Some Non-Isomorphic Binary Codes of Degree 253 Related to Mathieu Group M_{23}

VINCENT NYONGESA MARANI
Mathematics Department, Kibabii University, Bungoma, Kenya

Abstract- In this paper, we determine some non-isomorphic linear binary codes of degree 253 related to Mathieu group M_{23}. We discuss their properties. We further determine and discuss some properties of designs related to these codes

Indexed Terms- Non-Isomorphic Binary Codes, Mathieu Group M_{23}.

I. INTRODUCTION

M_{23} is the point stabilizer in M_{24}. It is a 3-transitive permutation group on 23 objects. It is the automorphism group of the Steiner system S (4,7,23), whose 253 heptads arise from the octads of S (5,8,24) containing the fixed point. It is also described as the automorphism group of the binary Golay code of dimension 12, length 23, and minimal weight 7, or as a subcode of even weight words [1].

There are seven primitive permutation representations of degree 23, 253, 253, 506, 1288, 1771, and 40320 respectively [1]. The seven primitive permutation representations are as shown in the table 1, where column one gives the structure of the maximal subgroups; two gives the degree (the number of cosets of the point stabilizer); three gives the order of the maximal subgroups; four gives the number of orbits of the point-stabilizer, and the rest give the length of the orbits.

Table 1: Primitive permutation representations of M_{23}.

Max. Sub	Degree	Order	#	Length	Length	Length	Length	Length
M_{22}	23	443520	2	22				
$L_3(4)$: 2_2	253	40320	3	42	210			
24 : $A7$	253	40320	3	112	140			
A_8	506	20160	4	15	210	280		
M_{11}	1771	7920	8	20	60	90	160	480(3)
$2^4 : 3 \times A_5 : 2$	1288	7920	4	165	330	792		
23 : 11	40320	253	164	23(4)	253(159)			

The action of G on geometrical objects points, duad, heptad, octad, dodecad, and triad respectively describes the primitive representations. The elements of each degree generate a permutation module over F. We determine orbits of the point stabilizer through cosset action of a group G on its maximal subgroups.
In this paper, we enumerate and classify all G-invariant codes preserved by primitive group of degree 253 using modular representation method. We study the properties of some binary codes of small dimensions. We determine symmetric 1-designs from the primitive group G.

II. THE 1^{ST} REPRESENTATION OF DEGREE 253

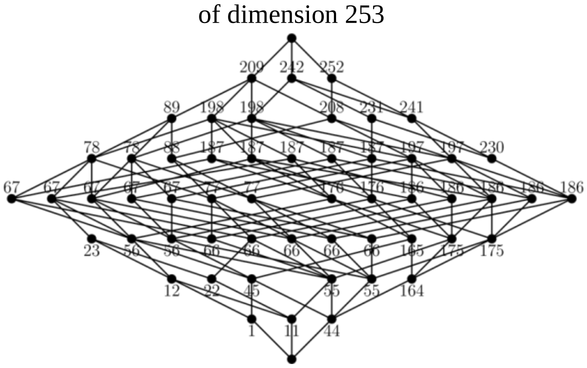
Let G be the Mathieu group M_{23}. Group G acts on a duad to generate the stabilizer $L_4(4)$: 2. The stabilizer is a maximal subgroup of degree 253 in G. The group G acts on this maximal subgroup over F2 to form a module of dimension 253 invariant under G. The module breaks down into three completely irreducible parts of length 1, 11, 44, 44 and 120 with multiplicities 1, 2, 2, 1, 1 and 1 respectively. The submodules of dimension 1, 11 and 44 are irreducible. The module splits into 54 maximal submodules. These submodules are the dimensions of the codes related with the module of dimension 253 invariant under *G*. Table 2 shows the Submodules from a Module of dimension 253. Column *k* represents the dimension of the submodule and # the number of the submodules of each dimension.

Table 2: Submodules from a Module of dimension 253

k	#	k	#	k	#	k	#
0	1	55	2	164	1	208	1
1	1	56	2	165	1	209	1
11	1	66	5	175	2	230	1
12	1	67	5	176	2	231	1
22	1	77	2	186	5	241	1
23	1	78	2	187	5	242	1
44	1	88	1	197	2	252	1
45	1	89	1	198	2	253	1

The submodule lattice is as shown in Figure 1

Figure 1: Submodule Lattice of Permutation Module of dimension 253



We discuss three non-trivial submodules of small dimensions 11, 12 and 22. The binary linear codes from these representations are [253, 11,112], [253, 12,112] and [253, 22, 22]. We make some observations about the properties of these codes. These properties are examined with certain detail in Proposition 2.1.

Proposition 2.1. *Let G be the Mathieu group M_{23} and $C_{253,1}$, $C_{253,2}$, $C_{253,3}$, $C_{253,4}$ be nontrivial binary code of dimension 11, 12, 22, 23 respectively obtained from the permutation module of degree 23. Then the following holds;*

i. *$C_{253,1}$ is self-orthogonal doubly even projective [253, 11,112] binary code. [253, 242,3] is the dual code of $C_{253,1}$. Furthermore $C_{253,1}$ is irreducible and Aut ($C_{253,1}$) $\simeq M23$.*

ii. *$C_{253,2}$ is projective [253, 12,112] binary code. [253, 241, 4] is the dual code of $C_{253,2}$. Furthermore $C_{253,2}$ is decomposable and Aut ($C_{253,2}$) $\simeq M_{23}$.*

iii. *$C_{253,3}$ is self-orthogonal singly even projective [253, 22,22] binary code.* $[253,231,3]_2$ *is the dual code of $C_{253,3}$. Furthermore Aut($C_{253,1}$) $\simeq S_{253}$.*

proof

i. The submodule 11 represents the dimension of binary code $C_{253,1}$. From this submodule we determine the binary linear code $[253, 11,112]_2$. The polynomial of this code is $W(x) = 1 + 253x^{112} + 506x^{120} + 1288x^{132}$. From the polynomial we deduce that the weight of this codewords are divisible by 4. Hence $C_{253,1}$ is doubly even. The minimum weight of $C^{\perp}_{253,1}$ code is 3. Hence $C_{253,1}$ is projective. From the lattice structure the submodule 11 cannot be broken down which implies that $C_{23,1}$ is irreducible. For the structure of the automorphism group, let $G \simeq Aut(C_{253,1})$. G has only one Composition factor M_{253} and the order of G is 10200960. This implies that $G = M_{23}$. Since $M_{23} \subseteq G$, we conclude that $G \simeq M_{23}$

ii. The submodule 12 represents the dimension of binary code $C_{253,2}$. From this submodule we determine the binary linear code $[253, 12,112]_2$. The partial weight enumerator of this code is $W(x) = 1 + 253x^{112} + 506x^{120} + 1288x^{121} + \ldots$ The minimum weight of $C^{\perp}_{253,2}$ code is 4. Hence $C_{253,2}$ is projective. From the lattice structure the submodule 12 is a direct sum of 11 and 1 which implies that $C_{23,2}$ is irreducible. For the structure of the automorphism group, let $G \simeq Aut(C_{253,2})$. G has only one Composition factor M_{253} and the order of G is 10200960. This implies that $G = M_{23}$. Since $M_{23} \subseteq G$, we conclude that $G \simeq M_{23}$

iii. The submodule 22 represents the dimension of binary code $C_{253,3}$. From this submodule we determine the binary linear code $[253, 22,22]_2$. The polynomial of this code is $W(x) = 1 + 23x^{22} + 253x^{42} + 1771x^{60} + 8855x^{76} + 33649x^{90} +$

$100947x^{102}$ + $245157x^{112}+490314x^{120}+817190x^{126}+1144066x^{130}$ $+1352078x^{132}$. We deduce that the weights of this codewords are divisible by 2. $C_{253,2}$ is singly even. The weight of $C^{\perp}_{253,3}$ code is 3. Hence $C_{253,3}$ is projective. For the structure of the automorphism group, let $G \simeq Aut(C_{253,1})$. G has two Composition factors M_{253} and Z2. This implies that $G = S_{253}$. We conclude that $G \simeq M_{23}$

I. Designs of Codewords of Minimum Weight in $C_{253,i}$ Code

We determine designs of codewords of minimum weight in $C_{23,i}$. Table 3 shows Deigns of codewords in $C_{253,i}$ where column one represents the code $C_{23,i}$ of minimum weight m and column two gives the parameters of the t-designs D_{wm} . In column three we list the number of blocks of D_{wm}, four tests whether or not a design D_{wm} is primitive .

Table 3: Deigns of codewords in $C_{253,i}$

m	Dw_m	No of Blocks	primitive
112	1-(253, 112, 112)	253	yes
22	1-(253, 22, 2)	23	yes
3	1-(253, 3, 21)	1771	yes
4	1-(253, 4, 1260)	79695	yes

Remark 2.2. *From the results in table 5.6 we observe that Aut(C) is primitive on* D_{wm}

II. Symmetric 1- Designs

In this section we consider G to be the simple Mathieu group M_{253} and examine symmetric 1-design invariant under G constructed from orbits of the rank - 3 permutation representation of degree 253. Table 4 shows Symmetric 1-Design where column one represents the 1-design D_k of orbit length k, column two gives the orbit length, t column three shows the parameters of the symmetric 1-design D_k and column four gives the automorphism group of the design.

Table 4: Symmetric 1-Design

Design	orbit length	parameters	Automorphism Group
D42	42	1-(253,42,42)	$A_{23}:2$
D210	210	1-(253,210,210)	$A_{23}:2$
D43	43	1-(253,43,43)	$A_{23}:2$
D211	211	1-(253,211,211)	$A_{23}:2$
D252	252	1-(253,252,252)	$A_{253}:2$

Proposition 2.3. *Let G be the mathieu simple group* M_{23}*, and* Ω *the primitive G-set of size 253 defined by the action on the cosets of* M_{23}*. Let* $\beta = \{M^g: g \in G\}$ *and* $D_k = (\Omega,\beta)$.

Then the following hold:

i. D_k *is a primitive symmetric* $1-(23,|M|,|M|)$ *design.*
ii. $Aut(D_k) \simeq A_{23}:2$ *for some k= 42, 210, 43, 211*

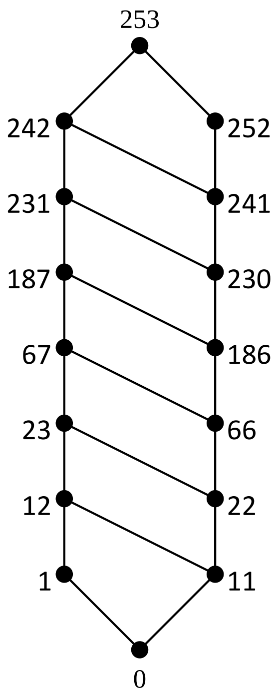
Proof

i. It is clear that G acts as an automorphism group, primitive on points and on blocks of the design and so $G \subseteq Aut(D_k)$.
ii. The composition factors of $Aut(D_k)$ are Z_2 and A_{23} and so $Aut(D_k)= A_{23}:2$. This implies that $Aut(D_k) \cong A_{23}:2$

III. The 2nd Representation of Degree 253

Let G be the Mathieu group M_{23}. Group G acts on heptad to generate a maximal subgroup of degree 253 in G. The group G acts on the maximal subgroup over F2 to form a module of dimension 253 invariant under *G*. The module breaks down into three completely irreducible parts of dimensions 1, 11, 44, 44 and 120 with multiplicities 1, 2, 2, 1 and 1 respectively. The two irreducible submodules are of dimension 1 and 11. The module splits into 14 submodules of dimension 1, 11, 12, 22, 23, 66, 67, 186, 187, 230, 231, 241, 242 and 252. These submodules are the dimensions of the codes related with the module of dimension 253. The submodule lattice is as shown in Figure 2

Figure 2: Submodule lattice of permutation module of dimension 253



We discuss three non-trivial submodules of small dimensions 11, 12 and 22 . The binary linear codes from these representations are [253, 11,112], [253, 12, 77] and [253, 22, 88]. We make some observations about the properties of these codes. These properties are examined with certain detail in Proposition 3.1.

Proposition 3.1. *Let G be the Mathieu group* M_{23} *and* $C_{253,1}$, $C_{253,2}$, $C_{253,3}$, $C_{253,4}$ *be nontrivial binary code of dimension 11, 12, 22, 23 respectively obtained from the permutation module of degree 253. Then the following holds;*

i. $C_{253,1}$ *is self-orthogonal, doubly even and projective [253, 11,112] binary code . [253, 242, 4] is the dual code of* $C_{253,1}$ *. Furthermore* $C_{253,1}$ *is irreducible and Aut(* $C_{253,1}$*)* $\simeq M23$.

ii. $C_{253,2}$ *is [253, 12,77] binary code. [253, 241, 4] is the dual code of* $C_{253,2}$ *. Furthermore* $C_{253,2}$ *is decomposable and Aut(* $C_{253,2}$*)* $\simeq M_{23}$.

iii. *iii* $C_{253,3}$ *is self-orthogonal, doubly even and projective [253, 22,88] binary code . [253, 231, 5] is the dual code of* $C_{253,3}$ *. Furthermore* $C\perp_{253,3}$ *is 3-error correcting code and Aut(*$C253,3$*)* $\simeq M23$.

Proof

i. The submodule 11 represents the dimension of binary code $C_{253,1}$. From this submodule we determine the binary linear code $[253, 11,112]_2$. The polynomial of this code is $W(x) = 1 + 253x^{112} + 1771x^{128} + 23x^{176}$. We deduce that the weight of codewords are divisible by 4. $C_{253,1}$ is doubly even. The weight of $C^{\perp}_{253,1}$ code is 4. Hence $C_{253,1}$ is projective. From the lattice structure the submodule 11 is trivial which implies that $C_{23,1}$ is irreducible. For the structure of the automorphism group, let $G \simeq Aut(C_{253,1})$. G has only one composition factor M_{23} and the order of G is 10200960. This implies that $G = M_{23}$. Since $M_{23} \subseteq G$, we conclude that $G \simeq M_{23}$

ii. The submodule 12 represents the dimension of binary code $C_{253,2}$. From this sub-module we determine the binary linear code $[253, 12,112]_2$. The weight of $C^{\perp}_{253,2}$ code is 4. Hence $C_{253,2}$ is projective. From the lattice structure the submodule 12 is a direct sum of 11 and 1 which implies that $C_{23,2}$ is decomposable. For the structure of the automorphism group, let $G \simeq Aut(C_{253,2})$. G has only one composition factor M_{23} and the order of G is 10200960. This implies that $G = M_{23}$. Since $M_{23} \subseteq G$, we conclude that $G \simeq M_{23}$

iii. The submodule 22 represents the dimension of binary code $C_{253,3}$. From this submodule we determine the binary linear code $[253, 22,88]_2$. From weight distribution, $C_{253,3}$ is doubly even. The weight of $C^{\perp}_{253,3}$ code is 5. For the structure of the automorphism group, let $G \simeq Aut(C_{253,3})$. G has only one composition factor M_{23} and the order of G is 10200960. This implies that $G = M_{23}$. Since $M_{23} \subseteq G$, we conclude that $G \simeq M_{23}$

IV. Designs of codewords of minimum weight in $C_{253,i}$

We determine designs of codewords of of minimum weight in $C_{253,i}$. Table 5.8 shows Deigns of codewords of minimum weight in $C_{253,i}$ where column one represents the code $C_{23,i}$ of weight m and column two gives the parameters of the 1-designs D_{wm} . In column three we list the number of blocks of D_{wm}, four tests whether or not a design D_{wm} is primitive.

Table 5: Deigns of codewords of minimum weight in $C_{253,i}$

Code	m	Designs	No of Blocks	Automorphism group	Primitive
C253,1	112	1-(253, 112, 112)	253	M_{23}	Yes
C253,2	77	1-(253, 77, 7)	23	M_{23}	yes
C253,3	88	1-(253, 88, 448)	1288	M_{23}	yes

Remark 3.2. *From the results in table 5, we observe that Aut(C) is primitive on all designs of minimum weight.*

Maximal subgroups of degree 23, 253, and 1288 in table 1 are stabilizers in M_{23} and the blocks 23, 253, and 1288 in table 5 represents codewords of weight 77, 88 and 112 respectively.

V. Symmetric 1- Designs

In this section we take G to be the Mathieu group M_{23} and examine symmetric 1-design invariant under G constructed from orbits of the rank - 3 permutation representation of degree 253.

Table 5.9 shows Symmetric 1-Design where column one represents the 1-design D_k of orbit length k, the column two gives the orbit length, column three shows the parameters of the symmetric 1-design D_k and column four gives the automorphism group of the design. Table 6: Symmetric 1-Design

Design	orbit length	parameters	Automorphism Group
D112	112	1-(253,112,112)	M_{23}
D140	140	1-(253,140,140)	M_{23}
D113	113	1-(253,113,113)	M_{23}
D141	141	1-(253,141,141)	M_{23}
D252	252	1-(253,252,252)	$A_{253}:2$

Proposition 3.3. *Let G be the mathieu simple group M_{23}, and Ω the primitive G-set of size 253 defined by the action on the cosets of M_{23}. Let $\beta = \{M^g : g \in G\}$ and $D_k = (\Omega,\beta)$.Let M=[112,140,113,141] and N=[252]. Then the following hold:*

i. *D_k is a primitive symmetric* $1-(23,|M|,|M|)$ *design.*
ii. *For $k \in M$, $Aut(D_k) \simeq M_{23}$*
iii. *For $k \in M$, $Aut(D_k) \simeq A_{253}:2$*

Proof

i. It is clear that G acts as an automorphism group, primitive on points and on blocks of the design and so G ⊆ Aut(D_k).
ii. Aut(D_k) has only one composition factor M_{23}. This implies that $Aut(D_k)$ u M_{23}
iii. The composition factors of Aut(D_k) are Z_2 and A_{253} This implies that $Aut(D_k) \simeq A_{253}:2$

CONCLUSION

Let G be the primitive group of degree 23 of M_{23} and C a linear code admitting G as an automorphism group. Then the following holds:

a) There exist a self-orthogonal irreducible doubly even projective code.
b) There exist a set of self-orthogonal doubly even projective codes.
c) There exist a set of Primitive Designs related to M_{23}.
d) Aut(C) $\simeq M_{23}$
e) Aut(C) is primitive on all t-designs held by the support of codewords of minimum weight related to M_{24}.

REFERENCES

[1] R. A. Wilson, R. A. Parker, and J. N. Bray, Atlas of Finite Group Representations, http://brauer.maths.qmul.ac.uk/Atlas/clas/S62/.

[2] V.N. Marani (2019), Some Linear Codes, Graphs and Designs From Mathieu Groups M24 and M23. Ph.D. Thesis, Kibabii University.

[3] B. G. Rodrigues (2003), Codes of Designs and Graphs from Finite Simple Groups, Ph.D. thesis, University of Natal, Pietermaritzburg,