Classification of Some Internal Structures of Degree 120 Related To a Group of Extension$O_8^+(2)$: 2

JANET LILIAN MAINA[1], JOHN WANYONYI MATUYA[2], EDWARD NJUGUNA[3], VINCENT NYONGESA MARANI[4]

[1, 2, 3] *Department of Mathematics and Physical Sciences, Maasai Mara University.*

[4] *Department of Mathematics and Physical Sciences, Kibabii University*

Abstract- ***This paper uses the modular representation method to classify the internal structures of degree 120 related to a group of extension,$O_8^+(2)$: 2.Specifically, we determine the number of binary linear codes and construct their lattice structure, as well as investigate the properties of some linear codes and designs of minimum weights. Our findings reveal that there are 12 binary linear codes, consisting of 4 doubly even codes, 4 projective codes, 2 irreducible codes, and 2 decomposable codes. We also identify 2 primitive 1-designs of minimum weight. The results demonstrate the potential benefits of using linear codes and designs from finite groups of extension with modular representation methods, such as improved error correction, increased data storage capacity, improved security, efficient designs, and improved computational efficiency. However, it is important to note that this topic can be complex and technical, and we recommend that stakeholders collaborate with experts in the field to ensure the accuracy and reliability of the information being used. Overall, this study contributes to the understanding of the modular representation method and its applications in coding theory and related fields.***

I. INTRODUCTION

This study focuses on the modular representation method in coding theory, which is a technique used to construct error-correcting codes. The method involves representing elements of the code as vectors over a finite field and using modular arithmetic to manipulate these vectors. Linear codes and designs from groups of extensions using modular representation methods can address a variety of issues and challenges in coding theory and design theory. This study aims to develop algorithms and computational methods for constructing and analyzing linear codes and designs from groups of extension using the modular representation method. Specifically, the study aims to enumerate linear codes from degree 120 related to a group of extension$O_8^+(2)$: 2,construct a lattice diagram of linear codes obtained from degree 120 related to the group of extension, and investigate the properties of linear codes and designs constructed using the modular representation method. The significance of the study lies in the fact that linear codes and designs from maximal subgroups using the modular representation method have many theoretical and practical applications in coding theory, combinatorial mathematics, cryptography, and group theory. Overall, this study contributes to the understanding of the modular representation method and its applications in various fields.

2. Construction of binary linear Codes from Finite Groups

Our point of interest is finding binary linear codes from the primitive permutation representations. Maximal subgroups are expressed as primitive permutation representations in the atlas of finite group representations. For each primitive permutation representation of a group G we use atlas of finite groups and Magma software to generate permutation module over $\mathbb{F}_2$.The permutation module is decomposed into submodules. The submodules represent the dimension of linear codes. These submodules are used to construct lattice diagram. The lattice diagram is used to point out some properties of the submodules. Finally, binary linear codes (n, k, d) are obtained from submodules through a linear mapping [11, 12, 13, 14, 15].

3. Representation of degree 120 related to the extension group $O_8^+(2)$: 2.

In this section, we discuss the representation of length 120. The following definitions and Lemmas will be important here and subsequent sections.

Definition 3.1. *A binary code is referred to as even if the weight of all its codewords is divisible by 2* [12].

Lemma 3.2. *A binary self-orthogonal code C is even* [12].

Definition 3.3. *A binary code is doubly even if the weight of all its codewords are divisible by 4.*

Lemma 3.4. *A double even code is self-orthogonal.*

Definition 3.5. *A code with its dual distance at least 3 is called projective.*

Lemma 3.6. *Let C be a code with minimum distance d.If d >s + 1 >2;then C can be used to detect up to s errors. If d >2t + 1; then C can be used to correct up to t errors.*

II. RESULTS

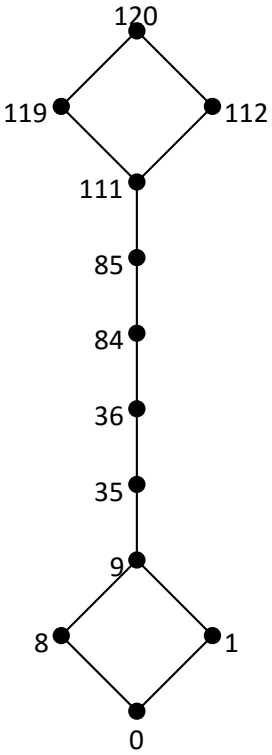
We construct a 120-dimensional permutation module invariant under permutation group G acting on a finite set Ω, of degree 120. We take the permutation module to be our working module and recursively find all submodules. This permutation module is decomposed into 12 submodules. The submodules are shown in the table below: From the table, m represents the submodule dimension and # is the submodule number of each dimension.

Table 1: Submodules from 120 Permutation Module

m	#	m	#
0	1	84	1
1	1	85	1
8	1	111	1
9	1	112	1
35	1	119	1
36	1	120	1

The submodules are the building blocks for the construction of a submodule lattice as shown in the figure below.

Figure 1: Submodule lattice of the 120 dimensional permutation module



From the lattice diagram, we see that the submodules of dimensions 8 and 1 are irreducible. The binary linear codes of the submodules are represented in the table below:

Table 2: Binary Linear codes of small dimensions

Name	Dimension	parameters
$C120,1$	8	$[120,8,56]_2$
$C120,2$	9	$[120,9,56]_2$
$C120,3$	35	$[120,35,24]_2$
$C120,4$	36	$[120,36,24]_2$

III. PROPERTIES OF SOME LINEAR CODES

We make some observations of non-trivial binary linear codes as follows:

4.1 $C120,1$

i . The polynomial of $C_{120,1}$is W(x)= 1+ $120x^{56}$ + 135 x^{64}. We observe that the weights of the two codewords are divisible by 4.

ii . $C_{120,1}^{\perp}$has a minimum weight of 3.

iii . has no other submodule apart from the trivial submodule.

Proposition 3.7. *Let G be a primitive group of degree 120 of the extension group* $O_8^+(2) : 2$.
Then $C_{120,1}$*is:*

i . Doubly even

ii . Projective

iii .Irreducible

Proof

i . See definition 3.3 and lemma 3.4.

ii . See definition 3.5 and lemma 3.6.

iii . See figure 1.

*4.2 C*120,2

i The polynomial of $C_{120,2}$is W(x)= 1+ $255x^{56}$ + 255 x^{64} +x^{120} . We observe that the weights of the three codewords are divisible by 4.

ii $C_{120,2}^{\perp}$has a minimum weight of 4.

iii has two submodules.

Proposition 3.8. *Let G be a primitive group of degree 120 of the extension group* $O_8^+(2)$:2

2. *Then* $C_{120,2}$*is:*

i . Doubly even

ii . Projective

iii .Decomposable

Proof

i . See definition 3.3 and lemma 3.4.

ii . See definition 3.5

iii . See figure 1.

IV. DESIGNS OF CODEWORDS OF MINIMUM WEIGHT IN $C_{120,i}$

We determine designs held by the support of codewords of minimum weight w_m in $C_{120,i}$.In Table 3 columns one, two, three and four respectively represents the codes $C_{120,i}$of Weight m, the parameters of the 1-designs Dw_m , the number of blocks of Dwm, and tests whether or not a design Dwm is primitive under the action of Aut(C).

Table 3: Designs of codewords of minimum weight in $C_{120,i}$

Code	Design	Number of blocks	Primitive
$[120,8,56]_2$	1-(120,56,56)	120	Yes
$[120,9,56]_2$	1-(120,56,119)	255	No

Remark 3.9. *From the results in the table above, we observe that the design 1-(120, 56 , 56) is primitive and 1-(120,56,119) is not primitive.*

CONCLUSION

Linear codes and designs from finite groups of extension using modular representation method can provide a range of benefits in various fields, including improved error correction, increased data storage capacity, improved security, efficient designs and improved computational efficiency. These benefits can lead to more effective and efficient systems as well as provide solutions to complex problems in various industries.

RECOMMENDATION

Linear codes and designs from finite groups of extension using modular representation method can be complex and technical. It is recommended that stakeholders collaborate with experts in the field to ensure that the information being used is accurate and reliable.

REFERENCES

[1] Berlekamp, E. R. (2015). *Algebraic coding theory* (revised edition). WorldScientific.

[2] Peterson, W. W., Peterson, W., Weldon, E. J., and Weldon, E. J. (1972). *Errorcorrecting codes.* MIT press.

[3] Bierbrauer, J. (2016). *Introduction to coding theory.* CRC Press.

[4] Fletcher, C. R. (1984).*Finite fields* Rudolf Lidl and Harald Niederreiter.Pp 755. 57 80.

1983. ISBN 0-201-13519-3 (Addison-Wesley). The Mathematical Gazette, 68(446), 306-307.

[5] Hankerson, D. C., Hoffman, G., Leonard, D. A., Lindner, C. C., Phelps, K. T., Rodger, C. A., and Wall, J. R. (2000). *Coding theory and cryptography: the essentials.* CRC Press.

[6] Richardson, T., and Urbanke, R. (2008). *Modern coding theory.* Cambridgeuniversity press.

[7] Baylis, D. J. (1997). *Error Correcting Codes: A Mathematical Introduction (Vol.15).* CRC Press.

[8] Bierbrauer, J. (2016). *Introduction to coding theory.* CRC Press.

[9] Ryan, W., and Lin, S. (2009). *Channel codes: classical and modern.* Cambridgeuniversity press.

[10] Davey, M. C., and MacKay, D. J. (1998). *Low density parity check codes overGF (q). In 1998 Information Theory Workshop* (Cat. No. 98EX131) (pp. 70-71).IEEE.

[11] Robinson, D. J. (1996). The Theory of Group Extensions. *In A Course in theTheory of Groups* (pp. 310-355). Springer, New York, NY.

[12] Chikamai, W. L. (2012). *Linear codes obtained from 2-modular representations of some finite simple groups* (Doctoral dissertation).

[13] Maina, J. L. (2019). *2-Modular Representations of Unitary Group U3 (4) AsLinear Codes* (Masters Dissertation, Kibabii University.

[14] Marani, V.N (2019). *Some Linear Codes, Graphs and Designs from MathieuGroups* M_{24} *and* M_{23} (Doctoral dissertation, Kibabii University).

[15] Pham, D. M., Premkumar, A. B., and Madhukumar, A. S. (2011). Error detection and correction in communication channels using inverse gray RSNS codes. *IEEETransactions on communications*, 59(4), 975-986.