The Binary Linear Codes of Mathieu Group M_{24}

Vincent Nyongesa Marani[1]Lucy Chikamai[2]& Prof. Shem Aywa [3]
1,2,3-Kibabii University
Corresponding e-mail:

Abstract
We use coding theory to study the internal structure of simple groups. Coding theory deals with methods of constructing and analyzing error-correcting codes. In this paper, we construct all binary linear codes from M_{24} and determine their properties. We link these codes to designs and graphs.We develop the algorithm that determine these codes and add the algorithm to the Magma software.

Mathematics Subject Classification: 05B05, 20D45, 94B05

Key words: Binary codes, designs and Modules.

1.0 Introduction
Finite simple groups have been classified as cyclic groups with prime order, alternating groups of degree at least 5, a simple group of Lie type and ,the 26 sporadic simple groups based on external structures .This classification took many years and involved many researchers. The current research is about these classified groups and their internal structure. We use coding theory to study the internal structure of simple groups. Coding theory emerged following the publication of Shannon's seminal 1948 paper [1]. Coding theory deals with methods of constructing and analyzing error-correcting codes.

In a series of 3 lectures given at the NATO Advanced Study Institute "Information Security and Related Combinatorics" held in Croatia, the author discussed two methods for constructing codes and designs for finite groups (mostly simple finite groups) [3]. The first method dealt with construction of symmetric 1-designs and binary codes obtained from the action on the maximal subgroups, of a finite group G. The second method introduces a technique from which a large number of non-symmetric 1-designs could be constructed. Using these methods they constructed codes from Janko groups, J_1 and J_2 and from the sporadic group $CO_2$of Conway.
Three methods have been used for constructing codes and designs for finite groups [3]. The first method dealt with construction of symmetric 1-designs and binary codes obtained from the action on the maximal subgroups, of a finite group G. The second method introduces a technique from which a large number of non-symmetric 1-designs could be constructed. In the third method, each primitive representation of a given permutation group G, meat-axe and magma are used to construct the associated permutation modules and subsequently a chain of its maximal submodules.
In the 19th century E. Mathieu discovered and studied five multiply transitive permutation groups. The groups are called the Mathieu groups and it turned out that all five are simple. These remarkable groups are constructed in [2], with special focus on the small Mathieu groups M_{11} andM_{12}. All maximal subgroups of M_{11} and M_{12} are described and classified. It is also shown that the other Mathieu groups are subgroups of M_{24}. Finally the simplicity of the five Mathieu groups is proved.
Though codes have been constructed from M_{24}, only small degree of 24 was considered.In this paper we are interested in constructing codes of M_{24} group using large degrees. We examine the properties of these sub modules as codes and present their weight distributions. Using Assmus-Mattson theorem and the transitivity of the groups, we shall determine some designs or graphs that are defined by code words of

several weights in the codes and we use the properties of these designs or graphs and their geometry to gain some insight into the nature of some classes of codewords, mainly those of minimum weight.

2.0 Literature Review

2.1 Introduction

In this section we discuss some of the basic concepts that are used in this proposal.

2.2 Modular Representations

Let F be a field of characteristic p and let V be an F vector space. Let G be a finite group of order n. Then we define a linear representation V of G over F as a homomorphism $\emptyset: \mathrm{G} \rightarrow \mathrm{GL(V)}$. We say that the representation is faithful if $\emptyset$ is injective. Representations are similar or equivalent if they correspond to isomorphic FG-modules. A module M is irreducible or simple if the only submodules are M and 0. If not then M is reducible. M is decomposable if there exist nonzero submodules M_1 and M_2 such that $\mathrm{M} = \mathrm{M}_1 \oplus \mathrm{M}_2$. M is completely reducible if it can be written as the direct sum of irreducible submodules.[4]

2.3 Binary Linear Codes

A binary linear (n, k) code C is a k-dimensional subspace of the n-dimensional vector space over $\mathrm{GF}(2)$. A code C of length n, dimensionk, and minimum weight d, is denoted by $[\mathrm{n}, \mathrm{k}, \mathrm{d}]$. The Hamming weight w(c) of a codeword c is the number of nonzero components in the code word. The Hamming distance between two codewords d(x; y) is the number of places in which the codewords x and y differ. The minimum (Hamming) distance of a code $C$is the minimum distance between any two codewords in the code. In general, a code that has minimum distance d can be used to either detect up to $\mathrm{d} - 1$ errors or correct up to $[(\mathrm{d} - 1)/2]$ errors. [4]

A code is called self orthogonal if $c \sqsubseteq c^{\perp}$. All the weights in a binary self orthogonal code must be even since every vector must be orthogonal to itself. A code is doubly even if all the codewords have weights divisible by 4. A code is self-dual if$c = c^{\perp}$. If c is an [n, k] code, then $c^{\perp}$is an [n, n-k] code.

2.4 Designs

An incidence structure$\mathrm{D} = (\mathrm{P}, \mathrm{B}, \mathrm{I})$, with point setP, block set B and incidence I is a $t - (v, k, \lambda)$ design, if $|P| = v$, every block $\beta \in B$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. A design D is symmetric if it has the same number of points and blocks. A $\mathrm{t} - (\mathrm{v}, \mathrm{k}, 1)$ design is called a Steiner System. A $2 - (\mathrm{v}, 3, 1)$ Steiner system is called a Steiner Triple System. A $\mathrm{t} - (\mathrm{v}, 2, \lambda)$ design D can be regarded as a graph with ρ as points and β as edges.[4]

3.0 Methodology

In this paper, we use the following analytical methods:

2 Generate the permutation representations of M_{24} of degree 216 from the Atlas of finite groups.

3 Use Magma software to:

- I) Determine the permutation module of the permutation representation of degree 216
- II) Use permutation modules to determine dimensions of all maximal submodules of the permutation module.
- III) List all the maximal submodules of the permutation modules.
- IV) Sort out the maximal submodules by removing the Isomorphic copies.
- V) Derive codes from the maximal submodules and then determine the properties of these codes
- VI) Link these codes to some designs or graphs.

4.0 Results

4.1 The 24-Dimensional Representation

We generate the permutation group M_{24} from the atlas of finite groups using a permutation representation of degree 276.The permutation module of this group is a Gmodule of dimension 276. By recursively determining a chain of maximal submodules of the permutation module we find that the permutation module has three maximal submodules of dimension 23, 12 and 1 respectively. From the $12-$dimensional maximal module we derive a linear code $C_{24,1} = [24, 12, 8]_2$. $C_{24,1} = [24, 12, 8]_2$is a self dual, self orthogonal, doubly even and projective code. This code is an extended golay code which was originally constructed using design theory. The design held by this code is S(5,8,24).

4.2 The 276-Dimensional Representation

We generate the permutation group M_{24} from the atlas of finite groups using a permutation representation of degree 276.The permutation module of this group is a Gmodule of dimension 276. By recursively determining a chain of maximal submodules of the permutation module we find that the permutation module has 26 maximal submodules after eliminating the isomorphic copies. For any permutation representation of degree n we denote the determined codes by $C_{n,1}$,$C_{n,2}$…….. $C_{n,r}$, if r codes are obtained and by $C_{n,}$ if we only have one code upto isomorphism. The codes and their properties are shown in the table 1.

Table 1: Codes and their codes

Code $C_{n,r}$	Parameters	Dual()$C_{n,r}$	Hull($C_{n,r}$)	Self Dual	Self Orthogonal
$C_{26,1}$	[276,265,3]	[276,11,128]	[276,11,128]	False	False
$C_{26,2}$	[276,275,2]	[276,1,276]	[276,1,276]	False	False
$C_{26,3}$	[276,22,7]	[276,55]	[276,55]	False	False
$C_{26,4}$	[276,254,3]	[276,22,44]	[276,22,44]	False	False
$C_{26,5}$	[276,264,4]	[276,12,44]	[276,12,44]	False	False
$C_{26,6}$	[276,210]	[276,66]	[276,66]	False	False
$C_{26,7}$	[276,220]	[276,56]	[276,56]	False	False
$C_{26,8}$	[276,253,4]	[276,23,44]	[276,23,44]	False	False
$C_{26,9}$	[276,199]	[276,77]	[276,77]	False	False
$C_{26,10}$	[276,209]	[276,67]	[276,66]	False	False
$C_{26,11}$	[76,252,4]	[276,24,23]	[276,22]	False	False
$C_{26,12}$	[276,79]	[276,197]	[276,77]	False	False
$C_{26,13}$	[276,198]	[276,78]	[276,77]	False	False
$C_{26,14}$	[276,208]	[276,68]	[276,66]	False	False
$C_{26,15}$	[276,68,23]	[276,208]	[276,66]	False	False
$C_{26,16}$	[276,78]	[276,198]	[276,77]	False	False
$C_{26,17}$	[276,197]	[276,79]	[276,77]	False	false
$C_{26,18}$	[276,24,23]	[276,252]	[276,22]	False	False
$C_{26,19}$	[276,67]	[276,209]	[276,66]	False	False
$C_{26,20}$	[276,77]	[276,199]	[276,77]	False	True
$C_{26,21}$	[276,186]	[276,90]	[276,66]	False	False
$C_{26,22}$	[276,23,44]	[276,253]	[276,22]	False	False
$C_{26,23}$	[276,66]	[276,210]	[276,66]	False	True
$C_{26,24}$	[276,22,44]	[276,254]	[276,22,44]	false	True
$C_{26,25}$	[276,55]	[276,221]	[276,55]	False	True
$C_{26,26}$	[276,11,128]	[276,265]	[276,11,128]	False	True

Theorem 1

$C_{26,1}^{\perp} = C_{26,26}$

$C_{26,3}^{\perp} = C_{26,25}$

$C_{26,4}^{\perp} = C_{26,24}$

$C_{26,6}^{\perp} = C_{26,23}$

$C_{26,8}^{\perp} = C_{26,22}$

$C_{26,9}^{\perp} = C_{26,20}$

$C_{26,10}^{\perp} = C_{26,19}$
$C_{26,11}^{\perp} = C_{26,18}$

PROOF

As shown by magma

Designs Held by Codes

No	Design	Simple	Uniform	Balanced	Complete	Symmetric	Steiner
1	1-(276,3,22)	True	True	True	No	No	No
2	2-(276,2,1)	True	True	True	True	No	True
4	1-(276,3,22)	True	True	True	No	No	No
5	1-(276,4,1617)	True	True	True	No	No	No
8	1-(276,4,462)	True	True	True	No	No	No
11	1-(276,4,462)	True	True	True	No	No	No
18	1-(276,23,2)	True	True	True	No	No	No
22	1-(276,44,44)	True	True	True	No	No	No
24	1-(276,44,44)	True	True	True	No	No	No
26	1-(276,128,352)	True	True	True	No	No	No

References

1. Cannon, J., Steel, A., & White, G. (2006). Linear codes over finite fields. Handbook of Magma Functions, 2, 3951-4023.
2. Chikamai, L., Moori, J., & Rodrigues, B. G. (2012). 2-modular representations of the alternating group A8 as binary codes. GLASNIK MATEMATICKI, 47(67), 225-252.
3. Key, J. D., and J. Moori. (2012) "Some Irreducible Codes Invariant under the Janko Group, J_1 or J_2." JCMCC-Journal of Combinatorial Mathematics and Combinatorial Computing 81 165.
4. Smith, K. J. C., & Durham, G. N. D. A. D. (1968). An application of incomplete block designs to the construction of error-correcting codes. University of North Carolina. Department of Statistics.