# On linear codes constructed from finite groups with a trivial Schur multiplier*

Mohammad Reza Darafsheh[1], Bernardo G. Rodrigues[2] and Amin Saeidi[1,†]

[1] *Department of Mathematics, Statistics and Computer Science, University of Tehran, P. O. Box 14155-6455, Tehran, Iran*
[2] *Department of Mathematics and Applied Mathematics, University of Pretoria, Hatfield 0028, South Africa*

Received July 16, 2022; accepted March 26, 2023

**Abstract.** Using a representation theoretic approach and considering $G$ to be a finite primitive permutation group of degree $n$ with a trivial Schur multiplier, we present a method to determine all binary linear codes of length $n$ that admit $G$ as a permutation automorphism group. In the non-binary case, we can still apply our method, but it will depend on the structure of the stabilizer of a point in the action of $G$. We show that every binary linear code admitting $G$ as a permutation automorphism group is a submodule of a permutation module defined by a primitive action of $G$. As an illustration of the method, we consider $G$ to be the sporadic simple group $M_{11}$ and construct all binary linear codes invariant under $G$. We also construct some point- and block-primitive 1-designs from the supports of some codewords of the codes in the discussion and compute their minimum distances, and in many instances we determine the stabilizers of non-zero weight codewords.

**AMS subject classifications**: 94B05, 05B05

**Keywords**: Linear code, Mathieu group, Schur multiplier, triangular graph

## 1. Introduction

Given a prescribed permutation group $G$, it is an interesting coding theory problem to determine all non-trivial codes invariant under $G$, i.e., all non-trivial codes that admit $G$ as a permutation group of automorphisms, acting transitively on the code coordinate positions.

Recall that the code $\mathcal{C}$ admits the group $G$ as a primitive permutation automorphism group (or $\mathcal{C}$ is a $G$-invariant code) if $G$ is contained in the permutation automorphism group of $\mathcal{C}$ (see Section 3). This justifies our choice of a transitive group $G$ and the suggestion to construct all $G$-invariant codes. There are different methods to construct codes from algebraic structures. Using maximal submodules of permutation modules defined by the primitive action of some simple groups, in

*This research is supported by the Iran National Science Foundation (INSF) (Grant No. 97013746). The second author acknowledges research support by the National Research Foundation of South Africa (Grant Number 120846).

†Corresponding author. *Email addresses:* darafsheh@ut.ac.ir (M. R. Darafsheh), bernardo.rodrigues@up.ac.za (B. G. Rodrigues), saeidi.amin@gmail.com (A. Saeidi)

[5, 6, 7], Chikamai, Moori and Rodrigues studied some binary codes from 2-modular representations of some simple groups.

As an attempt to address the problem stated above, in this paper we introduce a method to construct all $G$-invariant linear codes. This method is based on a result of [14]. In particular, given $G$ a finite simple group, we can find all $G$-invariant binary linear codes of length $|G{:}M|$, where $M$ is a maximal subgroup of the group $G$. We can still apply our method in the non-binary case, but it will depend on the structure of $M$. We give an example of this situation in Section 7.1. In addition, using the well-known Assmus-Mattson theorem, we can construct other combinatorial configurations which admit $G$ as a permutation group of automorphisms. More concretely, we can construct point- and block-primitive 1-designs that are invariant under $G$.

A finite group $T$ is a covering group of $G$ by a group $M$ if $T/M \cong G$ and $M \leq Z(T) \cap T'$, where $Z(T)$ and $T'$ are the center and the derived subgroup of $T$, respectively. We call $M$ the Schur multiplier of $G$ and denote it by $M(G)$. Every finite group $G$ has a universal covering group [9, Theorem 4.226], which is a covering group of $G$ by $M(G)$ (see also [9, §4.15]). In this paper, we focus on groups with a trivial Schur multiplier. In the case when the Schur multiplier of the group $G$ is not trivial, one can still apply the method proposed in the paper by considering the permutation modules of the covering group of $G$. We have not done so in this paper, but in a forthcoming paper [16] we consider this case and a generalization of some of the results presented in this paper.

To illustrate the applicability of the method, we consider $G$ to be the Mathieu group $M_{11}$, this is the smallest sporadic simple group with a trivial Schur multiplier and also because its primitive permutation representations are of moderate size. However, the results of this paper can be generalized to any finite primitive permutation group with a trivial Schur multiplier.

The paper is organized as follows: in Section 2, we outline the terminology and notation. In Section 3, we restate some well-known facts on codes. Section 4 is devoted to modular representation theory. Furthermore, we also prove Theorem 2, which is the main result of this paper that describes the method of construction of the codes. In Section 5, we state some results of the Mathieu group $M_{11}$. In Section 6, we give a brief overview of triangular graphs and find some codes and their structures. In Section 7, we apply the method presented in the paper to determine all linear codes invariant under the Mathieu group $M_{11}$ and study some of their most interesting properties.

## 2. Terminology and notation

Our notation for designs, graphs and groups will be standard, and it is as in [2] , [4] and $\mathbb{ATLAS}$ [8]. An incidence structure is a triple $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ with point set $\mathcal{P}$, block set $\mathcal{B}$ disjoint to $\mathcal{P}$ and incidence set $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$. If the ordered pair $(p, B) \in \mathcal{I}$, we say that $p$ is incident with $B$. We can assume that the blocks in $\mathcal{B}$ are subsets of $\mathcal{P}$, so $(p, B) \in \mathcal{D}$ if and only if $p \in B$. For a positive integer $t$, we say that $\mathcal{D}$ is a $t$-design if every block $B \in \mathcal{B}$ is incident with exactly $k$ points and every $t$ distinct points are together incident with $\lambda$ blocks. In this case, we write $\mathcal{D} = t - (v, k, \lambda)$, where $v = |\mathcal{P}|$. We say that $\mathcal{D}$ is symmetric if it has the same number of points and blocks.

A linear code $\mathcal{C}$ of length $n$ and dimension $k$ is an $F_q$-subspace of dimension $k$ in the vector space $F_q^n$, where $F_q$ is a field of $q$ elements. We may write $\mathcal{C} = [n, k]_q$. If $q = 2$, then we call $\mathcal{C}$ a binary code of most interest. Each element of $\mathcal{C}$ is a codeword and $F_q$ is called the alphabet of $\mathcal{C}$. The Hamming distance of two distinct codewords $c_1$ and $c_2$ of code $\mathcal{C}$ is the number of coordinate positions in which they differ. We denote the Hamming distance of $c_1$ and $c_2$ by $d(c_1, c_2)$. The smallest distance between all pairs of distinct codewords is called the minimum distance of $\mathcal{C}$ and it is denoted by $d(\mathcal{C})$.

Every linear code of length $n$ over $F_q$ contains the zero vector $0 \in F_q$, all of whose coordinates are the zero element of the field. The weight of a codeword $c$ is defined to be $d(c, 0)$. We denote the weight of $c$ by $\mathrm{wt}(c)$. Note that the linear property of $\mathcal{C}$ implies that there exists a codeword whose weight equals $d(\mathcal{C})$. Hence the minimum distance of a linear code is just the minimum weight of the code. Assume that $W = \{w_1, ..., w_n\}$ is the set of weights of all codewords of $\mathcal{C}$, and $w_1 < ... < w_n$. Then the weight distribution of $\mathcal{C}$ is defined as below:

$$\mathcal{WD}(\mathcal{C}) = \{w_1^{n_1}, ..., w_k^{n_k}\},$$

where $n_i$ for each $i$ is the number of codewords of weight $w_i$. The capability of a linear code to detect errors depends on the minimum distance of the code. If the minimum distance of a code is known, then we write $\mathcal{C} = [n, k, d]_q$, where $d = d(\mathcal{C})$. If $q = 2$, we simply write $\mathcal{C} = [n, k, d]$. Note that by [17], the problem of computing the minimum distance of a code is an $NP$-hard problem. Therefore, no efficient algorithms are known to find $d(\mathcal{C})$ in general. The dual code of $\mathcal{C}$ is defined as the set

$$\mathcal{C}^{\perp} = \{v \in \mathcal{C} : \langle v, c\rangle = 0, \text{ for all } c \in \mathcal{C}\},$$

where by $\langle v, c\rangle$ we mean the inner product of $v$ and $c$. A code $\mathcal{C}$ is self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, and it is self-dual if $\mathcal{C} = \mathcal{C}^{\perp}$. The code is called self-complementary if it contains the all-one vector. The all-one vector will be denoted by $\mathbf{1}$.

The support of a nonzero vector $x := (x_1, \ldots, x_n)$, where $x_i \in F_q$, is the set of indices of its non-zero coordinates: $\mathrm{supp}(x) = \{i | x_i \neq 0\}$. The support design of a code of length $n$ for a given non-zero weight $w$ is the design with $n$ points of coordinate indices and blocks the supports of all codewords of weight $w$.

## 3. Some results of codes

In this section, we state some basic results of codes. We start with the following lemma which gives the minimum distances of the repetition code and its dual. Recall that a repetition code of length $n$ is a code whose codewords are formed merely by repeating the message words $n$ times.

**Lemma 1.** *Let $\mathcal{C}$ be the repetition code of length $n$ over a finite field $F_q$ and $\mathcal{C}^{\perp}$ the dual of $\mathcal{C}$. Then $\mathcal{C} = [n, 1, n]_q$ and $\mathcal{C}^{\perp} = [n, n-1, 2]_q$.*

**Lemma 2.** *Let $\mathcal{C}$ be the code of length $n$ over a finite field $F_q$ and $\mathcal{C}^\perp$ the dual of $\mathcal{C}$. Then the all-one codeword $\mathbf{1}$ lies in $\mathcal{C}$ if and only if $q$ divides the sum of all coordinates of each $w \in \mathcal{C}^\perp$. In particular, if $q = 2$, then $\mathbf{1} \in \mathcal{C}$ if and only if the length of $\mathcal{C}^\perp$ is even.*

**Proof**. If $\mathbf{1} \in \mathcal{C}$, then for all $w \in \mathcal{C}^\perp$ we have $\langle w, \mathbf{1}\rangle = 0$. Since $\langle w, \mathbf{1}\rangle$ is the sum of all coordinates of $w$, we get $q \mid \langle w, \mathbf{1}\rangle$. This completes the proof. □

**Corollary 1.** *A binary code is even if and only if it is contained in the dual of the repetition code.*

**Definition 1.** *Let $N$ be a $k \times n$ matrix whose rows generate the linear code $\mathcal{C} = [n, k]_q$. Then the permutation automorphism group of $\mathcal{C}$ is the stabilizer of $\mathcal{C}$ in the symmetric group $S_n$ with respect to the action on the set of the columns of $N$. We denote the permutation automorphism group of $\mathcal{C}$ by* $\mathrm{PAut}(\mathcal{C})$*.*

**Remark 1.** *The permutation automorphism group of a code must be distinguished from the full automorphism group of a code: the stabilizer of the action of ${F_q^*}^n \rtimes S_n$ sending every column of $N$ to a scalar multiple of another column. Clearly* $\mathrm{Aut}(\mathcal{C}) = \mathrm{PAut}(\mathcal{C})$ *in the binary case.*

Notice that $A := \mathrm{PAut}(\mathcal{C})$ is also of degree $n$ and all codewords in $\mathcal{C}$ are of length $n$. If $g \in A$, then for $1 \leq i, j \leq n$ we have $i^g = j$ if and only if for any codeword $v \in \mathcal{C}$ the $i$-th coordinate of $v^g$ is replaced by $j$. This is how $A$ acts on $\mathcal{C}$. For a positive integer $m$, we define:

$$\mathbf{W}_m(\mathcal{C}) = \{v \in \mathcal{C} : \mathrm{wt}(v) = m\}.$$

If there is no ambiguity, we may simply write $\mathbf{W}_m$. Since the automorphisms of $\mathcal{C}$ preserve the weight of codewords, we deduce that $A$ acts on $\mathbf{W}_m$ for every integer $m$ with $\mathbf{W}_m \neq \varnothing$. The stabilizer of this action is of interest. If $v \in \mathbf{W}_m$, then the stabilizer of $v$ in $A$ is the set of all $g \in A$ with $v^g = v$. So if the code is binary, the stabilizer of $v$ in $A$ is isomorphic to the stabilizer of the support of $v$ in $A$. We can see that some 1-designs may be constructed from the codes using this action. We restate and prove the following result from [15].

**Proposition 1.** *Let $\mathcal{C} = [n, k, d]_2$ be a binary linear code admitting $G$ as a permutation automorphism group and $\boldsymbol{W}_m(\mathcal{C}) \neq \varnothing$. If $S$ is an orbit of the action of $G$ on $\boldsymbol{W}_m$, then we have a* 1-$(n, m, m|S|/n)$ *design with block set $\mathcal{B} = \{Supp(w) : w \in S\}$.*

**Proof**. Let $\mathcal{B} = \{B_1, \ldots, B_s\}$, where $s = |S|$ and notice that $|B_i| = m$ for $1 \leq i \leq s$. Suppose that $x \in S$ lies in exactly $\lambda$ blocks of $\mathcal{B}$. Since $G$ acts transitively on $S$, then every $y \in S$ also lies in exactly $\lambda$ blocks of $\mathcal{B}$. Based on this, we can obtain a 1-$(n, m, \lambda)$ design, say $\mathcal{D}$. Now observe that $\bigcup_{i=1}^{s} B_i = \{1, 2, \ldots, n\}$ and each number is repeated $\lambda$ times. Therefore, $n = sm/\lambda$ and the result follows. □

**Remark 2.** *If $\mathcal{C}$ is not a binary code, a similar result holds. We only need to replace $|S|$ by $|\mathcal{B}|$, since in the non-binary case it is possible that the supports of two different codewords coincide.*

## 4. Modular representation theory

Let $G$ be a finite group and $V$ a vector space of dimension $n$ over a field $F$. Then each homomorphism $\Phi : G \to GL(V)$ is called a representation of degree $n$. We can easily check that $V$ becomes a $G$-module by defining $g.v := \Phi(g)(v)$ for $g \in G$ and $v \in V$. Conversely, we can naturally obtain a representation of $G$ if $V$ has a $G$-module structure. Therefore, to each representation there corresponds an $F$-vector space with a $G$-module structure. A representation is irreducible (simple) if the corresponding $G$-module is irreducible. A reducible $G$-module is either completely reducible or indecomposable according to whether $V$ can or can not be written as a direct sum of simple modules. We denote the direct sum of the modules $W_1$ and $W_2$ by $W_1 \oplus W_2$. If $F$ is of characteristic zero or $char(F) \nmid |G|$, then according to Maschke's theorem, $FG$ is semisimple. In particular, indecomposable modules are the same as irreducible modules. However, Maschke's theorem fails if the characteristic of $F$ divides $|G|$. Therefore, in modular representation theory we may face indecomposable modules which are not irreducible. It is well-known that the number of irreducible representations of a finite group is finite. Now let $H$ be a subgroup of $G$ with an $FH$-module $W$. Then we can obtain an $FG$-module $Ind_H^G(W)$ called the induced module of $W$ to $G$ as follows:

$$Ind_H^G(W) = FG \otimes_{FH} W.$$

If $W$ is a one-dimensional module, then the image of the representation corresponding to $Ind_H^G(W)$ is an $m \times m$ matrix in which every row and column has exactly one non-zero entry. Here $m$ is the index of $H$ in $G$. The representation induced by the trivial representation of $H$ is called the permutation module of $G$ of degree $|G{:}H|$. The image of a permutation module is a permutation matrix, that is, a matrix in which each row and column has a unique non-zero entry 1. Conversely, assume that $G$ acts on a set of size $m$. Then we can identify the action of $G$ with the action on the set of rows of the identity $m \times m$ matrix. This clearly defines a representation $P$ of degree $m$ with the property that all rows and columns of the matrices in the image of $\Phi$ contain precisely a single 1 with 0's everywhere else. It is not difficult to show that the $FG$-module corresponding to $P$ is just the permutation module of degree $m$. That is, it is induced from a subgroup of $G$ of index $m$. Now assume that $G$ is a finite simple group with a maximal subgroup $M$. Then we consider the action of $G$ by conjugation on the set $\mathcal{M}$ of all conjugates of $M$ in $G$. It is easy to see that the action is primitive. Since $G$ is simple, the action is faithful and we can view $G$ as a permutation automorphism group of degree $m$, where $m = |G{:}M|$.

For our purpose the relations of these concepts to properties of the "permutation modules" related to the action of a finite group $G$ are important. Let $G$ act on the finite set $\Omega$ and let $F$ be a field. The formal sums $\sum_{\alpha\in\Omega} r_\alpha \alpha$ constitute an $F$-vector space on which $G$ acts as a group of $F$-linear mappings via $(\sum_{\alpha\in\Omega} r_\alpha \alpha)^g = \sum_{\alpha\in\Omega} r_\alpha \alpha^g$, giving the structure of an $FG$-module denoted by $F\Omega$. This module is called the *permutation module* over $F$ to the action of $G$ on $\Omega$ (or the permutation group $G$ if $G$ is a permutation group on $\Omega$). Clearly, the set $\Omega$ can be viewed as an $F$-basis of the permutation module and $(F\Omega, \Omega)$ is a Hamming space in the sense introduced above. Moreover, the action of $G$ on $F\Omega$ preserves the Hamming weight and the canonical bilinear form with orthonormal basis $\Omega$. So the submodules of $F\Omega$ can be considered as linear codes with ambient space $F\Omega$ and ambient basis $\Omega$, whereas $G$ acts as a permutation group of automorphisms on any such code. For simplicity - bearing this in mind - we denote the codes and submodules by the same letters.

Let $\mathcal{LC}(m,q)$ be the set of all linear codes of length $m$ over $GF(q)$ that admit $G$ as their permutation automorphism group. Then one may ask whether $\mathcal{LC}(m,q)$ can be completely determined.

The following result derived from [14] is the starting step towards an answer to this question.

**Theorem 1** ([14], Corollary 3.2)**.** *Assume $(G,X)$ is a primitive permutation automorphism group and $F$ is a field such that $Ext(G/G',F^*)=0$. Let $E$ be a stem cover of $G$ and $E_0$ the inverse image in $E$ of the stabilizer $G_0$. Induce up to $E$ all 1-dimensional $FE_0$-modules. Then the submodules of the resulting $FE$-modules provide for a complete list of codes over $F$ admitting $(G,X)$ as a permutation automorphism group.*

Notice that if $G$ is a perfect group, then $Ext(G/G',F^*)=0$, and the stem extension is simply a central extension. We prove the following main result.

**Theorem 2.** *Let $G$ be a finite simple group and $M$ a maximal subgroup of $G$. Let $P$ be the permutation $FG$-module corresponding to the primitive action of $G$ on $M$, where $F$ is a finite field. Assume that the Schur multiplier of $G$ is trivial and $(|M/M'|,|F^*|)=1$. Then $\mathcal{LC}(m,q)$ equals the set of all submodules of $P$.*

**Proof**. Since the Schur multiplier of $G$ is trivial, then $G$ is its own covering group. Therefore, by Theorem 1, $\mathcal{LC}(m,q)$ is the set of all submodules of the induced modules of 1-dimensional $FM$-modules to $G$. Now, let $\Phi$ be a representation of $M$ of degree 1. We claim that $\Phi$ is trivial. Indeed, $M/\ker\Phi$ lies in a subgroup of $F^*$. As $F^*$ is abelian, we have $M'\leq\ker\Phi$. Hence $|M{:}\ker\Phi|$ divides both $|F^*|$ and $|M/M'|$. Thus we have $M=\ker\Phi$ and the claim is proved. We conclude that $\mathcal{LC}(m,q)$ is the set of all submodules of the permutation module of $G$ of degree $|G{:}M|$. The result now follows.

□

**Remark 3.** *Under the hypotheses of* Theorem 2*, if $|F|=2$, then the equality $(|M/M'|,|F^*|)=1$ holds. So our method can be applied to find all binary codes of length $|G{:}M|$, invariant under $G$. However, for $|F|>2$, the method may not work for some maximal subgroups.*

**Corollary 2.** *Assume the hypothesis and the notation as in Theorem 2. If $M=M'$, then $\mathcal{LC}(m,q)$ equals the set of all submodules of $P$.*

**Proof**. The proof follows as in the proof of Theorem 2 noticing that $(|M/M'|,|F^*|)=1$ over any finite field $F$ for which $|F|\geq 2$.

□

## 5. On the Mathieu group $M_{11}$

In the sequel, to illustrate the constructed method discussed in the paper we consider $G$ to be the Mathieu group $M_{11}$. Recall that $M_{11}$ is the smallest sporadic simple group and it is of order $7920 = 2^4 \times 3^2 \times 5 \times 11$. From the $\mathbb{ATLAS}$ [8], we know that the Schur multiplier of $G$ is trivial. Moreover, up to conjugation, the group has five classes of maximal subgroups, as listed for example in Table 1, where the notation used for the maximal subgroups follows that of the $\mathbb{ATLAS}$.

| No. | Max. sub. | Deg. |
|---|---|---|
| 1 | $M_{10}$ | 11 |
| 2 | $PSL(2,11)$ | 12 |
| 3 | $M_9{:}2$ | 55 |
| 4 | $S_5$ | 66 |
| 5 | $2.S_4$ | 165 |

Table 1: *Maximal subgroups of* $\mathrm{M}_{11}$

For each maximal subgroup $M$ of $G$, the action of $G$ by conjugation on the set of conjugates of $M$, gives a primitive action of degree

$$|G{:}M| \in \{11, 12, 55, 66, 165\}.$$

In this and the remaining sections our aim is to apply Theorem 2 to construct all linear codes invariant under $G$. Using Remark 3 we deduce that every binary code of length $|G{:}M|$ that admits $G$ as a permutation group of automorphisms is a submodule of the permutation module of degree $|G{:}M|$. In general, Theorem 2 holds for codes over $\mathrm{GF}(q)$ provided $(|M{:}M'|, q-1) = 1$.

Observe that $M \cong \mathrm{PSL}(2,11)$ is a perfect group. It follows from Corollary 2 that we can determine all linear codes of length 12 over $GF(q)$, with $q$ dividing $|G|$, and admitting $G$ as a permutation group of automorphisms. However, for the rest of the maximal subgroups $M$ of $G$, the value of $|M{:}M'|$ is 2 or 4. Therefore, Theorem 2 is not applicable in these cases.

We need the following result concerning the number of irreducible $\mathbb{F}_2$-modules of $M_{11}$.

**Proposition 2.** *Let $G$ be the Mathieu group $\mathrm{M}_{11}$. Then there are four irreducible $G$-invariant modules over $GF(2)$, with dimensions $1, 10, 32$ and $44$. With the exception of the submodule of dimension $32$ which splits into two irreducible modules of dimension $16$ over $GF(4)$, the other submodules are absolutely irreducible.*

**Proof**. Follows from the Atlas of Brauer characters [11] or [1]. □

Throughout the paper, by $M_i$ $(1 \leq i \leq 5)$ we mean a maximal subgroup of $G$ which appears in the $i$-th row of Table 1. Denote by $P_i(q)$ the permutation module over $GF(q)$ with respect to the primitive action of $G = M_{11}$ on the set of the conjugates of $M_i$ in $G$. Our aim is to find the set of all binary codes whose automorphism groups contain $G$. According to Theorem 2, the codes are of type $\mathcal{C} := [n, k, d]_2$, where $n = |G{:}M| \in \{11, 12, 55, 65, 165\}$. We usually exclude the cases

$k = 0$ and $k = n$. Furthermore, if $k = 1$, then $\mathcal{C} = [n, 1, n]$ is the repetition code. The repetition code and its dual $[n, n-1, 2]$ have very restricted and well-known structures, so we consider these codes along with the codes of type $[n, 0, n]$ and $[n, n, 1]$ as the trivial codes.

## 6. On triangular graphs and their codes

For a positive integer $n$, the triangular graph $T(n)$ is defined to be the line graph of the complete graph $K_n$. The codes constructed from the triangular graphs have been discussed in [10] and [13]. Since we will encounter instances of binary codes of triangular graphs in the sequel, it seems appropriate at this stage to provide some background of codes from this class of graphs. In this section, we restate some definitions and theorems from those references and also prove some additional results.

The graph $T(n)$ is a strongly regular graph on $v = \binom{n}{2}$ vertices, i.e., on the pairs of letters $\{i, j\}$, where $i, j \in \{1, \ldots, n\}$. If $N$ is the vertex-edge incidence matrix of $K_n$, then $A = N^T N (\text{mod } 2)$ is the adjacency matrix of $T(n)$. The codes generated by $N$ and $A$ are denoted by $\mathcal{C}_N$ and $\mathcal{C}_A$, respectively. Following the discussion before [10, Theorem 4.1], we have that $\mathcal{C}_N$ is an $n-1$ dimensional binary code and $\mathbf{1} \notin \mathcal{C}_N$. According to [10, Theorem 4.1], we have the following result.

**Proposition 3.** *Let $\mathcal{C}_A$ and $\mathcal{C}_N$ be as above.*

- *If $n$ is odd, then $\mathcal{C}_A = \mathcal{C}_N$ and the weight distribution of $\mathcal{C}_A$ is as follows:*

$$\mathcal{WD}(\mathcal{C}_A) = \{i(n-i)^{\binom{n}{i}} : 0 \leq i \leq n/2\}.$$

- *If $n$ is even, then $\mathcal{C}_A = \mathcal{C}_N \cap \mathbf{1}^{\perp}$ and the weight distributions of $\mathcal{C}_A$ and $\mathcal{C}_N$ are as follows:*

$$\mathcal{WD}(\mathcal{C}_N) = \{i(n-i)^{\binom{n}{i}} : 0 \leq i < n/2\} \cup \{n^2/4^{\binom{n}{n/2}/2}\},$$
$$\mathcal{WD}(\mathcal{C}_A) = \{i^j \in \mathcal{WD}(\mathcal{C}_N) : i \ \ \textit{is even}\}.$$

We may view the vertices of $T(n)$ as the sets $\{a, b\}$, where $a \neq b$ and $\{a, b\} \subset \{1, 2, \ldots, n\}$. Each row $\{a, b\}$ of the adjacency matrix of $T(n)$ affords a codeword $v^{\{a,b\}}$ of weight $2(n-2)$. In fact, $\{c, d\} \in Supp(v^{\{a,b\}})$ if and only if $|\{a, b\} \cap \{c, d\}| = 1$. Let $v^{\{a_1 \ldots a_m\}}$ be a codeword of weight $m$ in which the position $\{a_1, a_m\}$ and the positions $\{a_i, a_{i+1}\}$ (for $1 \leq i \leq m-1$) are 1, and 0 elsewhere. We can see that

$$v^{\{a_1 \ldots a_m\}} = v^{\{a_1, a_2\}} + \ldots + v^{\{a_n - 1, a_n\}} + v^{\{a_1, a_m\}}.$$

**Definition 2.** *For $m \geq 3$, assume that the codeword $v^{\{a_1 \ldots a_m\}}$ is as defined above. Then we say that $v^{\{a_1 \ldots a_m\}}$ is of $m$-cycle type. We denote the set of all such codewords by $\mathcal{V}(m)$.*

**Lemma 3.** *Let $\mathcal{C}_A$ be as above. Then ${\mathcal{C}_A}^{\perp}$ contains all codewords of $m$-cycle type $(3 \leq m \leq n)$.*

**Proof**. Let $w = v^{\{a_1,\ldots,a_m\}}$ be a codeword of $m$-cycle type and $v = v^{\{x,y\}} \in \mathcal{C}_A$. We put $S := Supp(v) \cap Supp(w)$. Since $v$ is a generating vertex of $\mathcal{C}_A$, it suffices to prove that $|S|$ is even. If $S = \varnothing$, then we are done. Without loss of generality, we may assume that $x = a_1$ and consider the following cases: If $y = a_2$, then $S = \{\{a_1, a_m\}, \{a_2, a_3\}\}$. Similarly, if $y = a_n$, then

$$S = \{\{a_1, a_2\}, \{a_{m-1}, a_m\}\}.$$

If $y = a_r$, $r \neq 1$ and $r \neq m$, then

$$S = \{\{a_1, a_2\}, \{a_1, a_m\}, \{a_r, a_{r+1}\}, \{a_{r-1}, a_r\}\}.$$

Finally, if $y \neq a_i$ for $1 \leq i \leq m$, then $S = \{\{a_1, a_m\}, \{a_1, a_m\}\}$.

□

**Remark 4.** *Using an argument similar to that used in the proof of Lemma 3, it can be shown that for $3 \leq m \leq 5$, every codeword of weight $m$ in $\mathcal{C}_A^\perp$ is of $m$-cycle type. So there are exactly $\binom{n}{m}(m-1)!/2$ codewords of weight $m$. Furthermore, $(\mathcal{C}_N \oplus \mathbf{1})^\perp$ is simply the set of all codewords of even weight in $\mathcal{C}_A{}^\perp$. Hence the minimum distance of $(\mathcal{C}_N \oplus \mathbf{1})^\perp$ is equal to 4.*

For $n = 11$ and 12, the codes we constructed from $T(n)$ are clearly invariant under the Mathieu group $M_{11}$. We will define another graph related to $T(n)$ in order to construct more codes invariant under $M_{11}$. Let $\mathcal{B} = \{B_1, \ldots, B_n\}$, where $B_i$ is the set of vertices $\{a, b\}$ in $T(n)$, not intersecting at the point $i$. Then it is clear that $\mathcal{B}$ is a block set for a $1-(\binom{n}{2}, \binom{n-1}{2}, n-2)$ design. Let $\mathcal{C}_B$ be the linear code constructed from the incidence matrix of the design. Then we have the following result.

**Lemma 4.** *The weight distribution of $\mathcal{C}_B$ is $\{\binom{n}{k}^{w_k} : 0 \leq k \leq n\}$, where:*

$$w_k = \begin{cases} \binom{n}{2} - k(n-k) & if\ n\, is\, odd, \\ k(n-k) & if\ n\, is\, even. \end{cases}$$

**Proof**. The code $\mathcal{C}_B$ has $n$ generating codewords $c_i$, each of weight $\binom{n-1}{2}$. For each codeword $v$ of length $m$, we define $f_v : \{1, \ldots, m\} \to \{0, 1\}$, with $f_v(i) = 1$ if and only if $i \in Supp(v)$. Every codeword is the sum of $k$ generating codewords. Suppose that $w = c_1 + \ldots + c_k$ and let $\{i, j\}$ be any point. If neither $i$ nor $j$ lie in $\{1, \ldots, k\}$, then for $1 \leq r \leq k$, we have $f_{c_r}(\{i, j\}) = 1$ and we have $\binom{n-k}{2}$ choices for $r$. If both $i$ and $j$ lie in $\{1, \ldots, k\}$, then for all $1 \leq r \leq k$ with $r \neq i$ and $r \neq j$, we have $f_{c_r}(\{i, j\}) = 1$ and we have $\binom{k}{2}$ choices for $r$. In either case, we have $\mathrm{wt}(v) = k - 2 = k \pmod 2$. Now assume that either $i$ or $j$ lies in $\{1, \ldots, k\}$. Then we have $\mathrm{wt}(v) = k - 2 \pmod 2$ and the number of remaining cases is

$$\binom{n}{2} - \binom{n-k}{2} - \binom{k}{2}.$$

If $k$ is odd, then $k - 1 = 0 \pmod 2$. Hence we have:

$$\mathrm{wt}(v) = \binom{n-k}{2} + \binom{k}{2} = \binom{n}{2} - k(n-k),$$

and if $n$ is even, then:

$$\mathrm{wt}(v) = \binom{n}{2} - \binom{n-k}{2} - \binom{k}{2} = k(n-k).$$

□

## 7. Constructing linear codes invariant under $\mathrm{M}_{11}$

Let $G$ be a group with a trivial Schur multiplier and let $M$ be a maximal subgroup of $G$. Then using Theorem 2, we can find all $G$-invariant linear codes of length $|G{:}M|$ that satisfy $(|M{:}M'|, |F^*|) = 1$. Notice that the latter always holds in the binary case, i.e., we can find all $G$-invariant binary codes of length $|G{:}M|$. However, for the case of non-binary codes, we may find all $G$-invariant codes of length $|G{:}M|$ only for some specific types of maximal subgroups (see Corollary 2). In fact, if $|F| > 2$ and $M$ is a maximal subgroup of $G = M_{11}$, then $(|M{:}M'|, |F^*|) = 1$ if and only if $|F| = 3$ and $|G{:}M| = 12$. So we can only guarantee to find all $G$-invariant ternary codes of length 12. Note that applying our method to other maximal subgroups of $G$ will still give us some $G$-invariant codes, but the method does not guarantee to cover all possible such linear codes.

### 7.1. Linear codes of lengths 11 and 12 invariant under $\mathrm{M}_{11}$

We first show that all binary $M_{11}$-invariant codes of lengths 11 and 12 are trivial.

**Proposition 4.** *Let $\mathcal{C}$ be a binary code of length $n = 11$ or $12$ which is invariant under $\mathrm{M}_{11}$. Then $\mathcal{C}$ is a trivial code.*

**Proof**. Let $\mathcal{C}$ be of dimension $m$. We can assume that $m \neq 0$ and $m \neq n$. By Theorem 2, $\mathcal{C}$ corresponds to a submodule of the permutation module of degree $n$. Furthermore, by Proposition 2, $\mathcal{C}$ is a sum of submodules of dimensions 1 and 10. If $n = 11$, then $m = 1$ or 10, and the result follows. So we can assume that $n = 12$. In this case we can easily check that $P_{12}(2)$ has only submodules of dimensions $0, 1, 11$ and 12, and so by Theorem 2, $\mathcal{C}$ is a trivial code.

□

In the remainder of this section, we will construct some non-binary codes. Observe that if $M$ is a maximal subgroup of index 12 in $M_{11}$, then by Table 1 we have $M \cong PSL(2,11)$. Now, since $M = M'$, we can apply Corollary 2 to construct all non-trivial linear codes of length 12 invariant under $G$. We will show that the only non-trivial and non-binary code of length 12 invariant under $\mathrm{M}_{11}$ is the extended ternary Golay code $\mathcal{C} = [12, 6, 6]_3$, which is a self-dual code containing the repetition code. Moreover, the weight distribution of $\mathcal{C}$ is:

$$\{0^1, 6^{264}, 9^{440}, 12^{24}\},$$

and we have $\mathrm{Aut}(\mathcal{C}) \cong 2.\mathrm{M}_{12}$ and $\mathrm{PAut}(\mathcal{C}) \cong \mathrm{M}_{11}$.

In Table 2, we present the structure of the stabilizers of the codewords of $\mathcal{C}$ in $\mathrm{PAut}(\mathcal{C})$ and in $\mathrm{Aut}(\mathcal{C})$, respectively. The first column give the weight $m$ of the codewords in $\mathcal{C}$. The second and the fourth column gives the number of the orbits of the action of $\mathrm{Aut}(\mathcal{C})$ and the fourth $\mathrm{PAut}(\mathcal{C})$, respectively, on the set $\mathbf{W}_m$. The stabilizers of these elements are given in columns 3 and 5, respectively.

| Weight | no. of orbs under Aut | Stab in Aut | no. of orbs under PAut | Stab in PAut |
|---|---|---|---|---|
| 6 | 1 | $S_6$ | 3 (Sizes: $22, 22$ and $220$) | $A_6$, $A_6$ and $S_3 \times S_3$ |
| 9 | 1 | $3^2$:2.$S_4$ | 2 (Sizes: 220 and 220) | $S_3 \times S_3$ and $S_3 \times S_3$ |
| 12 | 1 | $M_{11}$ | 3 (Sizes: $1, 1$ and $22$) | $M_{11}$, $M_{11}$ and $A_6$ |

Table 2: *The stabilizers of the codewords of* $\mathcal{C} = [12, 6, 6]_3$

**Proposition 5.** *Let* $\mathcal{C} = [12, 6, 6]_3$ *be the extended ternary Golay code. Then we have the following support designs obtained from the non-zero codewords of* $\mathcal{C}$. *The notation* $\mathcal{D}_{6i}$ *is used to refer to the* $i$*-th design constructed from the codeword of weight* 6.

- $\mathcal{D}_{61} =$ 3-$(12, 6, 2)$;
- $\mathcal{D}_{62} =$ 3-$(12, 6, 10)$;
- $\mathcal{D}_{63} =$ 5-$(12, 6, 1) = S(5, 6, 12)$;
- $\mathcal{D}_9 =$ 9-$(12, 9, 1) = S(9, 9, 12)$.

**Proof**. The sizes of the orbits are given in Table 2. So by Proposition 1 and Remark 2, we find 1-designs 1-$(12, m, m|\mathcal{B}|/120)$ for $m = 0, 6, 9, 12$. Since for $m = 0$ and $m = 12$ the designs are trivial, we exclude these cases.

Let $m = 6$, and consider the action of $\mathrm{PAut}(\mathcal{C})$ on the set $\mathbf{W}_m$. We can see that

$$\mathbf{W}_m = X \cup 2X \cup Y,$$

where $X$ and $2X$ are orbits of sizes 22. Moreover, all non-zero coordinates of $X$ and $2X$ are 1 and 2, respectively. Furthermore, $Y$ is an orbit of size 220 and the coordinates of its codewords contain 0, 1 and 2. Taking $X$ or $2X$, we can construct a 1-design 1-$(12, 6, \lambda)$, where $\lambda = 22 \times 6/12 = 11$. This design is isomorphic to a 3-$(12, 6, 2)$ design. So assume that $\mathrm{PAut}(\mathcal{C})$ acts on the orbit of size 220. Here the situation described in Remark 2 occurs, since by switching the 1s and 2s, the support of the codewords remains unchanged. Hence, the number of blocks is equal to 110 and we can construct a 1-$(12, 6, \lambda)$ with $\lambda = 110 \times 6/12 = 55$. This design is in fact a 3-$(12, 6, 10)$ design.

For $m = 9$, we have two orbits, say $X$ and $2X$, of sizes 220 with 220 blocks each. Hence, from each of these orbits we construct a 1-$(12, 9, 165)$ design. We can easily show that this is a 9-$(12, 9, 1)$ design.

Now we construct designs by considering the action of $A = \mathrm{Aut}(\mathcal{C})$ on $\mathbf{W}_m$. Note that $A$ acts transitively on $\mathbf{W}_m$, for $m = 6, 9$. All designs constructed by using these orbits are known. Moreover, for $m = 6$, we have a 1-$(12, 6, 66)$ design with 132 blocks. This is in fact a 5-$(12, 6, 1)$ design, a well-known Steiner system $S(5, 6, 12)$, whose automorphism group is isomorphic to $M_{12}$. This completes the proof. □

**Remark 5.** *The support designs, i.e., designs constructed from the supports of the codewords in $\boldsymbol{W}_m$ are $G$-invariant. In particular, note that the linear codes constructed from these designs will not span new codes (this follows from Theorem 2). Here we can see that the linear code constructed from $\mathcal{D}_{61}$ is $\mathcal{C}$, while the code constructed by $\mathcal{D}_{62}, \mathcal{D}_{63}, \mathcal{D}_9$ and $\mathcal{D}_{12}$ is $[12, 12, 11]_3$, the dual of the repetition code.*

## 7.2. Linear codes of length 55

In this section, we study the binary codes of length 55 that admit $G$ as a permutation automorphism group. In the following theorem, we have listed all non-trivial binary codes of length 55.

**Proposition 6.** *Let $\mathcal{C}$ be a non-trivial binary code of length 55 which is invariant under $G = \mathrm{M}_{11}$. Then $\mathcal{C}$ is one of the following codes:*

- $\mathcal{C}_1 = [55, 10, 10]$*;*
- $\mathcal{C}_2 = [55, 44, 4]$*;*
- $\mathcal{C}_3 = \mathbf{1} \oplus \mathcal{C}_1 = C_2^{\perp} = [55, 11, 10]$*;*
- $\mathcal{C}_4 = \mathbf{1} \oplus \mathcal{C}_2 = C_1^{\perp} = [55, 45, 3]$.

*Moreover, $P_3(2) = \mathbf{1} \oplus \mathcal{C}_1 \oplus \mathcal{C}_2$ is a semisimple module and for $1 \leq i \leq 4$ we have $Hull(\mathcal{C}_i) = 0$. The automorphism groups of $\mathcal{C}_i$ $(1 \leq i \leq 4)$ are isomorphic to $S_{11}$.*

**Proof**. The permutation module $P_3(2)$ contains six proper non-zero submodules of distinct dimensions:

$$1, 10, 11, 44, 45, 54.$$

Moreover, by Proposition 2 we have that the submodules of dimensions 1, 10 and 44 are irreducible and so $P_3(2)$ can be expressed as the direct sum of these submodules. Hence, $P_3(2)$ is semisimple. By Theorem 2, there are exactly 6 $G$-invariant binary codes of length 55, four of which are non-trivial. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the irreducible codes of dimensions 10 and 44. It is clear that $\mathcal{C}_1$ is isomorphic to the code $\mathcal{C}_A = [55, 10, 10]$. By Lemma 3 or [13], we have $C_1^{\perp} = [55, 45, 3]$. The code $\mathcal{C}_2$ is the dual of the code $\mathbf{1} \oplus \mathcal{C}_1$. We can easily obtain the weight distribution of $\mathbf{1} \oplus \mathcal{C}_1$ from that of $\mathcal{C}_1$. In particular, we have $\mathbf{1} \oplus \mathcal{C}_1 = [55, 11, 10]$. To complete the proof, we need to compute the minimum distance of $\mathcal{C}_2$. It suffices to observe that $\mathcal{C}_2 = (\mathbf{1} \oplus \mathcal{C}_\mathbf{1})^{\perp}$. Hence, by Remark 4, we have $\mathcal{C}_2 = [55, 44, 4]$. The automorphism groups of the codes are given in [13].

□

We will now focus on the codes $\mathcal{C}_1 = [55, 10, 10]$ and $\mathcal{C}_3 = [55, 11, 10]$. The weight distribution of $\mathcal{C}_1$ is as follows:

$$\mathcal{WD}(\mathcal{C}_1) = \{0^1, 10^{11}, 18^{55}, 24^{165}, 28^{330}, 30^{462}\}.$$

Since $\mathcal{C}_3 = [55, 11, 10]$ is a direct sum of $\mathcal{C}_2$ and the repetition code, the weight distribution of $\mathcal{C}_3$ can be immediately computed. In fact, we have:

$$\mathcal{WD}(\mathcal{C}_3) = \{0^1, 10^{11}, 18^{55}, 24^{165}, 25^{462}, 27^{330}, 28^{330}, 30^{462}, 31^{165}, 37^{55}, 45^{11}, 55^1\}.$$

**Proposition 7.** *Let $w$ be a codeword of the code $\mathcal{C}_i$ $(i = 1, 3)$ of weight $m$ and $A = \mathrm{Aut}(\mathcal{C}_i) \cong S_{11}$. If $\boldsymbol{W}_m(C_i) \neq \varnothing$, then the action of $A$ on $\boldsymbol{W}_m(\mathcal{C}_i)$ is transitive. The stabilizer of $w \in \boldsymbol{W}_m(\mathcal{C}_i)$ in $A$ is a maximal subgroup of $\mathrm{M}_{11}$ and the support designs constructed from these codes are given in Table 3.*

| m | $s := \lvert\mathbf{W}_m\rvert$ | Stabilizer | Maximal in $A$ | Design |
|---|---|---|---|---|
| 10 | 11 | $S_{10}$ | Yes | 1-$(55, 10, 2)$ |
| 18 | 55 | $S_9 \times S_2$ | Yes | 1-$(55, 18, 18)$ |
| 24 | 165 | $S_8 \times S_3$ | Yes | 1-$(55, 24, 72)$ |
| 25 | 462 | $S_6 \times S_5$ | Yes | 1-$(55, 25, 210)$ |
| 27 | 330 | $S_7 \times S_4$ | Yes | 1-$(55, 27, 162)$ |
| 28 | 330 | $S_7 \times S_4$ | Yes | 1-$(55, 28, 168)$ |
| 30 | 462 | $S_5 \times S_6$ | Yes | 1-$(55, 30, 252)$ |
| 31 | 165 | $S_8 \times S_3$ | Yes | 1-$(55, 31, 93)$ |
| 37 | 55 | $S_9 \times S_2$ | Yes | 1-$(55, 37, 37)$ |
| 45 | 11 | $S_{10}$ | Yes | 1-$(55, 45, 9)$ |

Table 3: *The stabilizers and designs from the code* $[55, 11, 10]$

**Proof**. If $w \in \mathcal{C}_1$, then the weight of $w$ equals $m\colon = i(11 - i)$ for some $i$. Moreover, the number of codewords of weight $m$ equals $v = \binom{n}{2}$. So the stabilizer of $w$ permutes $i$ and $11 - i$ words. Hence $St_A(w) = S_i \times S_{n-i}$, which is a maximal subgroup of $A_{11}$. For odd $m$, we have $55 - (55 - m)$. Hence $St_A(w)$ equals $St_A(w')$, where $w'$ is a codeword of even weight $55 - m$. The support designs constructed from the codewords of weight $m$ are of type 1-$(55, m, \lambda)$, where $\lambda$ is the number of codewords in $\mathbf{W}_m$ whose support contains 1. By Proposition 1, we have $\lambda = ms/55$, where $m$ and $s$ are given in the first two columns of Table 3. This completes the proof.

□

We devote the last part of this section to the codes of dimensions 44 and 45, respectively. We know that $\mathcal{C}_1 \oplus \mathcal{C}_2 = \mathcal{C}_4$, and the automorphism group of both codes is isomorphic to $S_{11}$. Here we only obtain the stabilizers for the codewords of weight $m \leq 7$. A similar approach can be used to construct the stabilizers of codewords for other values of $m$. If $w$ is a codeword of weight $m$, then the support of $w$ is the set of $m$ unordered 2-subsets $\{a, b\}$, where $1 \leq a < b \leq n$. So we can construct a graph $\Gamma(w)$ whose vertex-set is a subset of $\{1, 2, \ldots, 12\}$ and the edge-set is $Supp(w)$.

**Proposition 8.** *Let $w$ be a codeword of the code $\mathcal{C}_i$ $(i = 2, 4)$ of weight $m \leq 8$ and $A = \mathrm{Aut}(\mathcal{C}_i) \cong S_{11}$. The stabilizer of $w$ in $A$ and the designs constructed from $\mathcal{C}_2$ and $\mathcal{C}_4$ are given in Table 4.*

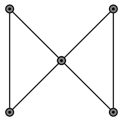
**Proof**. Let $w$ be a codeword of weight $m$. It is easy to see that the set $\mathcal{V}(m)$ of all codewords of $m$-cycle type is an orbit of the action. The stabilizer of an element $w \in \mathcal{V}(m)$ is isomorphic to the automorphism group of a 2-regular graph, which is $D_{2m}$, the dihedral group of order $2m$. On the other hand, $St_A(w)$ permutes all $11 - m$ points outside $\mathcal{V}(m)$. Therefore $St_A(w) \cong S_{11-m} \times D_{2m}$. By Remark 4, for $3 \leq m \leq 5$, every codeword of weight $m$ in ${\mathcal{C}_A}^{\perp}$ lies in $\mathcal{V}(m)$. Hence the stabilizers in these cases are isomorphic to $S_8 \times D_6$, $S_7 \times D_8$ and $S_6 \times D_{10}$, respectively. Now suppose that $m = 6$. If $w$ is of 6-cycle type, then $St_A(w) \cong S_5 \times D_{12}$. If $w$ is a sum of two codewords of 3-cycle type, then $St_A(w) \cong S_{11-6} \times (U_1{:}2)$, where $U_1$ is the automorphism group of the graph of two disjoint copies of $K_3$, i.e.,

$$St_A(w) \cong S_5 \times (D_6 \times D_6){:}2.$$

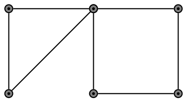
| m | no. of orbits | Orbit sizes | Stabilizer | Design |
|---|---|---|---|---|
| 3 | 1 | 165 | $S_8 \times D_6$ | 1-$(55, 3, 9)$ |
| 4 | 1 | 990 | $S_7 \times D_8$ | 1-$(55, 4, 72)$ |
| 5 | 1 | 5544 | $S_6 \times D_{10}$ | 1-$(55, 5, 504)$ |
| 6 | 3 | 27720 | $S_5 \times D_{12}$ | 1-$(55, 6, 3024)$ |
| - | - | 4620 | $S_5 \times [(D_3 \times D_3){:}2]$ | 1-$(55, 6, 504)$ |
| - | - | 6930 | $S_6 \times D_8$ | 1-$(55, 6, 756)$ |
| 7 | 4 | 118800 | $S_4 \times D_{14}$ | 1-$(55, 7, 15120)$ |
| - | - | 34650 | $S_4 \times D_6 \times D_8$ | 1-$(55, 7, 4410)$ |
| - | - | 83160 | $S_5 \times C_2 \times C_2$ | 1-$(55, 7, 10584)$ |
| - | - | 4620 | $S_6 \times D_{12}$ | 1-$(55, 7, 588)$ |

Table 4: *The stabilizers and designs from codes $\mathcal{C}_2$ and $\mathcal{C}_4$*

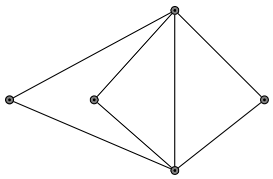
The final possibility for a codeword of weight 6 is that there exists one vertex in $\Gamma(w)$ of degree 4, while the other 4 vertices are of degree 2. In this case, we have $St_A(w) \cong S_6 \times U_2$, where $U_2$ is the automorphism group of the following graph, which is $D_8$.



Now assume that $m = 7$. We have an orbit of 7-cycle type whose stabilizer is $S_4 \times D_{14}$. Furthermore, if $w$ is a sum of two codewords $v_1 \in \mathcal{V}(3)$ and $v_2 \in \mathcal{V}(4)$, then we have $St_A(w) \cong S_4 \times D_6 \times D_8$. There are two more possibilities in this case: if there exists a codeword of weight 4 in $\Gamma(w)$, then $St_A(w) \cong S_5 \times U_3$, where $U_3 = C_2 \times C_2$ is the automorphism group of the following graph:



In addition, if there are two vertices of degree 4 in $\Gamma(w)$, then $St_A(w) \cong S_5 \times U_4$, where $U_4 = D_{12}$ is the automorphism group of the following graph:



So, the structure of the stabilizers for the codewords of weight $m \leq 7$ are as given in Table 2. The proof is now complete.

□

### 7.3. Binary codes of length 66

In this section, we study the binary codes of length 66 that admit $G$ as a permutation automorphism group. Here we can find two non-semisimple codes of dimension 11.

The permutation module $P_4(2)$ contains 16 proper non-zero submodules of dimensions:

$$1, 10, 11^3, 12, 21, 22, 44, 45, 54, 55^3, 56, 65,$$

where the submodules of dimensions 1, 10 and 44 are irreducible. So by Theorem 2, we have exactly 14 non-trivial $M_{11}$-invariant codes of length 66 (excluding the codes of dimensions 1 and 65), as listed in the statements of the following two theorems. By Proposition 3, we have $\dim \mathcal{C}_A = 10$ and $\dim \mathcal{C}_N = 11$. $\mathcal{C}_A \oplus \mathbf{1}$ is also another code of dimension 11, not isomorphic to $\mathcal{C}_N$.

**Proposition 9.** *The following binary codes of length 66 are invariant under $G = \mathrm{M}_{11}$.*

- $\mathcal{C}_1 = \mathcal{C}_A = [66, 10, 20]$, $\mathcal{C}_1^{\perp} = [66, 56, 3]$ *and*

$$\mathcal{WD}(\mathcal{C}_1) = \{0^1, 20^{66}, 32^{495}, 36^{462}\};$$

- $\mathcal{C}_2 = \mathcal{C}_1 \oplus \mathbf{1} = [66, 11, 20]$, $\mathcal{C}_2^{\perp} = [66, 55, 4]$ *and,*

$$\mathcal{WD}(\mathcal{C}_2) = \{0^1, 20^{66}, 30^{462}, 32^{495}, 34^{495}, 36^{462}, 46^{66}, 66^1\};$$

- $\mathcal{C}_3 = \mathcal{C}_N = [66, 11, 11]$, $\mathcal{C}_3^{\perp} = [66, 55, 3]$ *and,*

$$\mathcal{WD}(\mathcal{C}_3) = \{0^1, 11^{12}, 20^{66}, 27^{220}, 32^{495}, 35^{792}, 36^{462}\};$$

- $\mathcal{C}_4 = \mathcal{C}_B = [66, 11, 20]$, $\mathcal{C}_4^{\perp} = [66, 55, 4]$ *and*

$$\mathcal{WD}(\mathcal{C}_4) = \mathcal{C}_B = \{0^1, 20^{66}, 31^{792}, 32^{495}, 36^{462}, 39^{220}, 55^{12}\};$$

- $\mathcal{C}_5 = \mathcal{C}_N \oplus \mathbf{1} = [66, 12, 11]$, $\mathcal{C}_5^{\perp} = [66, 54, 4]$ *and*

$$\begin{aligned}\mathcal{WD}(\mathcal{C}_5) = \{&0^1, 11^{12}, 20^{66}, 27^{220}, 30^{462}, 31^{792}, 32^{495},\\ &34^{495}, 35^{792}, 36^{462}, 39^{220}, 46^{66}, 55^{12}, 66^1\}.\end{aligned}$$

*Moreover, for $1 \leq i \leq 5$, we have* $\mathrm{Aut}(\mathcal{C}_i) = \mathrm{Aut}(\mathcal{C}_i{}^{\perp}) = S_{12}$.

**Proof**. The code $\mathcal{C}_1$ is obtained from the binary row span of the adjacency matrix of $T(12)$. So by Proposition 3, we have $\mathcal{C}_1 = [66, 10, 20]$ and

$$\mathcal{WD}(\mathcal{C}_1) = \{0^1, 20^{66}, 32^{495}, 36^{462}\}.$$

Furthermore, by Remark 4, we have $\mathcal{C}_1^{\perp} = [66, 56, 3]$. The weight distribution of $\mathcal{C}_2 := \mathcal{C}_1 \oplus \mathbf{1}$ can be easily obtained from that of $\mathcal{C}_1$ by adjoining the all one-vector:

$$\mathcal{WD}(\mathcal{C}_2) = \{0^1, 20^{66}, 30^{462}, 32^{495}, 34^{495}, 36^{462}, 46^{66}, 66^1\}.$$

In particular, we have $\mathcal{C}_2 = [66, 11, 20]$. Moreover, by Remark 4, we have $\mathcal{C}_2^{\perp} = [66, 55, 4]$. Let $\mathcal{C}_3 = \mathcal{C}_N$, generated by the vertex-edge incidence matrix of the complete graph $K_{12}$; then by Proposition 3 we have $\mathcal{C}_3 = [66, 11, 11]$ and the weight distribution of this code is as follows:

$$\mathcal{WD}(\mathcal{C}_3) = \{0^1, 11^{12}, 20^{66}, 27^{220}, 32^{495}, 35^{792}, 36^{462}\}.$$

Again, using Remark 4, we have $\mathcal{C}_3^{\perp} = [66, 55, 3]$. It is also clear by Lemma 4 that $\mathcal{C}_B$ is neither isomorphic to $\mathcal{C}_2$ nor to $\mathcal{C}_N$. So $\mathcal{C}_4 = \mathcal{C}_B$ and by Lemma 4 we have:

$$\mathcal{WD}(\mathcal{C}_4) = \{0^1, 20^{66}, 31^{792}, 32^{495}, 36^{462}, 39^{220}, 55^{12}\};$$

It is also easy to check that $\mathcal{C}_4^{\perp} = [66, 55, 4]$. On the other hand, since $\mathbf{1} \notin \mathcal{C}_{\mathcal{N}}$, we deduce that $\mathcal{C}_5 := \mathcal{C}_N \oplus \mathbf{1}$ is a code of dimension 12. Hence, the weight distribution of $\mathcal{C}_5$ may be easily obtained. So, we have $\mathcal{C}_5 = [66, 12, 11]$ and $\mathcal{C}_5^{\perp} = [66, 54, 4]$.

□

**Proposition 10.** *Let $\mathcal{C}$ be a non-trivial binary code of length 66 invariant under $G = \mathrm{M}_{11}$. If $\mathcal{C}$ is not one of the codes constructed in Proposition 9, then $\mathrm{Aut}(\mathcal{C}) = M_{11}$ and $\mathcal{C}$ is one of the following codes:*

- $\mathcal{C}_6 = [66, 21, 16]$, $\mathcal{C}_6^{\perp} = [66, 45, 8]$;
- $\mathcal{C}_7 = [66, 22, 11]$, $\mathcal{C}_7^{\perp} = [66, 44, 8]$.

**Proof**. Consider the rank 4 action of $G$ on 66 points. Using [12, Proposition 1] we construct a 1-$(66, 15, 15)$ symmetric design such that the Mathieu group $M_{11}$ acts primitively on points and on blocks. Let $\mathcal{C}_7$ be the linear code of this design. Since $\mathcal{C}_7$ contains codewords of weight 15, then it is not one of the codes $\mathcal{C}_i$, $1 \leq i \leq 5$. Direct computations with MAGMA [3] yield that $\mathcal{C}_7$ is a code of dimension 22 and $\mathrm{Aut}(\mathcal{C}_7) = M_{11}$. We can also compute the minimum distance of $\mathcal{C}_7$. In particular, $\mathcal{C}_7 = [66, 22, 11]$. On the other hand, the submodule lattice of $P_4(2)$ shows that the code $\mathcal{C}_6$ of dimension 21 lies in the dual of the repetition code. Since the latter is an even weight code, we conclude that $\mathcal{C}_6$ consists of even weight codewords of $\mathcal{C}_7$, i.e., $\mathcal{C}_6 = [66, 21, 16]$. Using the weight distribution of these codes and the MacWilliams identities, we have $\mathcal{C}_6^{\perp} = [66, 45, 8]$ and $\mathcal{C}_7^{\perp} = [66, 44, 8]$. □

**Proposition 11.** *Let $w$ be a codeword of the code $\mathcal{C}_5$ of weight $m$ and $A = \mathrm{Aut}(\mathcal{C}_5) \cong S_{12}$. Then the action of $A$ on $\boldsymbol{W}_m(\mathcal{C}_5)$ is primitive. The stabilizer of $w \in \boldsymbol{W}_m$ in $A$ and the designs constructed from $\mathcal{C}_5$ are given in Table 5. Moreover, $St_A(w)$ are maximal subgroups of $A$.*

**Proof**. Let $w$ be a codeword of weight $m$ in $\mathcal{C}_5$. If $w \in C_N = \mathcal{C}_3$, then $m = i(i-1)$. Using an approach similar to that given in the proof of Theorem 7 we deduce for $i \neq 6$ that the stabilizer of $w$ in $S_{12}$ is isomorphic to $S_i \times S_{12-i}$. If $i = 6$, then $St_A(w)$ permutes two subsets of the $Supp(w)$ of size 6. So in the case $i = 6$, the stabilizer is $(S_6 \times S_{12-6})$:2. If $w \in \mathcal{C}_2$ or $\mathcal{C}_4$, then $St_A(w) = St(\mathbf{1} - w)$, and we can compute the stabilizers of the remaining codewords. Examining the list of maximal subgroups of $S_{12}$, using MAGMA [3], we observe that all these stabilizers are maximal subgroups of $S_{12}$. This completes the proof. □

| m | Stabilizer | Maximal in $S_{12}$ | Design |
|---|---|---|---|
| 11 | $S_{11}$ | Yes | 1-$(66, 11, 2)$ |
| 20 | $S_{10} \times S_2$ | Yes | 1-$(66, 20, 20)$ |
| 27 | $S_9 \times S_3$ | Yes | 1-$(66, 27, 72)$ |
| 30 | $(S_6 \times S_6)$:2 | Yes | 1-$(66, 30, 210)$ |
| 31 | $S_7 \times S_5$ | Yes | 1-$(66, 31, 372)$ |
| 32 | $S_8 \times S_4$ | Yes | 1-$(66, 32, 240)$ |
| 34 | $S_8 \times S_4$ | Yes | 1-$(66, 30, 255)$ |
| 35 | $S_7 \times S_5$ | Yes | 1-$(66, 35, 420)$ |
| 36 | $(S_6 \times S_6)$:2 | Yes | 1-$(66, 36, 252)$ |
| 39 | $S_9 \times S_3$ | Yes | 1-$(66, 39, 130)$ |
| 46 | $S_{10} \times S_2$ | Yes | 1-$(66, 46, 46)$ |
| 55 | $S_{11}$ | Yes | 1-$(66, 55, 10)$ |

Table 5: *The stabilizers of codewords and designs from the code* $\mathcal{C}_5 = [66, 12, 11]$

## 7.4. Codes of length 165

In this section, we obtain the binary codes of length 165 which are invariant under $\mathrm{M}_{11}$. The permutation module of dimension 165 over $\mathbb{F}_2$ has 156 submodules, and thus 156 binary linear codes[§]. We are not going to examine all these codes in this paper; however, we use a method which is a generalization of triangular graphs to find the weight distribution and the stabilizers of a code with parameters $[165, 11, 45]_2$.

Recall that a triangle in a graph $\Gamma$ is the subset $\{a, b, c\}$ of the vertices of $\Gamma$, where $a, b$ and $c$ are mutually adjacent. We state the following definition which is a generalization of the notion of a line graph.

**Definition 3.** *For a graph $\Gamma$, we define the graphs $\Gamma_{3,i}$ $(0 \leq i \leq 2)$ as follows. The set of vertices of these graphs is the set of triangles of $\Gamma$, and two triangles $\{a, b, c\}$ and $\{c, d, e\}$ in $\Gamma_{3,i}$ are adjacent if $|\{a, b, c\} \cap \{c, d, e\}| = i$. If $\Gamma$ is the complete graph $K_n$, then we write $\Gamma_3 := T_{3,i}(n)$.*

**Lemma 5.** *The graphs $K_{3,i}(n)$ is $r_i$-regular and $S_n$-invariant, where $r_0 = \binom{n-3}{3}$, $r_1 = 3\binom{n-3}{2}$ and $r_2 = 3(n-3)$. Moreover, they yield the following 1-designs:*

$$\mathcal{D}_{3,0}(n) = 1 - (\tbinom{n}{3}, \tbinom{n-3}{3}, \tbinom{n-3}{3})$$

$$\mathcal{D}_{3,1}(n) = 1 - (\tbinom{n}{3}, \tbinom{n-1}{2}, 3)$$

$$\mathcal{D}_{3,2}(n) = 1 - (\tbinom{n}{3}, n-2, 3)$$

**Proof**. The first part is obvious. So, we only need to find the design parameters. For $\mathcal{D}_{3,0}$, the block set is the set of

$$\{B_{rst}{:}1 \leq r < s < t \leq n\},$$

and a triangle $A = \{a, b, c\}$ lies in $B_{rst}$ if $\{r, s, t\} \cap \{a, b, c\} = \emptyset$. Hence, we have $\binom{n-3}{3}$ blocks, each of size $\binom{n-3}{3}$.

[§] The submodule lattice of $P_{165}(2)$ is given in https://goo.by/5Ze0u

Now consider the block set $\mathcal{B} = \{B_1, \ldots, B_n\}$ for $\mathcal{D}_{3,1}$. A triangle $A = \{a, b, c\}$ lies in $B_j$ if $j \in \{a, b, c\}$. Hence, the design has $n$ blocks and each block is of size $\binom{n-1}{2}$.

Finally, the block set of the design $\mathcal{D}_{3,2}$ is

$$\{B_{rs}{:}1 \leq r < s \leq n\},$$

and a triangle $A = \{a, b, c\}$ lies in $B_{rs}$ if $\{r, s\} \subset \{a, b, c\}$. Hence, we have exactly $\binom{n}{2}$ blocks, and each block is of size $n - 2$. The proof is now completed. □

In what follows, $\binom{x}{y}$ is assumed to be zero for $x < y$.

**Proposition 12.** *Let $\mathcal{C}_{3,1}(n)$ be a binary linear code constructed from the incidence matrices of the design $\mathcal{D}_{3,1}(n)$. Then the weight distribution of this code is as follows:*

$$\{k\binom{n-k}{2} + \binom{k}{3}^{\binom{n}{k}} : 0 \leq k \leq n\}$$

**Proof**. The generating matrix of the code contains $n$ codewords of weights $\binom{n-1}{2}$. The support of $c_i$ corresponds to the triangles whose vertex set contains $i$. Let $t_0$ denote the zero codeword $\mathbf{0}$ and $t_k$ for $1 \leq k \leq n$ the sum of $k$ generating codewords. It is clear that we can choose $t_k$ in $\binom{n}{k}$ different ways. It remains to compute the weight of $t_k$. Assume that $t_k = c_1, \ldots, c_k$. Then the support of $t_k$ corresponds to the triangles which have one or three elements in $\{1, \ldots, k\}$ as their vertices. If we fix $i \in \{1, \ldots, k\}$, then it is clear that there are exactly $\binom{n-k}{2}$ triangles which have $i$ as a vertex and the other 2 vertices lie outside $\{1, \ldots, k\}$. Hence, we have $k\binom{n-k}{2}$ triangles that have exactly one vertex in $\{1, \ldots, k\}$. Furthermore, we have $\binom{k}{3}$ triangles all of whose vertices lie in $\{1, \ldots, k\}$. Therefore, the weight of $t_k$ is equal to

$$k\binom{n-k}{2} + \binom{k}{3}.$$

Hence, the weight distribution of the code is computed. □

**Remark 6.** *It may sometimes happen that for two different values of* $0 < k_1 < k_2 < n$*, we have*

$$m := k_1\binom{n-k_1}{2} + \binom{k_1}{3} = k_2\binom{n-k_2}{2} + \binom{k_2}{3}$$

*In this case, we have $\binom{n}{k_1} + \binom{n}{k_2}$ codewords of weight $m$. So we should replace $m^{\binom{n}{k_1}}$ and $m^{\binom{n}{k_2}}$ by $m^{\binom{n}{k_1}+\binom{n}{k_2}}$.*

For $n = 11$, we have the following result which gives us one of the codes of length 165 invariant under $M_{11}$.

**Corollary 3.** *There exists a binary linear code $\mathcal{C}_{3,1}(11) = [165, 11, 45]$, with automorphism group $S_{11}$. The weight distribution of this code is*

$$\{0^1, 45^{11}, 72^{55}, 77^{330}, 80^{627}, 85^{627}, 88^{330}, 93^{55}, 120^{11}, 165^1\}.$$

The set of even weight codewords of $\mathcal{C}_{3,1}(11)$ is the irreducible code of dimension 10. Hence, $\mathcal{C}_{3,1}(11)$ is of type $1 \oplus 10$. It is worth mentioning that the situation stated in Remark 6 happens here. In fact, we have two types of codewords of weights 80 and 85, respectively. For example, if we put $k = 3$, then we obtain 165 codewords of weight 85, while for $k = 5$, we find 462 codewords of weight 85.

**Proposition 13.** *Let $w$ be a codeword of the code $\mathcal{C}_{3,1}(11)$ of weight $m$ and let $A = \mathrm{Aut}(\mathcal{C}_{3,1}(11)) \cong S_{11}$. Then the action of $A$ on $\boldsymbol{W}_m(\mathcal{C}_{3,1}(11))$ is primitive. The structure of the stabilizers of $w \in \boldsymbol{W}_m$ in $A$ and the designs constructed by $\mathcal{C}_{3,1}(11)$ are given in Table* 6*.*

**Proof**. Using the weight distribution of $\mathcal{C}_{3,1}(11)$, we can set the first two columns of Table 6. Let $\sigma \in St_A(w)$ be an element of the stabilizer of $w$. Since $w$ is a codeword, then it is a sum of $k$ generating codewords. We can assume that the set of indices is $K := \{1, 2, \ldots, k\}$. Each triangle in the support of $w$ has either 1 or 3 vertices in $K$. In the former case, $\sigma$ fixes every $i$ outside $K$ and moves every $i$ inside $K$. In the latter case, the converse applies. Therefore, the stabilizer is $S_k \times S_{n-k}$. The remainder of the proof is straightforward. □

| k | m | Orbit size | Stabilizer | Maximal in $S_{11}$ | Design |
|---|---|---|---|---|---|
| 1 | 45 | 11 | $S_{10}$ | Yes | 1-$(165, 45, 3)$ |
| 2 | 72 | 55 | $S_9 \times S_2$ | Yes | 1-$(165, 72, 24)$ |
| 3 | 85 | 165 | $S_8 \times S_3$ | Yes | 1-$(165, 85, 85)$ |
| 4 | 88 | 330 | $S_7 \times S_4$ | Yes | 1-$(165, 88, 176)$ |
| 5 | 85 | 462 | $S_6 \times S_5$ | Yes | 1-$(165, 85, 238)$ |
| 6 | 80 | 165 | $S_6 \times S_5$ | Yes | 1-$(165, 80, 80)$ |
| 7 | 77 | 330 | $S_7 \times S_4$ | Yes | 1-$(165, 77, 154)$ |
| 8 | 80 | 462 | $S_8 \times S_3$ | Yes | 1-$(165, 80, 224)$ |
| 9 | 93 | 55 | $S_9 \times S_2$ | Yes | 1-$(165, 93, 31)$ |
| 10 | 120 | 11 | $S_{10}$ | Yes | 1-$(165, 120, 8)$ |

Table 6: *The stabilizers and designs from the code $\mathcal{C}_{3,1}(11) = [165, 11, 45]$*

## Acknowledgement

The authors thank the referee for the helpful and constructive comments and suggestions.

## References

[1] R. Abbott, J. Bray, S. Linton, S. Nickerson, S. Norton, R. Parker, I. Suleiman, J. Tripp, P. Walsh, R. Wilson, *Atlas of finite group representations*, `http://brauer.maths.qmul.ac.uk/Atlas/v3/spor/M11/` (accessed May 2020).

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

[3] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system, I: The user language*, J. Symbolic Comput. **24**(1997), 235–265.

[4] P. J. Cameron, J. H. van Lint, *Designs, graphs, codes and their links*, Cambridge University Press, Cambridge, 1991.

[5] L. Chikami, J. Moori, B. G. Rodrigues, 2*-modular codes admitting the simple group* $L_3(4)$ *as an* 2*-automorphism group*, Util. Math. **95**(2014), 357–399.

[6] L. Chikami, J. Moori, B. G. Rodrigues, *Some irreducible* 2*-modular codes invariant under the symplectic group* $S_6(2)$, Glas. Mat. Ser. III **49**(2014), 235–262.

[7] L. Chikami, J. Moori, B. G. Rodrigues, 2*-modular representations of the alternating group* $\mathrm{A}_8$ *as binary codes*, Glas. Mat. Ser. III **47**(2012), 225–252.

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

[9] D. Gorenstein, *Finite simple groups: an introduction to their classification*, Plenum Press, New York, 1982.

[10] W. H. Haemers, R. Peeters, J. M. van Rijckevorsel, *Binary codes of strongly regular graphs*, Des. Codes Cryptogr. **17**(1999), 187–209.

[11] C. Jansen, K. Lux, R. Parker, R. Wilson, *An Atlas of Brauer Characters*, Oxford Scientific Publications, Clarendon Press, Oxford, 1995.

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

[13] J. D. Key, J. Moori, B. G. Rodrigues, *Permutation decoding for the binary codes from triangular graphs*, European J. Combin. **25**(2004), 113–123.

[14] W. Knapp, P. Schmid, *Codes with prescribed permutation automorphism*, J. Algebra **67**(1980), 415–435.

[15] J. Moori, B. G. Rodrigues, *A self-orthogonal doubly even code invariant under* $\mathrm{M^cL}$:2, J. Combin. Theory Ser. A **110**(2005), 53–9.

[16] B. G. Rodrigues, A. Saeidi, *On linear codes invariant under finite primitive permutation groups with non-trivial Schur multiplier*, in preparation.

[17] A. Vardy, *The intractability of computing the minimum distance of a code*, IEEE Trans. Inform. Theory **43**(1997), 1757–1766.