}$. If a linear code over a field of order q is of length n, dimension k, and minimum weight d, then we write $[n, k, d]_q$ to represent this information. If c is a codeword then the **support** of c is the set of non-zero coordinate positions of c. A **constant word** in the code is a codeword all of whose coordinate entries are either 0 or 1. The all-one vector will be denoted by $\jmath$, and is the constant vector of weight the length of the code. 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 a code is any permutation of the coordinate positions that maps codewords to codewords. An automorphism thus preserves each weight class of C.

3 Preliminary results

The designs and codes in this paper come from the following standard construction, described in [9, Proposition 1] and in [10]:

Result 1 *[9, Proposition 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 $\mathcal{B}$ forms a self-dual 1-$(n, |\Delta|, |\Delta|)$ design with n blocks, with G acting as an automorphism group on this structure, primitive on the points and blocks of the design.

Note that if we form any union of orbits of the stabilizer of a point, including the orbit consisting of the single point, and orbit this under the full group, we will still get a self-dual symmetric 1-design with the group operating. Thus the orbits of the stabilizer can be regarded as building blocks. Because of the maximality of the point stabilizer, there is only one orbit of length 1: see [9].

The following two theorems deal with the automorphism groups of the designs and codes constructed from a finite primitive permutation group in a manner described in Theorem 1.

Theorem 1 *[12] Let $\mathcal{D}$ be a self-dual 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 the automorphism group of $\mathcal{D}$ contains G.*

Proof: Suppose that G acts primitively on $\Omega = G/G_\alpha$. Primitivity of G implies that G_α is a maximal subgroup. Let $\mathcal{B} = \{\Delta^g : g \in G\}$ and suppose that $B = \Delta^g$, and $B' = \Delta^{g'}$. Then we have that $(\Delta^g)^{g^{-1}g'} = \Delta^{gg^{-1}g'} = \Delta^{g'}$, and so G acts transitively on $\mathcal{B}$. Now, if $h \in G$ and $\alpha \in \Delta^g$ then $\alpha^h \in (\Delta^g)^h$. Hence, we have that $\alpha^h \in \Delta^{gh}$ and therefore $G \subseteq Aut(\mathcal{D})$. ■

Theorem 2 *If C is a linear code of length n of a symmetric $1-(v,k,k)$ design $\mathcal{D}$ over a finite field F_q, then the automorphism group of $\mathcal{D}$ is contained in the automorphism group of C.*

Proof: Suppose that $\mathcal{D}$ is a $1-(v,k,k)$ design with $\mathcal{P} = \{p_1, p_2, \ldots, p_v\}$ the point set of $\mathcal{D}$ and $\mathcal{B} = \{B_1, B_2, \cdots, B_v\}$ the block set. Let A be an incidence matrix for $\mathcal{D}$, then $\mathcal{P}$ determines uniquely the rows of A, since each point is incident with precisely k blocks. If $\alpha \in Aut(\mathcal{D})$, then α sends p_i to p_j for $1 \leq i,j \leq v$ and $B_{i'}$ to $B_{j'}$ where $1 \leq i', j' \leq v$, and α preserves the incidence relation. Now if C is a code from $\mathcal{D}$, then we have that the columns of A span C. Let R_i and R_j denote the i-th and j-th columns of A respectively, with the entries of R_i and R_j labelled as the blocks indices. Then R_i and R_j have each exactly k non-zero entries, since they represent the incidence relation of a point with the corresponding k blocks of $\mathcal{D}$. Now the self-duality of $\mathcal{D}$ implies that R_i and R_j are weight k vectors in C. Now since α permutes the coordinate positions of the k non-zero entries of R_i to R_j, we deduce that α is an automorphism of C. ■

4 The M^cL group

It was shown by McLaughlin [11] that there exists a regular graph $\mathcal{G} = (\Omega, \mathcal{E})$ with 275 vertices possessing a transitive automorphism group $Aut(\mathcal{G})$ is isomorphic to $M^cL{:}2$, with M^cL a new simple group of order $2^7 \times 3^6 \times 5^3 \times 7 \times 11$. The McLaughlin graph $\mathcal{G}$ is a rank-3 graph of valency 112 on 275 points in which the point stabilizer $U = (M^cL)_x$ is a maximal subgroup isomorphic to $U_4(3)$. The orbits under the action of U are $\{x\}$, Φ and Ψ with lengths 1, 112 and 162, respectively. The action of U on Φ is equivalent to the representation of $U_4(3)$ on the set of totally singular lines of the 4-dimensional unitary space V over the Galois field $GF(9)$ with the stabilizer of a point having the form $3^4{:}A_6$ and orbits of lengths $[1, 30, 81]$. The action of U on Ψ is equivalent to the representation of $U_4(3)$ on the left cosets of a subgroup isomorphic to $L_3(4)$ with the stabilizer of a point having orbits of lengths $[1, 56, 105]$. Thus the two point stabilizers of M^cL on Ω are isomorphic to either $3^4{:}A_6$ or $L_3(4)$. From this we conclude that $U \cap U^g \cong 3^4{:}A_6$ or $L_3(4)$, for any two distinct conjugate subgroups isomorphic to $U_4(3)$.

The group M^cL has precisely one conjugacy class of involutions and the centralizer of an involution in M^cL is isomorphic to $2{\cdot}A_8$, the unique perfect central extension of the alternating group A_8 by a group of order 2. Finkelstein [5] showed that the proper non-abelian simple subgroups of M^cL are isomorphic to A_5, A_6, A_7, $L_2(7)$, $U_4(2)$, $U_3(3)$, $L_3(4)$, $U_3(5)$, $U_4(3)$, M_{11} and M_{22}. There are two classes of M_{22} subgroups, interchanged by the outer automorphism.

Theorem 3 *(Finkelstein [5]) The McLaughlin simple group has precisely twelve conjugacy classes of maximal subgroups. The isomorphism types in these classes are as follows:*

(i) two groups of classical type, namely, $U_4(3)$ *and* $U_3(5)$*;*

(ii) four groups of Mathieu type, namely, M_{11}, M_{22} *(two classes) and* $L_3(4){:}2_2$,
the set stabilizer of two points in the canonical representation of M_{23}*;*

(iii) six p-local subgroups, namely, $2^4{:}A_7$ *(two classes),* $2{\cdot}A_8$, $3^4{:}M_{10}$, $3^{1+4}_{+}{:}2.S_5$
and $5^{1+2}_{+}{:}3{:}8$. ■

5 Computations for M^cL

Using the construction method outlined in Result 1 we have implemented a computer programme that was used in Magma [2] to construct a $1-(2025, 1232, 1232)$ self-dual symmetric design $\mathcal{D}$. Subsequently for the prime $p = 2$ we have constructed its associated code C which is a $[2025, 22, 848]_2$ and determined its basic properties. In addition we have determined the weight distribution for C and for $C^\perp$ and the hull of $\mathcal{D}$. The complementary design of $\mathcal{D}$ is a 1-$(2025, 793, 793)$ self-dual symmetric design $\overline{\mathcal{D}}$ whose binary code $\overline{C}$ is a $[2025, 23, 729]_2$ code . We show in Section 5 that $C \subset \overline{C}$.

The twelve primitive representations referred to in Theorem 3 are listed in Table 1. The first column gives the ordering of the primitive representations as given by Magma (or the ATLAS [4]) and as used in our computations; the second column gives the maximal subgroups while the third list the degrees (the number of cosets of the point stabilizer). We should add that the Magma version 2.10 (13/05/2003) was used for most of the computations in this paper.

No.	Max. sub.	Deg.
1	$U_4(3)$	275
2	M_{22}	2025
3	M_{22}	2025
4	$U_3(5)$	7128
5	$3_+^{1+4} : 2{\cdot}S_5$	15400
6	$3^4 : M_{10}$	15400
7	$L_3(4) : 2_2$	22275
8	$2{\cdot}A_8$	22275
9	$2^4 : A_7$	22275
10	$2^4 : A_7$	22275
11	M_{11}	113400
12	$5_+^{1+2} : 3 : 8$	299376

Table 1: Maximal subgroups of M^cL

5.1 The $1-(2025, 1232, 1232)$ design

Using Theorem 3 and Table 1 we deduce that there are just two classes of maximal subgroups of M^cL group of index 2025. These maximal subgroups are interchanged by an outer automorphism of M^cL. For each class a representative is a group isomorphic to the Mathieu group M_{22}. The M^cL group acts as a rank-4 primitive group on the cosets of M_{22}, with the stabilizer of the action having orbits of length 1, 330, 462 and 1232. We take the orbit of length 1232 and form as indicated in Result 1, a self-dual symmetric 1-(2025, 1232, 1232) design, on which M^cL acts.

Theorem 4 below deals with this design and its automorphism group and in Theorem 5 we show that M^cL is the automorphism group of its associated $[2025, 22, 848]_2$ self-orthogonal doubly-even binary code.

Theorem 4 *For M^cL of degree 2025, the automorphism group of the the design with parameters $1-(2025, 1232, 1232)$ is a non-abelian finite simple group of order 898128000. Moreover this group is isomorphic to the simple sporadic group M^cL.*

Proof: Let Aut($\mathcal{D}$) be the automorphism group of the $1-(2025, 1232, 1232)$ design $\mathcal{D}$ obtained from an orbit of length 1232 for M^cL of degree 2025.

Computations with Magma show that Aut($\mathcal{D}$) is a non-abelian group of order 898128000. Since by Theorem 1 we have Aut($\mathcal{D}$) $\supseteq M^cL$ the result follows. ■

5.2 The $[2025, 22, 848]_2$ code

We found that the 1-(2025, 1232, 1232) design yields a $[2025, 22]_2$ binary code C. In the following theorem we determine some of the properties of C and furthermore we show that Aut(C) $\cong M^cL$.

Theorem 5 *The group M^cL is the automorphism group of the $[2025, 22]_2$ code C obtained from the $1-(2025, 1232, 1232)$ design $\mathcal{D}$. The code C is self orthogonal doubly-even, with minimum distance 848. Its dual is a $[2025, 2003, 4]_2$ with 2338875 words of weight 4. Moreover $\jmath \in C^{\perp}$ and M^cL acts irreducibly on C as a $GF(2)$-module.*

Proof: Let Aut(C) $= \Gamma$. Then by Theorem 2 we have that Aut($\mathcal{D}$) $\subseteq \Gamma$. Our computations show that $|\Gamma| = 898128000 = |\text{Aut}(\mathcal{D})|$ and hence $\Gamma =$ Aut($\mathcal{D}$). Now since Aut($\mathcal{D}$) $= M^cL$ by Theorem 4, the results follows.

Since the blocks of $\mathcal{D}$ are of even size, we have that $\jmath$ meets evenly every vector of C, so $\jmath \in C^{\perp}$. We used Magma to calculate the weight distribution of C which is listed in Table 2. In Table 2, i represents the weight of a codeword and A_i denotes the number of words in C of weight i. From the weight distribution of C we deduce that the minimum weight of C is 848. That C is doubly-even follows immediately from Table 2, since its weights are all divisible by 4. Since C is a binary doubly-even code, it follows that C is self-orthogonal.

TABLE 2
The weight distribution of C

i	A_i
0	1
848	2025
896	22275
912	22275
972	15400
988	356400
1004	1247400
1008	1247400
1024	801900
1052	356400
1068	113400
1100	7128
1232	2025
1296	275

That $C^{\perp}$ has minimum weight 4 was found using Magma. The full weight distribution of $C^{\perp}$ can be obtained.

Notice that $\dim(C) = 22$ and it can be easily shown using Table 3 below that C does not contain invariant subspaces of dimensions 1 and 21 respectively, under M^cL. Thus we deduce that C is the smallest non-trivial $GF(2)$ module on which M^cL acts irreducibly (see [8]). ■

Now if w_i is a word of weight i in C, in Section 6 we determine the structures of $(M^cL)_{w_i}$, i.e, the stabilizers of w_i in M^cL. These are listed in Table 3. Also for each w_i, we take the support of w_i and orbit it under the action of $G = M^cL$ to form the blocks of the $1-(2025, i, k_i)$ designs $\mathcal{D}_{w_i}$ where $k_i = |(w_i)^G| \times \frac{i}{2025}$. Information on these designs is listed in Table 4. In Section 6, Lemmas 6 and 7 deal with the action of M^cL on the codewords of C.

6 Stabilizer of a codeword w_i of weight i

Since M^cL acts as an automorphism group of C we consider this action and determine the structure of $(M^cL)_{w_i}$ where i is in L or $\overline{L}$ with L and $\overline{L}$ as defined below.

Let $L = \{848, 896, 912, 972, 1068, 1100, 1232, 1296\}$ and $\overline{L}$ be the set $\{988, 1004, 1008, 1024, 1052\}$. For $i \in L \cup \overline{L}$ we define C_i to be the set $\{w_i \in C \mid \text{wt}(w_i) = i\}$, where $\text{wt}(w_i)$ denotes the weight of a word w_i. We show in Lemma 6 that $(M^cL)_{w_i}$ is a maximal subgroup of M^cL for all $i \in L$. Now for $w_i \in C_i$ we take the support of w_i and orbit that under M^cL to form the blocks of a 1-design D_{w_i}. We show that for $i \in L$, M^cL acts primitively on D_{w_i}.

Now if $w_i \in C_i$ where $i \in \overline{L}$ we show in Lemma 7 that $(M^cL)_{w_i}$ is not a maximal subgroup of M^cL for all i except when $i = 1024$. Moreover for $i = 1024$, C_{1024} splits into two orbits of lengths 22275 and 779625, namely $C_{(1024)_1}$ and $C_{(1024)_2}$ respectively. We show that $(M^cL)_w$ is isomorphic to $2^4{:}A_7$ or $2^4 : [(A_4 \times 3) : 2]$, where $w \in C_{(1024)_1}$ or $w \in C_{(1024)_2}$ respectively.

Lemma 6 *Let $i \in L$ and $w_i \in C_i$. Then $(M^cL)_{w_i} = M_i$, where M_i is a maximal subgroup of M^cL. Furthermore M^cL is primitive on $\mathcal{D}_{w_i}$ for each i.*

Proof: For any w_i in C_i and $i \in L$ our computations show that ${w_i}^{M^cL} = C_i$. Therefore each C_i forms an orbit under the action of M^cL and thus M^cL is transitive on each C_i. For $w_i \in C_i$ we use Magma to construct $(M^cL)_{w_i}$ as a permutation group inside M^cL. Furthermore we determine its structure by computing its composition factors. We deduce that for $i \in L$, $(M^cL)_{w_i} \in \{M_{22},\ 2^4 : A_7,\ L_3(4) : 2_2,\ 3^4 : M_{10},\ M_{11},\ U_3(5),\ U_4(3)\}$. By the transitivity of M^cL on the code coordinates, the codewords of C_i form a 1-design $\mathcal{D}_{w_i}$ with A_i blocks. This implies that M^cL is transitive on the blocks of D_{w_i} for each w_i and since $(M^cL)_{w_i}$ is a maximal subgroup of M^cL, we deduce that M^cL acts primitively on $\mathcal{D}_{w_i}$. ■

Lemma 7 *Let $i \in \overline{L}$ and $w_i \in C_i$. If $i \neq 1024$, then $(M^cL)_{w_i} \in \{S_6, A_7\}$. If $i = 1024$, then $(M^cL)_{w_i} \cong 2^4{:}A_7$ or $2^4 : [(A_4 \times 3) : 2]$, where $2^4 : [(A_4 \times 3) : 2]$ is not a maximal subgroup of M^cL but sits maximally inside $2^4{:}A_7$.*

Proof: Case 1. Take $w_i \in C_i$ so that $i \in \{988, 1004, 1008, 1052\}$. Our computations show that $w_i{}^{M^cL} = C_i$. Thus each C_i forms an orbit under M^cL and so M^cL is transitive on each C_i. Form our computations with Magma we deduce that $(M^cL)_{w_i} \in \{S_6, A_7\}$ and hence they are not maximal subgroups of M^cL. For details see Table 3 below.

Case 2. Consider $C_{1024} = \{w_i \in C \mid \mathrm{wt}(w_i) = 1024\}$. Then C_{1024} splits into two orbits of lengths 22275 and 779625, namely $C_{(1024)_1}$ and $C_{(1024)_2}$ respectively.

Let $w = w_{(1024)_1} \in C_{(1024)_1}$ and $\overline{w} = w_{(1024)_2} \in C_{(1024)_2}$. Then $(M^cL)_w$ is a subgroup of order 40320 and thus maximal. Using Magma we determine its composition factors and from the list of maximal subgroups of M^cL we deduce that $(M^cL)_w \cong 2^4{:}A_7$.

Since $|(M^cL)_{\overline{w}}| = 1152$, it is not a maximal subgroup of M^cL. Direct computations with Magma shows that $(M^cL)_{\overline{w}}$ has 17 conjugacy classes of elements. The structure of $(M^cL)_{\overline{w}}$ however was not easy to determine by only finding the composition factors, as additional information about the group was needed.

We briefly describe the method used to determine the structure of this group. Using the information listed in the Atlas on the maximal subgroups of the M^cL and the structure of the Sylow subgroups of $(M^cL)_{\overline{w}}$ we are able to determine by direct calculations that $(M^cL)_{\overline{w}}$ sits maximally in a maximal subgroup of M^cL of types $U_4(3)$, $2{\cdot}A_8$ or $2^4{:}A_7$. However a subgroup of $U_4(3)$ or $2{\cdot}A_8$ of order 1152 has 22 conjugacy classes of elements. Therefore $(M^cL)_{\overline{w}}$ is maximal subgroup of $2^4 : A_7$ of type $2^4 : [(A_4 \times 3) : 2]$. ■

7 Observations

(i) In Table 3 the first column represents the words of weight i and the second column represents the stabilizer in M^cL of a codeword w_i of C_i. In the final column we test the maximality of $(M^cL)_{w_i}$ in M^cL. Observe that some of the maximal subgroups of M^cL do not feature in Table 3, namely $3_+{}^{1+4} : 2{\cdot}S_5$, $2{\cdot}A_8$ and $5_+{}^{1+2} : 3 : 8$.

TABLE 3
Stabilizer of a word w_i

i	$(M^cL)_{w_i}$	Maximality
848	M_{22}	Yes
896	$2^4 : A_7$	Yes
912	$L_3(4) : 2_2$	Yes
972	$3^4 : M_{10}$	Yes
988	A_7	No
1004	S_6	No
1008	S_6	No
$(1024)_1$	$L_3(4) : 2_2$	Yes
$(1024)_2$	$2^4 : [(A_4 \times 3) : 2]$	No
1052	A_7	No
1068	M_{11}	Yes
1100	$U_3(5)$	Yes
1232	M_{22}	Yes
1296	$U_4(3)$	Yes

(ii) In Table 4 the first column represents the words of weight i and the second column gives the structure of the designs $\mathcal{D}_{w_i}$ which were defined in Section 6. In the third column we list the number of blocks of $\mathcal{D}_{w_i}$. We test the primitivity for the action of M^cL on $\mathcal{D}_{w_i}$ in the final column.

Table 4
1-designs $\mathcal{D}_{w_i}$ from M^cL

i	$\mathcal{D}_{w_i}$	No. of blocks	Primitivity
848	1-(2025, 848, 848)	2025	Yes
896	1-(2025, 896, 9856)	22275	Yes
912	1-(2025, 912, 10032)	22275	Yes
972	1-(2025, 972, 7392)	15400	Yes
988	1-(2025, 988, 173888)	356400	No
1004	1-(2025, 1004, 618464)	1247400	No
1008	1-(2025, 1008, 620928)	1247400	No
$(1024)_1$	1-(2025, 1024, 112640)	22275	Yes
$(1024)_2$	1-(2025, 1024, 394240)	779625	No
1052	1-(2025, 1052, 185152)	356400	No
1068	1-(2025, 1068, 59808)	113400	Yes
1100	1-(2025, 1100, 3872)	7128	Yes
1232	1-(2025, 1232, 1232)	2025	Yes
1296	1-(2025, 1296, 176)	275	Yes

(iii) From Table 2 it can be observed that $A_{896} = A_{912} = 22275$ and $A_{972} = 15400$. However from Table 1 we have that there are more than one maximal subgroup of M^cL of indices 22275 and 15400 respectively. So for the proof of Lemma 6 in order to ascertain the structures of $(M^cL)_{w_i}$ where $i \in \{896, 912, 972\}$, by using Magma, we have computed their respective composition factors in each case.

(iv) Notice from Table 2 that $A_{988} = A_{1052} = 356400$, and $A_{1004} = A_{1008} = 1247400$. These numbers do not equal the indices of maximal subgroups of M^cL. So for the proof of Case 1 in Lemma 7 in order to determine the structures of $(M^cL)_{w_i}$ where $i \in \{988, 1052, 1004, 1008\}$ by using Magma we have computed their respective composition factors in each case. With the help of the composition factors we deduce that $(M^cL)_{w_i} \cong A_7$ if $i \in \{988, 1052\}$ and $(M^cL)_{w_i} \cong S_6$ if $i \in \{1004, 1008\}$.

(v) The complementary design of $\mathcal{D}$ is a 1-$(2025, 793, 793)$ self-dual design whose binary code is a $[2025, 23, 729]_2$ code that contains the code C and has weight distribution as follows:

```
[<0, 1>,<729, 275>,<793, 2025>,<848, 2025>,<896,22275>,
<912,22275>,<925, 7128>,<957, 113400>,<972, 15400>,
<973,356400>,<988, 356400>, <1001, 801900>,
<1004, 1247400>, <1008, 1247400>,<1017, 1247400>,
<1021, 1247400>, <1024, 801900>, <1037, 356400>,
<1052, 356400>,<1053, 15400>,<1068, 113400>,
<1100, 7128>, <1113, 22275>,<1129, 22275>,
<1177, 2025>, <1232,2025>, <1296, 275>, <2025, 1> ].
```

This code is obtained from C by adjoining the $\jmath$ vector.

(vi) As we mentioned in Subsection 5.1, the M^cL group acts as a rank-4 primitive group on the cosets of M_{22}, with the stabilizer of the action having orbits of length 1, 330, 462 and 1232. If we now take the orbit of length 330 and form as indicated in Result 1, a self-dual symmetric 1-$(2025, 330, 330)$ design, then the hull of this design is a $[2025, 22, 848]_2$ code whose weight distribution is:

```
[ <0, 1>, <848, 2025>, <896, 22275>, <912, 22275>,
<972, 15400>,  <988, 356400>, <1004, 1247400>,
<1008, 1247400>,  <1024, 801900>,  <1052, 356400>,
<1068, 113400>, <1100, 7128>, <1232, 2025>, <1296, 275> ].
```

Magma calculations shows that this code is isomorphic to the code C discussed in detail in Subsection 5.2.

References

[1] E. F. Assmus, Jr. and J. D. Key, *Designs and their Codes*, Cambridge University Press, 1992, Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[2] W. Bosma and J. Cannon, *Handbook of Magma Functions*, Department of Mathematics, University of Sydney, November 1994.

[3] A. R. Calderbank and D. B. Wales, *A global code invariant under the Higman-Sims group*, J. Algebra **75** (1982), 233–260.

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

[5] L. Finkelestein, *The Maximal Subgroups of Conway's Group Co_3 and McLauglin's Group*, J. Algebra **25** (1973), 58–89.

[6] W. H. Haemers, C. Parker, V. Pless, and V. D. Tonchev, *A design and a code invariant under the simple group Co_3*, J. Combin. Theory, Ser. A **62** (1993), no. 2, 225–233.

[7] W. C. Huffman, *Codes and Groups*, Handbook of Coding Theory (In V. S. Pless and W. C. Huffman, eds.), Elsevier, 1998, Volume 2, Part 2, Chapter 17, pp. 1345–1440.

[8] C. Jansen, K. Lux, R. Parker, and R. Wilson., *An Atlas of Brauer Characters*, London Mathematical Society Monographs. New Series, vol. 11, The Clarendon Press Oxford University Press, New York, 1995, Appendix 2 by T. Breuer and S. Norton, Oxford Science Publications.

[9] J. D. Key and J. Moori, *Designs, codes and graphs from the Janko groups J_1 and J_2*, J. Combin. Math and Combin. Comput. **40** (2002), 143–159.

[10] J. D. Key, J. Moori, and B. G. Rodrigues, *On some designs and codes from primitive representations of some finite simple groups*, J. Combin. Math and Combin. Comput. **45** (2003), 3–19.

[11] J. McLaughlin, *A simple group of order* 898,128,000, Theory of Finite Groups (Symposium, Harvard Univ., Cambridge, Mass., 1968), Benjamin, New York, 1969, pp. 109–111.

[12] B. G. Rodrigues, *Codes of Designs and Graphs from Finite Simple Groups*, Ph.D. thesis, University of Natal, Pietermaritzburg, 2002.