CLASSIFICATION OF INTERNAL STRUCTURES OF SOME GROUPS OF EXTENSION USING MODULAR REPRESENTATION METHOD

JANET LILIAN MAINA

A THESIS SUBMITTED TO THE SCHOOL OF PURE AND APPLIED SCIENCES IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF DOCTOR OF PHILOSOPHY DEGREE IN PURE MATHEMATICS, MAASAI MARA UNIVERSITY

2024

Declaration

This thesis is the author's original work prepared with no other than the indicated sources and support and has not been presented elsewhere for a degree or any other award.

Signature.. Date ....

Janet Lilian Maina

SP02/JP/MN/16619/2022

Declaration and Approval.

We the undersigned certify that we have read and hereby recommend for acceptance of Maasai Mara University a thesis entitled,"Classification of Internal Structures of some groups of extension using modular representation method."

Signature.. Date.........................

Dr. John W. Matuya

Department of Mathematics and Physical Sciences

Maasai Mara University

Signature.. Date........................

Dr. Edward Njuguna

Department of Mathematics and Physical Sciences

Maasai Mara University

Signature.. Date........................

Dr. Vincent N. Marani

Department of Mathematics

Kibabii University

Dedication

I dedicate this thesis to my lovely children Wayne Wekesa and Delight Nangami.

Acknowledgment

I thank the almighty God for giving me life and grace that has enabled me do this work. I acknowledging the support, advice and profound efforts of my supervisors Dr. John W. Matuya, Dr. Edward Njuguna and Dr. Vincent N. Marani. I sincerely thank Maasai Mara University for offering me a chance and the space to carry out my research. I appreciate Department of Mathematics and Physical Sciences, Maasai Mara University for their valuable input in this research.

Table of Contents

List of Tables

List of Figures

Abstract

In the communication process, a sender encodes a message which is then send through a communication channel. There could be a barrier in the channel such that the message gets distorted before it reaches the recipient. A solution is in the need for construction of more optimal codes for error detecting and correcting. This research focused on representing the internal structures of groups of extensions using modular representation method. Specifically, it examined the maximal subgroups of four groups: $0_8^+(2) : 2, L_3(4) : 2, L_3(4) : 2^2$ and $L_3(3) : 2$. For each of these groups, detailed analysis was provided on the irreducible representations of their maximal subgroups, across varying representation degrees. The key goal was to classify internal structures of the groups using modular representations method. The specific objectives were to classify maximal subgroups of the groups of extension , enumerate linear codes from the maximal subgroups, construct lattice diagrams of linear codes obtained and analyze the properties of linear codes and designs constructed using the modular representation method. By decomposing into irreducible constituents, the work uncovered new linkages between representation theory, finite group extensions, and combinatorial designs. For the group $0_8^+(2) : 2$, representations of degree 120, 135, and 960 across multiple maximal subgroups were explored. Similarly, representations ranging from degree 21 to 336 were analyzed for the maximal subgroups under $L_3(4) : 2$ and $L_3(4) : 2^2$. Finally, representations up to degree 234 were examined among the maximal subgroups under $L_3(3) : 2$. In mapping these finite groups through their maximal subgroups representations systematically, the work contributes enhanced understanding of how extended finite groups can be classified internally based on modular representation structures. Findings fill a gap in current group representation theory literature related to certain orders of linear groups of extensions. Outcomes point to opportunities for further exploration into additional families of finite groups using similar representation mapping techniques. Findings from the research on this classification of linear codes and designs for error correction gets their applicability in digital communication, data storage and cryptography.

Symbols and abbreviations

$\mathbb{N}$	Set of Natural numbers
$\mathbb{Z}$	Set of Integers
$\mathbb{R}$	Set of Real numbers
$\mathbb{C}$	Set of Complex numbers
Ω	A finite set
$\mathbf{1}$	The all ones vector
S_n	the symmetric group on n symbols
V	Vector space
$\mathbb{F}$	A finite field
$\mathbb{F}_q$	A finite field of q elements
Char($\mathbb{F}$)	Characteristic of a field $\mathbb{F}$
Aut(G)	Automorphism group of G
I_G	The identity element of G
K $\leq$ G	K is a subgroup of G
K $\trianglelefteq$ G	K is a normal subgroup of G
$\|G\|$	Order of a group G
H $\cong$ G	H is Isomorphic to G
$[n, k, d]_q$	A q-ary code of length n, dimension k and minimum distance d
C	A linear code
(E, C)	An incidence structure with E points and C blocks
Γ	Graph
PG(V)	The projectile geometry
FG	Group algebra
$\mathbb{F}\Omega$	$\mathbb{F}$G -module
GL$_n$(q)	General linear group of dimension n over F_q
#	Number of Orbits

Chapter 1

Introduction

1.1 Background of the study

In encoding science, the modular representation approach is a procedure employed to create error-correcting codes. The technique is founded on the notion of depicting components of the code as vectors over a finite field, and then utilizing modular arithmetic to manipulate these vectors. The process commences by specifying a finite field, typically GF(q), where q is a prime power. The constituents of this field can be portrayed as integers modulo q, and arithmetic operations such as addition and multiplication are defined modulo q. Subsequently, a vector space over the finite field is delineated, with dimension n. The elements of the code are symbolized as vectors in this space, with each constituent of the vector being an element of the finite field. The code is then characterized as a subset of the vector space, with a specific quantity of constraints imposed on the vectors to guarantee that they fulfill the desired error-correcting attributes (Baylis, 1997; Hankerson et al., 2000; Peterson & Weldon, 1972).

To encode a communication using the code, the message is initially converted into a vector over the finite field. This vector is then multiplied by a generating matrix, which is an array with rows that extend the code. The resulting vector is the encoded message, which can be transmitted over a noisy channel. To rectify errors in the received message, the modular representation technique employs the syndrome decoding method. The syndrome of a received vector is obtained by multiplying it by the transpose of the generating matrix. If the received vector contains errors, the syndrome will not be zero. By performing certain operations on the syndrome, it is possible to ascertain which errors occurred and correct them. The modular representation approach is extensively utilized in coding theory because it allows for efficient encoding and decoding of error-correcting codes, and because it can be easily implemented using digital circuits (Berlekamp, 2015; Bierbrauer, 2016; Hankerson et al., 2000; Ryan & Lin, 2009).

The modular representation technique is merely one of numerous methods utilized in error-correcting codes. Its comparison to other techniques is contingent upon the particular application and requirements. One advantage of the modular representation approach is that it enables efficient encoding and decoding of codes. The method can be accomplished using digital circuits, making it appropriate for applications where hardware implementation is crucial, such as in communication systems or computer memory storage. Another benefit is that it can generate codes with desirable error-correcting attributes. By meticulously selecting the generating matrix, it is possible to create codes that can rectify a specific quantity of errors or even detect errors without correcting them. Nevertheless, the modular representation technique may not be the most suitable option for all applications. For example, if the code must be highly compact, then alternative methods such as turbo codes or low-density parity-check codes may be more fitting (Davey & MacKay, 1998; Richardson & Urbanke, 2008).

These codes can achieve similar or even better error-correcting performance with fewer bits. Additionally, the modular representation method relies on finite fields, which can have limited size. If the required code length or error-correcting capability exceeds the size of the available finite field, then other techniques such as algebraic geometry codes or cyclic codes may be more appropriate. In summary, the choice of error-correcting code technique depends on the specific requirements of the application. The modular representation method is a powerful and efficient technique, but it may not be the best choice for all scenarios (Baylis, 1997; Berlekamp, 2015; Bierbrauer, 2016; Pham et al., 2011).

The study of finite groups and their representations has broad and deep connections spanning group theory, combinatorics, coding theory, and number theory. In particular, investigating the structure and representations of finite groups of extensions through their maximal subgroups sheds light on internal classification and links to other mathematical structures. The origins of finite group representation theory date back to the 19th century work of Frobenius. Studies on group extensions also have a long history, with foundational results by Remak, Schur, and others (Berlekamp, 2015; Bierbrauer, 2016; Hankerson et al., 2000; Sayed, 2016).

More recent works have further explored representations of specific finite groups of extensions and related combinatorial designs (Chikamai, 2012). Specifically, the study centers on describing the representations of maximal subgroups under four finite groups of extensions: $O_8^+(2):2$, $L_3(4):2$, $L_3(4):2^2$ and $L_3(3):2$. By decomposing these complex finite groups into constituent subgroups and examining their representation structures, the work links modular representation theory with the classification of group extensions. The specific representation degrees analyzed across the varying maximal subgroups range from 21 to 960. Outcomes from the representation mapping enrich understanding of how extended finite groups can be classified internally based on the irreducible representations of their building maximal subgroups. The techniques developed expand existing knowledge related to representing certain linear groups of extensions using a modular approach. Findings also uncover new connections to linear codes and combinatorial designs.

1.2 Basic Concepts

1.2.1 Groups

The theory of groups is essential to this subject, providing the mathematical framework for studying finite groups and their properties, including group actions, group representations, and character theory. The symmetric group on a set Ω is the group S_Ω containing all permutations of Ω. A permutation group G on a set Ω is a subgroup of S_Ω, and G is considered transitive on Ω if, for any $\alpha, \beta \in \Omega$, there exists an element $g \in G$ such that the image α^g of α under g equals β (Hankerson et al., 2000).

Definition 1.2.1. *Let G be a group and Ω be a set. An action of G on Ω is a function that associates every $\alpha \in \Omega$ and $g \in G$ with an element α^g of Ω such that, for all $\alpha \in \Omega$ and all $g, h \in G$, $\alpha^1 = \alpha$, and $(\alpha^g)^h = \alpha^{gh}$ (*Hankerson et al., 2000*). An action naturally defines a permutation representation of G on Ω, which is a homomorphism ψ from G into S_Ω. Conversely, a permutation representation naturally defines an action of G on Ω (*Ryan & Lin, 2009*).*

Definition 1.2.2. *A collection of bijective transformations on a set Ω that forms a group under composition is termed primitive if it satisfies two conditions: it acts transitively on Ω, allowing any element to be mapped to any other, and the only partitions of Ω it leaves invariant are the trivial ones (either Ω itself or each element in its own subset). Conversely, such a collection is called imprimitive if it preserves at least one non-trivial partition of Ω under its action(*Hankerson et al., 2000*).*

Theorem 1.2.3. *For every n, the symmetric group S_n acts n-transitively on $\Omega = 1, 2, \ldots, n$ (*Ryan & Lin, 2009*).*

Theorem 1.2.4. *Every k-transitive group G (with $k \geq 2$) acting on a set Ω is primitive (*Ryan & Lin, 2009*).*

Definition 1.2.5. *Let G be a finite group. If N and G are groups, an extension of N by G is a group M such that:*

1. *$N \trianglelefteq M$, and*

2. *$M/N \cong G$ (*Berlekamp, 2015*).*

1.2.2 Representations

Let G be a group and $\mathbb{F}$ be a field. An $\mathbb{F}G$-module is defined as a vector space V over $\mathbb{F}$ equipped with a left action by elements of G, such that for any $g \in G$, the action of g on V is a linear transformation. There exists a one-to-one correspondence between representations of G and $\mathbb{F}G$-modules. Consequently, the theoretical results pertaining to

$\mathbb{F}G$-modules can be directly applied to representations (Hankerson et al., 2000; Ryan & Lin, 2009).

Theorem 1.2.6. *For a finite group G and a field $\mathbb{F}$, there exists a bijective correspondence between finitely generated $\mathbb{F}G$-modules and representations of G on finite-dimensional $\mathbb{F}$-vector spaces (*Ryan & Lin, 2009; Sayed, 2016*).*

The subsequent definitions are presented in the context of $\mathbb{F}G$-modules, with their equivalents in representation theory implied.

Definition 1.2.7. *Let V be an $\mathbb{F}G$-module. A subspace W of V is called an $\mathbb{F}G$-submodule of V if $gw \in W$ for all $w \in W$ and $g \in G$ (*Hankerson et al., 2000*).*

Definition 1.2.8. *A vector space V endowed with a group action over a field $\mathbb{F}$ is termed elementary or indecomposable if it contains no proper non-zero invariant subspaces under the group action. Conversely, such a vector space is considered decomposable if it admits at least one proper non-zero invariant subspace (*Hankerson et al., 2000; Ryan & Lin, 2009*).*

Definition 1.2.9. *An $\mathbb{F}G$-module V is said to be decomposable if it can be expressed as a direct sum of two $\mathbb{F}G$-submodules, i.e., if there exist submodules U and W of V such that $V = U \oplus W$. If V can be written as a direct sum of irreducible submodules, it is called completely reducible (*Ryan & Lin, 2009*).*

1.2.3 Characteristics and Attributes of Linear Codes

The study of linear codes forms a cornerstone in coding theory, providing essential tools for error detection and correction in data transmission and storage. This subsection explores the fundamental properties that define and distinguish linear codes, offering insights into their structure, capabilities, and applications. We begin by considering a finite field $\mathbb{F}_q$ of order q, where q is prime. Within this context, we define and examine several key concepts:

Definition 1.2.10. *A q-ary code C over* $\mathbb{F}_q$ *is a set of finite sequences composed of elements from* $\mathbb{F}_q$*, referred to as codewords. When all codewords in C have the same length n, we classify C as a block code of length n (*Hankerson et al., 2000; Peterson & Weldon, 1972; Sayed, 2016*).*

Central to the analysis of linear codes is the notion of distance between codewords.

Definition 1.2.11. *The Hamming distance* $d(x, y)$ *between two codewords x and y is defined as the number of positions in which they differ. For a linear code C, the minimum distance d is given by:* $[d = \min d(0, x) : 0, x \in C, x \neq 0]$ *where 0 represents the zero vector (*Hankerson et al., 2000; Berlekamp, 2015; Pham et al., 2011*).*

These definitions lay the groundwork for exploring more advanced properties of linear codes, including weight distributions, generator matrices, and dual codes. Through this examination, we gain insights into the error-correcting capabilities, efficiency, and practical applications of various code constructions.

Doubly even codes

Doubly even codes represent a significant area of study in coding theory. These error-correcting codes are defined over a binary alphabet $0, 1$ and possess the distinctive property that their length is invariably a multiple of 4. A key characteristic of doubly even codes is their self-duality, meaning a code C is identical to its dual code $C^{\perp}$. The dual code $C^{\perp}$ consists of all binary vectors orthogonal to every codeword in C (Peterson & Weldon, 1972).

The self-dual nature of these codes offers advantages in both encoding and decoding processes, enhancing error correction efficiency. Moreover, the minimum Hamming distance of doubly even codes is always even. Hamming distance, defined as the number of differing positions between two codewords, is crucial in determining error-correcting capability. The even minimum distance facilitates error detection and correction (Peterson & Weldon, 1972).

Interestingly, doubly even codes exist exclusively for lengths that are multiples of 8. This non-trivial result in coding theory underscores the mathematical depth of these structures. The study of doubly even codes thus intertwines fundamental concepts of linear algebra, combinatorics, and information theory, making them a rich subject for theoretical exploration and practical application in error-correcting systems (Peterson & Weldon, 1972).

Projective codes

Projective codes are a class of linear codes that are defined using projective geometry. They have good error-correcting capabilities and have a high minimum distance, which makes them effective at correcting errors in transmitted data. This property is particularly important in applications such as telecommunications and data storage. These codes have a large covering radius, which means they can cover a large portion of the space of possible codewords. This property is useful in applications such as cryptography and network coding. In addition, they have a natural symmetry structure that can be exploited in applications such as cryptography and coding theory. This symmetry can be used to construct codes with desirable properties, such as those that are invariant under certain automorphisms of the code. The projective codes also have a rich algebraic structure that is used to study their properties for instance minimum distance. Projective codes have connections to a variety of other areas of mathematics, including algebraic geometry, number theory, and group theory. This makes them a rich area of study with many interesting applications and connections to other fields (Peterson & Weldon, 1972; Sadiki et al., n.d.).

Irreducible codes

The length of irreducible codes is characterized by being either a prime number or a prime power. This structural property facilitates analysis and implementation by providing a well-defined code size. A notable feature of these codes is their tendency to possess large minimum distances, which directly correlates with their error-correcting prowess. The greater the minimum distance, the more errors a code can detect and correct (Peterson & Weldon, 1972).

The minimum distance of an irreducible code is intrinsically linked to the properties of the field upon which it is constructed. Furthermore, irreducible codes are distinguished by their efficient encoding and decoding processes, which leverage algebraic methods. These codes are often engineered to achieve optimality in error correction (Peterson & Weldon, 1972).

The combination of these attributes structured length, substantial minimum distance, and efficient algebraic processing renders irreducible codes particularly advantageous for real-world applications. Their optimality in error correction further enhances their appeal and utility in practical scenarios (Peterson & Weldon, 1972).

Decomposable codes

Decomposable codes have the property of being constructed through the composition of smaller component codes. The code is formed by combining two or more smaller codes in a specific way. This composition property allows for flexible design and construction of codes with desired properties. By composing smaller codes with suitable properties, decomposable codes can achieve improved error-correcting capabilities. The composition can be designed in such a way that the resulting code has a larger minimum distance or enhanced error correction performance compared to the individual component codes. To add on this, decomposable codes exhibit modularity, meaning that the code can be decomposed back into its constituent component codes. This modularity property facilitates efficient encoding and decoding algorithms by breaking down the code into smaller, manageable parts (Peterson & Weldon, 1972).

Also, the composition property of decomposable codes provides flexibility in code design. Different combinations of component codes can be used to achieve specific code properties, such as large minimum distance, high error correction capability, or resistance to specific types of errors. Decomposable codes often involve trade-offs between various code properties. For example, while combining component codes may improve error correction capability, it may also result in increased encoding and decoding complexity. Designing decomposable codes involves balancing these trade-offs based on specific application requirements (Peterson & Weldon, 1972).

1.2.4 Error Detection and Correction Strategies

This subsection explores the methodologies employed in interpreting and rectifying encoded messages. We focus on the practical application of codes in the context of message transmission and reception. Our analysis assumes the use of a symmetric q-ary channel, where each symbol in the code's alphabet has an equal probability of erroneous transmission, and in the event of an error, all incorrect symbols are equally likely to occur. The following theorem provides a precise quantification of a code's capacity for error detection and correction, given the assumption of a symmetric channel:

Theorem 1.2.12. *For a code C with minimum distance d, the following properties hold:*

i . C can detect up to d - 1 errors

ii . C can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors

This theorem establishes the fundamental relationship between a code's minimum distance and its error-handling capabilities, forming the basis for evaluating the effectiveness of various coding schemes (Berlekamp, 2015; Hankerson et al., 2000).

The error detection and correction process typically involves several steps. First, the received message is examined for potential errors. This is often done by checking if the received word is a valid codeword. If it is not, an error is detected. The number of errors that can be reliably detected depends on the minimum distance of the code, as stated in the theorem above (Peterson & Weldon, 1972).

Once an error is detected, the next step is error correction. This involves determining the most likely transmitted codeword given the received word. The most common approach is to choose the codeword that is closest to the received word in terms of Hamming distance. This method, known as maximum likelihood decoding, is optimal for symmetric channels (Ryan & Lin, 2009).

Various algorithms have been developed for efficient error correction in different types of codes. For linear codes, syndrome decoding is a widely used technique. This method involves computing the syndrome of the received word, which is zero if and only if the received word is a valid codeword. The syndrome provides information about the error pattern, which can be used to correct the errors (Bierbrauer, 2016).

For cyclic codes, algebraic decoding algorithms such as the Berlekamp-Massey algorithm are often employed. These algorithms exploit the algebraic structure of cyclic codes to achieve efficient error correction. In the case of Reed-Solomon codes, a popular class of cyclic codes, these algorithms can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors, which is optimal (Berlekamp, 2015).

More recently, iterative decoding algorithms have been developed for certain classes of codes, such as low-density parity-check (LDPC) codes and turbo codes. These algorithms can achieve near-optimal error correction performance with reasonable computational complexity, making them suitable for practical applications in digital communication systems (Richardson & Urbanke, 2008).

The choice of error detection and correction strategy depends on various factors, including the characteristics of the communication channel, the required level of reliability, and the available computational resources. The ongoing research in this field continues to produce new coding schemes and decoding algorithms, pushing the boundaries of what is achievable in terms of error correction performance (Pham et al., 2011).

1.2.5 Combinatorial Structures and Their Applications

The field of combinatorial design theory provides a rich framework for studying and applying structured arrangements of elements. This branch of mathematics explores the existence of structured arrangements where elements are grouped into collections of equal cardinality, with the property that any chosen subset of a specific size appears in a constant number of these collections. The theoretical foundations and practical applications of combinatorial designs offer valuable tools and techniques for:

i . Constructing optimal designs with desired properties

ii . Analyzing the characteristics of existing designs

iii . Applying design principles to solve problems in various domains

Central to this field is the concept of incidence structures, formally defined as follows:

Definition 1.2.13. *A combinatorial arrangement* $\mathcal{A} = (\mathcal{E}, \mathcal{C}, \mathcal{R})$ *consists of three components:*

i . $\mathcal{E}$ represents the collection of fundamental elements

ii . $\mathcal{C}$ denotes the family of element groupings

iii . $\mathcal{R}$ specifies the membership relationship between $\mathcal{E}$ and $\mathcal{C}$

This mathematical framework serves as the foundation for exploring more complex design structures and their properties, bridging theoretical concepts with practical applications in areas such as experimental design, coding theory, and cryptography (Hankerson et al., 2000; Ryan & Lin, 2009). One of the most fundamental types of combinatorial designs is the balanced incomplete block design (BIBD). A BIBD is an arrangement of v distinct objects into b blocks such that each block contains exactly k distinct objects, each object occurs in exactly r different blocks, and every pair of distinct objects occurs together in exactly λ blocks. These designs find applications in various fields, including agricultural experiments, software testing, and network security (Bierbrauer, 2016).

Another important class of combinatorial designs is t-designs, which generalize the concept of BIBDs. A t-(v, k, λ) design is an incidence structure where each block contains k points, and every t-subset of points is contained in exactly λ blocks. These designs have connections to coding theory, with certain t-designs giving rise to optimal error-correcting codes (Kananu, 2019).

Steiner systems are a special case of t-designs where $\lambda = 1$. The most famous example is perhaps the Steiner triple system, where $k = 3$. These systems have applications in coding theory, cryptography, and computer science. For instance, the unique Steiner triple system on 7 points (often denoted as STS(7)) is closely related to the Hamming $[7, 4, 3]$ code, a fundamental error-correcting code (Marani, 2019).

Hadamard matrices, which are square matrices of order n with entries ± 1 such that $HH^T = nI$, form another important class of combinatorial structures. These matrices have applications in coding theory, cryptography, and signal processing. The Paley construction, which uses quadratic residues in finite fields, provides a method for constructing Hadamard matrices of certain orders (Rodrigues, 2002).

In recent years, there has been increasing interest in the connections between combinatorial designs and quantum information theory. Mutually unbiased bases (MUBs) and symmetric informationally complete positive operator-valued measures (SIC-POVMs) are quantum structures that have deep connections to certain combinatorial designs. These connections are being explored for potential applications in quantum cryptography and quantum error correction (Sayed, 2016).

The study of combinatorial designs also intersects with graph theory. Many designs can be represented as graphs, and conversely, certain graphs give rise to designs. For example, strongly regular graphs are closely related to symmetric designs. This interplay between designs and graphs provides additional tools and perspectives for analyzing these structures (Chikamai, 2012). In conclusion, combinatorial structures and their applications form a rich and active area of research, with connections to many branches of mathematics and numerous practical applications. As technology advances and new challenges arise in fields such as data science, network design, and quantum computing, the importance of combinatorial designs is likely to continue growing, driving further theoretical developments and practical innovations.

1.3 Statement of the Problem

The exploration of mathematical groups and their structural properties has been an active area of research in algebra and coding theory (Chikamai, 2012; Kariuki, 2019; Maina, 2019 & Marani, 2019). Prior studies by these authors have shown that analyzing subgroups and representations of various finite groups can yield beneficial linear codes and combinatorial designs with valuable applications in communications systems, data storage, cryptography, and more. However, there remains a knowledge gap identified by (Chikamai, 2012) regarding the classification of subgroup structures and constructions of codes and designs from additional groups of extensions. This limited our understanding of these groups' representations and prevented us from assessing the parameters and applications of the structures they can produce. A systematic classification and analysis was needed to unlock their potential benefits.

This research aimed at addressing this gap by classifying and analyzing maximal subgroups and the internal structures within new groups of extension using modular representation techniques. Addressing this gap expands our knowledge of these groups' internal structures and modular constructions while revealing new optimal codes and designs for practical applications.

1.4 General objective of the study

The general objective of research was to classify internal structures of some groups of extension using modular representation method.

1.5 Specific objectives of the study

The specific objectives for the study were:

i . To classify maximal subgroups of some groups of extension.

ii . To enumerate linear codes from maximal subgroups of some groups of extension.

iii .To construct lattice diagrams of linear codes obtained from maximal subgroups.

iv .To analyse the properties of linear codes and designs constructed using the modular representation method.

1.6 Significance of the study

Linear codes and designs from maximal subgroups using the modular representation method are important because they have many theoretical and practical applications in coding theory and combinatorial mathematics. Some of the reasons why we need these codes and designs are:

i . Error-correcting codes: Linear codes are an important class of error-correcting codes used in digital communication systems, storage devices, and other applications like in Satellite Communication data streaming, wireless sensor networking and data management software. The construction of linear codes using the modular representation method can lead to codes with good error-correcting properties, which are important for ensuring reliable transmission and storage of data.

ii . Combinatorial designs: Combinatorial designs are important objects of study in combinatorial mathematics, and have applications in experimental design, statistics, and other areas. The construction of designs using the modular representation method can lead to designs with interesting properties related to the structure of finite groups.

iii . Cryptography: Linear codes and designs have applications in cryptography, where they are used for error correction and encryption. The construction of these objects using the modular representation method can lead to codes and designs with good cryptographic properties, such as resistance to attacks and efficient key exchange.

iv . Group theory: The construction of linear codes and designs from maximal subgroups using the modular representation method lead to new insights into the structure of finite groups and their applications in coding theory and combinatorial mathematics.

Chapter 2

Literature Review

2.1 Introduction

This chapter reviews literature on work of authors related to modular representation theory.

2.2 Empirical Literature

The doctoral research conducted by Chikamai (2012) explored the development of error-correcting schemes arising from specialized algebraic depictions of specific elementary symmetry structures. The study focused on understanding the properties of codes, with the aim of uncovering new insights and results. The research emphasized the significance of finite simple groups, fundamental mathematical structures with diverse applications in various branches of mathematics. By utilizing 2-modular representations, the study explored how these groups generated linear codes. Linear codes, crucial in coding theory, provided systematic and error-detecting methods for representing information, finding applications in telecommunications, cryptography and error correction.

The dissertation by Marani (2019) specifically focused on the utilization of Mathieu groups M_{24} and M_{23}, which are finite sporadic simple groups known for their exceptional properties. The study explored how these groups can be exploited to construct linear codes, graphs, and designs. Linear codes, fundamental in coding theory, enable systematic and error-detecting information representation. Graphs and designs, essential in combinatorial mathematics, had applications in computer science and network analysis. The study delved into the properties of these structures, providing valuable insights into their applications and advantages. By establishing the relationship between Mathieu groups and linear codes, graphs, and designs, this research significantly contributed to the advancement of coding theory and combinatorial mathematics.

The study on 2-modular representations of the unitary group $U_3(4)$ and their application as linear codes by Maina (2019) investigated the interplay between the group and the codes and designs. The research focused on the unitary group $U_3(4)$, a finite group with significant mathematical properties. By utilizing 2-modular representations, the study examined how this group generated optimal linear codes. The dissertation presented novel results obtained through the construction and analysis of linear codes based on 2-modular representations of the unitary group $U_3(4)$. By establishing the relationship between the unitary group $U_3(4)$ and linear codes, this research contributed to the advancement of coding theory and combinatorics.

Kananu (2019) investigated the properties of these mathematical structures, aimed at uncovering new insights and results. The research focused on projective symplectic group, $PS_8(2)$, a mathematical structure renowned for its unique properties. By exploiting this group, codes, designs and graphs were generated. The study investigated the properties of these mathematical structures, aimed at uncovering new insights and results. The research focused on projective symplectic group, $PS_8(2)$, a mathematical structure renowned for its unique properties. By exploiting this group, codes, designs and graphs were generated. The codes were fundamental in coding theory and systematically represented properties that could detect errors. Designs, on the other hand, had applications in experimental design and statistical analysis, while graphs played a key role in graph theory and had diverse applications in computer science, network analysis, and social sciences. By establishing the relationship between the projective symplectic group $PS_8(2)$ and codes, designs, and graphs, this research contributed to the advancement of coding theory, combinatorial mathematics, and graph theory.

In the study conducted by Kariuki (2019), ternary linear codes and designs derived from the Projective Special Linear Group $PSL_3(4)$ were explored. The Projective Special Linear Group $PSL_3(4)$ is a specific projective group known for its significant mathematical properties. The research focused on utilizing this group to construct and analyze ternary linear codes and designs, which played a fundamental role in coding theory for systematic and error-detecting methods of information representation, as well as in experimental design and statistical analysis. The author presented the findings obtained through the investigation of ternary linear codes and designs derived from the Projective Special Linear Group $PSL_3(4)$. The properties of the mathematical structures were analyzed, shedding light on their construction, invariance, and potential applications. The research established the relationship between the Projective Special Linear Group $PSL_3(4)$ and ternary linear codes and designs, providing insights into their properties and advantages.

Rodrigues (2002) examined constructions of combinatorial structures and their graphical representations, utilizing a range of fundamental algebraic objects as a foundation. The study focused on constructing codes from designs, and graphs using finite simple groups as a basis. Codes of designs provided systematic methods for representing combinatorial structures, while codes of graphs had applications in areas such as network coding and error correction. The properties of these mathematical structures were analyzed, shedding light on their construction, invariance, and potential applications. The research established the relationship between finite simple groups and codes of designs and graphs, offering insights into their properties and advantages and contributed to the understanding of finite simple groups and their internal structures.

Several linear codes have been constructed from different types of finite simple groups using 2-modular representations method by a number of authors. For instance, Chikamai (2012) derived error-correcting schemes from specific fundamental algebraic structures, Maina (2019) constructed systematic encoding methods from the Unitary Group $U_3(4)$, Marani (2019) explored various combinatorial configurations and their graphical representations originating from the exceptional permutation groups M_{24} and M_{23}, and Kananu (2019) generated coding theory objects, combinatorial arrangements, and network models based on a particular symplectic geometry. However, classification of linear codes and designs from some groups of extension using modular representation method has not been explored. This study aims to address this gap by classifying and analyzing the internal structures within new groups of extension using modular representation method.

Chapter 3

Methods

3.1 Introduction

In this chapter, we describe construction of linear codes and designs from finite groups using modular representation method. Computational tool, MAGMA was used together with modular representation method to construct optimal codes and designs and analyze their properties.

3.2 Modular representation method and binary linear Codes

Constructing linear codes and designs from groups of extension using modular representation method typically involved group actions and took the following steps:

i . Generate a given group of extension G.

ii . Determine the subgroups of G .

iii . Choose a maximal sub group H of G.

iv . Define a group action of G on the set of left cosets of H, denoted as G/H.

v . Construct a permutation module M associated with this action.

vi . Construct submodules from M by partitioning the module into smaller subspaces that are invariant under the action of G.

vii . Identify a submodule N of M considering the stabilizer subgroup of the identity coset of H.

vii . Construct a binary linear code C based on the submodule N.

ix . The resulting binary linear code C represents the information that can be transmitted or stored using the structure of the maximal subgroup H within the original group of extension G (Chikamai, 2012 ; Kananu, 2019 ; Maina, 2019 ; Marani, 2019 ; Rodrigues, 2002 & Sayed, 2016).

Chapter 4

Analysis of Maximal Subgroups for Selected Extension Groups

This chapter examines the maximal subgroups of four specific extension groups: $O_8^+(2):2$ of $S_6(2)$, $L_3(4):2$ of $L_3(4)$, $L_3(4):2^2$ of $L_3(4)$, and $L_3(3):2$ of $L_3(3)$.

4.1 Maximal Subgroups of $O_8^+(2):2$

$O_8^+(2):2$ is an extension group where $S_6(2)$ is a normal subgroup. Table 4.1 presents the 8 maximal subgroups of $O_8^+(2):2$, arranged by increasing degree.

Table 4.1: Maximal subgroups of $O_8^+(2):2$

Maximal subgroup	Degree	Order	No. of Orbits	Length of orbits
$S_6(2):2$	120	2,903,040	3	[1,56,63]
$2^6:S_8$	135	2,580,480	2	[56,64]
S_9	960	362,880	2	[36,84]
$2^2:S_4(3):3$	1120	311,040	3	[3,36,81]
$2^{13}:3^3$	1575	221,184	2	[24,96]
$L_2(7):2^{10}$	2025	172,032	2	[8,112]
$2^7:3^5$	11200	31,104	2	[12,108]
$2:S_5:S_5$	12,096	28,800	2	[56,64]

The analysis of $O_8^+(2):2$ reveals a complex subgroup structure with varying degrees and orbit lengths. The subgroup $S_6(2):2$ stands out with the highest order but a relatively low degree, suggesting a dense internal structure. In contrast, $2:S_5:S_5$ has the highest degree but the lowest order, indicating a more spread-out configuration. The varying number and lengths of orbits across subgroups hint at diverse symmetry patterns within the extension group.

4.2 Maximal Subgroups of $L_3(4):2$

$L_3(4):2$ is an extension of $L_3(4)$. Table 4.2 shows its 4 maximal subgroups:

Table 4.2: Maximal subgroups of $L_3(4):2$

Maximal subgroup	Degree	Order	No. of Orbits	Length of orbits
$2:A_5:2^4$	21	1920	2	[40,80]
$2:A_6$	56	720	3	[15,15,90]
$L_2(7):(2)$	120	336	4	[1,21,42,56]
$2^4 \times 3^2$	280	144	4	[12,18,18,72]

The maximal subgroups of $L_3(4):2$ display a clear trend of increasing degree corresponding with decreasing order. This pattern suggests that as the subgroups become more complex in structure (higher degree), they become less numerous (lower order). The orbit structures also become more fragmented as the degree increases, with the highest degree subgroup having the most evenly distributed orbit lengths.

4.3 Maximal Subgroups of $L_3(4):2^2$

$L_3(4):2^2$ extends $L_3(4)$. Table 4.3 presents its 5 maximal subgroups:

Table 4.3: Maximal subgroups of $L_3(4):2^2$

Maximal subgroup	Degree	Order	No. of Orbits	Length of orbits
$A_6:2^2$	56	1440	2	[30,90]
$2^8 \times 3$	105	768	3	[24,32,64]
$L_2(7):2^2$	120	672	4	[1,21,42,56]
$2^5 \times 3^2$	280	288	3	[12,36,72]
$2^2:A_5$	336	240	4	[10,20,30,60]

The maximal subgroups of $L_3(4):2^2$ show a general trend of increasing degree and decreasing order, similar to $L_3(4):2$. However, the relationship is less strict here, with some exceptions. The orbit structures are more varied, with no clear pattern emerging as the degree increases. This suggests a more complex interplay between the subgroup structures in this extension group.

4.4 Maximal Subgroups of $L_3(3):2$

$L_3(3):2$ extends $L_3(3)$. Table 4.4 shows its 4 maximal subgroups:

Table 4.4: Maximal subgroups of $L_3(3) : 2$

Maximal subgroup	Degree	Order	No. of Orbits	Length of orbits
$2^3 \times 3^3$	52	216	2	[36,108]
$2^5 \times 3$	117	96	3	[48,48,48]
$2 \times 3 \times 13$	144	78	6	[1,13,26,26,39,39]
$2^4 \times 3$	234	48	6	[8,16,24,24,24,48]

The maximal subgroups of $L_3(3) : 2$ exhibit a clear inverse relationship between degree and order. Interestingly, the number of orbits increases with the degree, suggesting that higher degree subgroups have more complex symmetry structures. The orbit lengths become more fragmented and varied as the degree increases, further supporting this interpretation.

Chapter 5

Representations of Maximal subgroups of $O_8^+(2):2$

In this chapter, we discussed the representations of Maximal subgroups of $O_8^+(2):2$. The findings were then summarized in form of a theorem at the end of each representation.

5.1 Analysis of the 120-Dimensional Representation

This section examines the properties and structure of a 120-dimensional permutation module. The module remains unchanged when subjected to the transformations induced by a symmetry-preserving algebraic structure G operating on a discrete collection of elements Ω containing 120 distinct members. Our study begin by considering this permutation module as our primary object of study and systematically identify all its submodules through recursive analysis.

Our investigation reveals that this permutation module decomposes into a total of 28 distinct submodules. To provide a clear overview of this decomposition, we present the dimensions of these submodules along with their respective frequencies in Table 5.1.

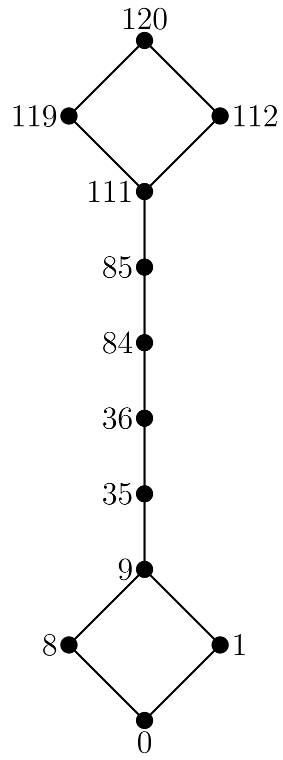
Table 5.1: Submodules from 120 Permutation Module

m	#	m	#	m	#	m	#	m	#
0	1	37	1	84	1	101	1	119	1
1	1	46	2	85	1	110	1	120	1
10	2	55	1	99	1	116	1		
19	1	56	1	100	1	117	1		
20	1	64	1						
21	1	65	1						
35	1	74	2						
36	1	83	1						

The submodules identified from the decomposition of the 120-dimensional permutation module serve as the fundamental components for constructing a submodule lattice. Figure

5.1 presents a visual representation of this lattice, illustrating the hierarchical relationships between the submodules.

Figure 5.1: Lattice diagram depicting the submodule structure of the permutation module of degree 120



Through careful examination of the lattice diagram, we identify that the submodules of dimensions 64 and 1 exhibit the property of irreducibility. This observation has significant implications for understanding the fundamental building blocks of the module's structure. To further elucidate the properties of these submodules, we generate binary linear codes corresponding to each submodule. These codes are presented in Table 5.2, offering a compact representation of the submodules in terms of coding theory.

Table 5.2: Binary Linear codes of small dimensions from 120 Permutation Module of $O_8^+(2):2$

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

For the code $C_{120,1}$, we observe the following properties:

i . The weight enumerator polynomial is given by $W(x) = 1 + 120x^{56} + 135x^{64}$. Notably, all non-zero weights (56 and 64) are divisible by 4.

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

iii . $C_{120,1}$ contains only the trivial submodule.

Proposition 5.1.1. *Let G be a primitive group of degree 120 of the extension group $O_8^+(2):2$. The code $C_{120,1}$ possesses the following characteristics:*

i . It is doubly even.

ii . It is projective.

iii . It is irreducible.

Proof.

i. To show $C_{120,1}$ is doubly even, we examine its weight polynomial $W(x) = 1 + 120x^{56} + 135x^{64}$. All non-zero weights (56 and 64) are divisible by 4, satisfying the definition of a doubly even code.

ii. For projectivity, we note that $C_{120,1}^{\perp}$ has a minimum weight of 3. A linear code whose corresponding dual code has a minimum Hamming weight of 3 or more is classified as a projective code. Thus, $C_{120,1}$ is projective.

iii. To prove irreducibility, we examine the submodule lattice in Figure 5.1. We observe that $C_{120,1}$, which corresponds to the submodule of dimension 8, has no proper non-zero submodules. This lack of proper submodules is the definition of irreducibility for codes.

□

For the code $C_{120,2}$, we observe the following properties:

i . The weight enumerator polynomial is $W(x) = 1 + 255x^{56} + 255x^{64} + x^{120}$.

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

iii . $C_{120,2}$ contains two non-trivial submodules.

Proposition 5.1.2. *Let G be a primitive group of degree 120 of the extension group $O_8^+(2) : 2$. The code $C_{120,2}$ possesses the following characteristics:*

i . It is doubly even.

ii . It is projective.

iii . It is decomposable.

Proof.

i . To prove $C_{120,2}$ is doubly even, we need to show that all codeword weights are divisible by 4. From the weight enumerator polynomial, we see that the non-zero weights are 56, 64, and 120. Indeed,

$$56 = 4 \cdot 14$$

$$64 = 4 \cdot 16$$

$$120 = 4 \cdot 30$$

Therefore, all weights are divisible by 4, and $C_{120,2}$ is doubly even.

ii . A code is projective if and only if its dual code has minimum distance at least 3. We are given that $C_{120,2}^{\perp}$ has a minimum weight of 4, which is greater than 3. Thus, $C_{120,2}$ is projective.

iii . The decomposability of $C_{120,2}$ follows from the existence of two non-trivial submodules. A module is said to be reducible if it can be decomposed into a direct product of two non-trivial component modules. The existence of two such non-zero submodules within $C_{120,2}$ establishes its reducibility.

□

Proposition 5.1.3. *Consider a highly symmetric permutation group G acting transitively on a set of 120 elements, where G is an extension of the orthogonal group $O_8^+(2)$ by the cyclic group of order 2. The dual codes $C_{120,1}^{\perp}$ and $C_{120,2}^{\perp}$ have the capacity to rectify up to 1 and 1.5 errors, respectively.*

Proof. We apply Theorem 1.2.12, which states that a code with minimum distance d can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors.

For $C_{120,1}^{\perp}$: The minimum distance $d = 3$. Thus, $\lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{3-1}{2} \rfloor = \lfloor 1 \rfloor = 1$.

For $C_{120,2}^{\perp}$: The minimum distance $d = 4$. Thus, $\lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{4-1}{2} \rfloor = \lfloor 1.5 \rfloor = 1$.

Therefore, $C_{120,1}^{\perp}$ can correct up to 1 error, and $C_{120,2}^{\perp}$ can correct up to 1 error. Note that while the calculation for $C_{120,2}^{\perp}$ yields 1.5, in practice it can only correct up to 1 error as we must take the floor of this value. □

Combinatorial Designs from Minimum Weight Codewords in Codes $C_{120,i}$

We determined designs formed by the set of coordinate positions of codewords with minimum weight wm in the codes $C_{120,i}$. Table 5.3 provides information about these designs in four columns:

Column 1: The code $C_{120,i}$ containing codewords of weight m.

Column 2: The parameters of the 1-design D_{wm} formed by the supports of minimum weight codewords.

Column 3: The number of blocks in the design D_{wm}.

Column 4: Whether the design D_{wm} is primitive or not under the action of the automorphism group $\mathrm{Aut}(C_{120,i})$ of the code.

Table 5.3: Combinatorial Designs from Minimum Weight Codewords in Codes $C_{120,i}$

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

Theorem 5.1.4. *Let G be the extension group $O_8^+(2):2$ and Ω be the primitive G-set of size 120 defined by the action of G on the cosets of its maximal subgroup $S_6(2):2$. Examine the significant binary codes $C_{120,1}$ and $C_{120,2}$ derived from the action of the group on the 120-element set. These codes exhibit the following characteristics:*

i) . The code $C_{120,1}$ is a self-orthogonal, geometrically significant, linear error-correcting code with parameters $[120, 8, 56]$ over the binary field. It generates a primitive symmetric 1-design with parameters 1-(120, 56, 56). The dual code of $C_{120,1}$ has parameters $[120, 112, 3]$. Moreover, $C_{120,1}$ is irreducible.

ii) . The code $C_{120,2}$ is a doubly even, projective $[120, 9, 56]$ binary code. Its dual code has parameters $[120, 111, 4]$. In contrast to $C_{120,1}$, the code $C_{120,2}$ is decomposable.

5.2 Analysis of the 135-Dimensional Representation

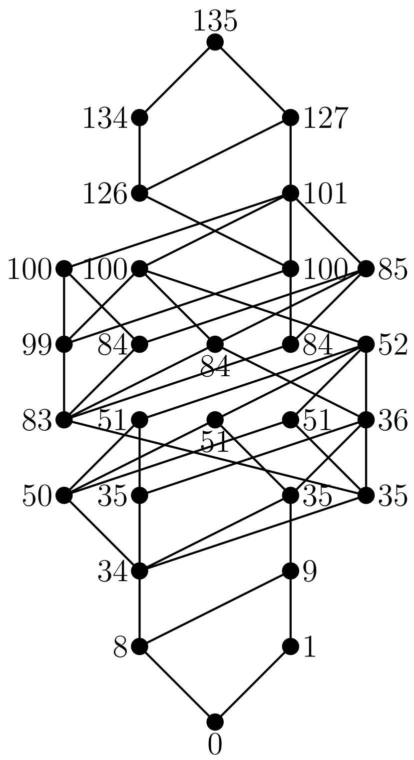
We constructed a permutation module of dimension 135, which is invariant under the action of a permutation group G on a finite set Ω of degree 135. We chose this permutation module as our object of study and recursively determined all its submodules. The decomposition of this permutation module yielded a total of 28 distinct submodules. Table 5.4 provides a comprehensive list of the invariant submodules of the permutation module over the finite field $\mathbb{F}_2$ for the representation of degree 135. The table displays the sizes of these smaller modules, where the column labeled m represents the size of each module, and the column labeled # indicates the quantity of modules of each size.

Table 5.4: Smaller modules from 135 Permutation Module

m	#	m	#	m	#
0	1	50	1	100	3
1	1	51	3	101	1
8	1	52	1	126	1
9	1	83	1	127	1
34	1	84	3	134	1
35	3	85	1	135	1
36	1	99	1		

The submodules identified from the decomposition of the 135-dimensional permutation module serve as the fundamental components for constructing a submodule lattice. Figure 5.2 presents a visual representation of this lattice, illustrating the hierarchical relationships between the submodules.

Figure 5.2: Lattice diagram depicting the submodule structure of the permutation module of degree 135



By examining the lattice diagram, we observed that the submodules with dimensions 8 and 1 exhibit the property of irreducibility. Table 5.5 presents the binary linear codes corresponding to the submodules derived from the permutation module of degree 135.

Table 5.5: Binary Linear codes of small dimensions of 135 Permutation Module

Name	Dimension	parameters
$C_{135,1}$	8	$[135, 8, 64]_2$
$C_{135,2}$	9	$[135, 9, 63]_2$
$C_{135,3}$	34	$[135, 34, 32]_2$
$C_{135,4}$	35	$[135, 35, 27]_2$

We analyzed the properties of the codes with small dimensions derived from the 135-dimensional permutation module. The following observations were made:

For the code $C_{135,1}$:

i) . The weight enumerator polynomial of $C_{135,1}$ is $W(x) = 1 + 135x^{64} + 120x^{72}$. We noted that the weights of the two non-zero codewords are divisible by 4.

ii) . The dual code $C_{135,1}^{\perp}$ has a minimum weight of 3.

iii) . $C_{135,1}$ contains no non-trivial submodules.

Proposition 5.2.1. *Suppose G is a primary group of order 135 within the extension group $O_8^+(2):2$. The code $C_{135,1}$ exhibits the following characteristics:*

i) . It is doubly even.

ii) . It is projective.

iii) . It is irreducible.

Proof.

i) . To prove that $C_{135,1}$ is doubly even, we examine its weight enumerator polynomial $W(x) = 1 + 135x^{64} + 120x^{72}$. All non-zero weights (64 and 72) are divisible by 4, satisfying the definition of a doubly even code.

ii) . A linear code is projective if its dual code has a minimum distance of at least 3. Since $C_{135,1}^{\perp}$ has a minimum weight of 3, $C_{135,1}$ is projective.

iii) . To prove irreducibility, we refer to the submodule lattice in Figure 5.2. The code $C_{135,1}$, corresponding to the submodule of dimension 8, has no non-trivial submodules, confirming its irreducibility.

□

For the code $C_{135,2}$:

i) . The dual code $C_{135,2}^{\perp}$ has a minimum weight of 4.

ii) . $C_{135,2}$ contains two non-trivial submodules of dimensions eight and one.

Proposition 5.2.2. *Suppose G is a primary group of order 135 within the extension group* $O_8^+(2):2$. *The code* $C_{135,2}$ *exhibits the following characteristics:*

i) . It is projective.

ii) . It is decomposable.

Proof.

i) . The dual code $C_{135,2}^{\perp}$ has a minimum weight of 4, which is greater than 3. By the definition of projective codes, $C_{135,2}$ is projective.

ii) . The decomposability of $C_{135,2}$ is evident from the submodule lattice in Figure 5.2. The presence of two non-trivial submodules of dimensions 8 and 1 confirms that $C_{135,2}$ is decomposable.

□

Proposition 5.2.3. *Let G be a primitive group of degree 135 in the extension group* $O_8^+(2):2$. *The dual codes* $C_{135,1}^{\perp}$ *and* $C_{135,2}^{\perp}$ *have the error-correcting capabilities of 1 and 1.5 errors, respectively.*

Proof. Theorem 1.2.12 states that a code with minimum distance d can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors. For $C_{135,1}^{\perp}$: The minimum distance $d = 3$. Therefore, $\lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{3-1}{2} \rfloor = \lfloor 1 \rfloor = 1$. For $C_{135,2}^{\perp}$: The minimum distance $d = 4$. Therefore, $\lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{4-1}{2} \rfloor = \lfloor 1.5 \rfloor = 1$. Thus, $C_{135,1}^{\perp}$ can correct up to 1 error, and $C_{135,2}^{\perp}$ can correct up to 1 error (as the floor function rounds down 1.5 to 1). □

Combinatorial Designs from Minimum Weight Codewords in Codes $C_{135,i}$

We examined the combinatorial designs formed by the supports of the codewords with minimum weight wm in the codes $C_{135,i}$. Table 5.6 presents the properties of these designs, with each column providing the following information:
Column 1: The code $C_{135,i}$ containing the codewords of weight m.

Column 2: The parameters of the 1-design D_{wm} formed by the supports of the minimum weight codewords.

Column 3: The number of blocks in the design D_{wm}.

Column 4: Classifies the design D_{wm} as primitive or non-primitive based on its behavior under the code's symmetry group.

Table 5.6: Combinatorial Designs from Minimum Weight Codewords in Codes $C_{135,i}$

Code	Design	Number of blocks	Primitive
$[135, 8, 64]_2$	1-(135,64,64)	135	Yes
$[135, 9, 63]_2$	1-(135,63,56)	120	Yes

Remark 5.2.4. *The 1-designs 1-(135,64,64) and 1-(135,63,56), generated by the codes $C_{135,1}$ and $C_{135,2}$ respectively, are both primitive.*

Theorem 5.2.5. *Let G be the extension group $O_8^+(2) : 2$, and let Ω be the primitive G-set of size 135 defined by the action of G on the cosets of its maximal subgroup $S_6(2) : 2$. Examine the significant binary codes $C_{135,1}$ and $C_{135,2}$ derived from the action of the group on the 135-element set. These codes exhibit the following characteristics:*

i) . The code $C_{135,1}$ is a doubly even, projective $[135, 8, 64]$ binary code. Its dual code has parameters $[135, 127, 3]$. Moreover, $C_{135,1}$ is irreducible and generates a primitive symmetric 1-design with parameters 1-(135,64,64).

ii) . The code $C_{135,2}$ is a projective $[135, 9, 63]$ binary code, with its dual code having parameters $[135, 126, 4]$. In contrast to $C_{135,1}$, the code $C_{135,2}$ is decomposable. It generates a primitive symmetric 1-design with parameters 1-(135,63,56).

5.3 Analysis of the 960-Dimensional Representation

A 960-dimensional representation space was constructed, invariant under the operations of a symmetry-preserving algebraic structure G acting on a discrete collection of elements Ω

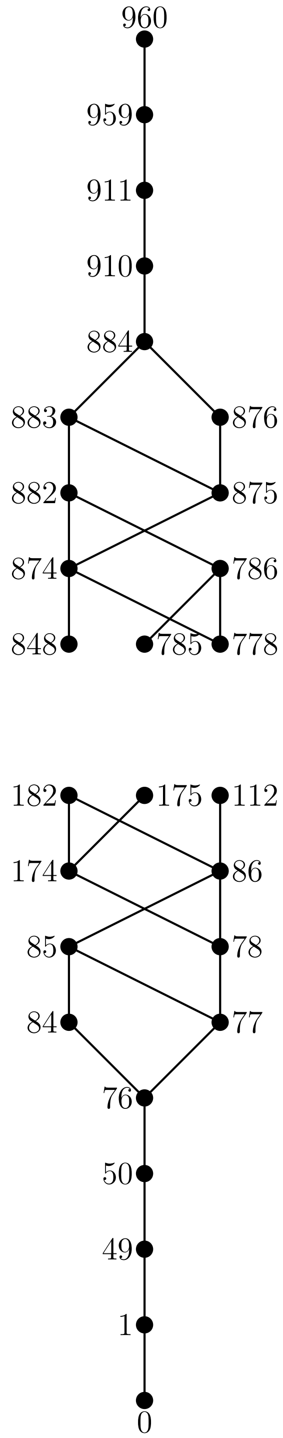
containing 960 distinct members. This representation space served as the primary object of study, and a systematic analysis was performed to identify its constituent invariant subspaces. The investigation revealed that this representation space decomposes into a total of 106 distinct invariant subspaces. Table 5.7 provides a comprehensive list of these invariant submodules of the permutation module over the finite field $\mathbb{F}_2$. The table presents the sizes of these smaller modules, where the column labeled m represents the size of each module, and the column labeled # indicates the quantity of modules of each size.

Table 5.7: Submodules from 960 Permutation Module

m	#	m	#	m	#	m	#	m	#	m	#
0	1	202	1	302	1	482	1	659	1	776	1
1	1	208	1	384	1	483	1	674	1	777	1
49	1	209	1	385	1	498	1	675	1	778	1
50	1	210	3	386	1	499	1	700	1	784	1
76	1	211	1	400	1	504	1	701	1	785	1
77	1	224	1	401	1	512	1	707	1	786	1
78	1	225	1	402	1	531	1	708	1	848	1
84	1	226	1	412	1	532	1	723	1	874	1
85	1	236	1	413	1	547	1	724	1	875	1
86	1	237	1	428	1	548	1	734	1	876	1
112	1	252	1	429	1	558	1	735	1	882	1
174	1	253	1	448	1	559	1	736	1	883	1
175	1	259	1	456	1	560	1	749	1	884	1
176	1	260	1	461	1	574	1	750	3	910	1
182	1	285	1	462	1	575	1	751	1	911	1
183	1	286	1	477	1	576	1	752	1	959	1
184	1	301	1	478	1	658	1	758	1	960	1

The submodules identified from the decomposition of the 960-dimensional permutation module serve as the fundamental components for constructing a submodule lattice. Figure 5.3 presents a visual representation of this lattice, illustrating the hierarchical relationships between the submodules.

Figure 5.3: Lattice diagram depicting the submodule structure of the permutation module of degree 960



Remark 5.3.1. *The high dimensionality of the submodules posed computational chal-*

lenges. As a result, our computational tool, MAGMA, was unable to generate the corresponding binary linear codes due to these large dimensions.

Chapter 6

Representations of Maximal subgroups of $L_3(4):2$

This chapter examines the representations of the extension group $L_3(4):2$. We present a detailed analysis of these representations and their properties. To conclude each representation, we consolidate our findings into a comprehensive theorem, which encapsulates the key results of our investigation.

6.1 Analysis of the 21-Dimensional Representation

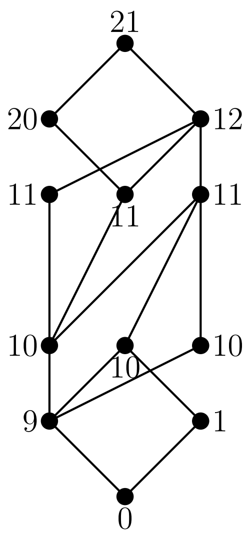
We developed a 21-dimensional permutation module that remains unchanged when subjected to the transformations induced by a symmetry-preserving algebraic structure G operating on a discrete collection of elements Ω containing 21 distinct members. This permutation module served as our primary object of study, and we systematically identified all its submodules through recursive analysis. Our investigation revealed that this permutation module decomposes into a total of 12 distinct submodules. Table 6.1 provides a comprehensive overview of these submodules. In this table, the column labeled m denotes the dimension of each submodule, while the column labeled # indicates the frequency of submodules with that dimension. It's important to note that for each submodule of dimension k, there exists a corresponding submodule of dimension $n-k$, where n is the dimension of the full module.

Table 6.1: Submodules from 21 Permutation Module.

m	#
0	1
1	1
9	1
10	3
11	3
12	1
20	1
21	1

The submodules identified from the decomposition of the 21-dimensional permutation module serve as the fundamental components for constructing a submodule lattice. Figure 6.1 presents a visual representation of this lattice, illustrating the hierarchical relationships between the submodules.

Figure 6.1: Lattice diagram depicting the submodule structure of the permutation module of degree 21



Through careful examination of the lattice diagram, we identify that the submodules of dimensions 9 and 1 exhibit the property of irreducibility. This observation has significant implications for understanding the fundamental building blocks of the module's structure.

To further elucidate the properties of these submodules, we generate binary linear codes corresponding to each submodule. These codes are presented in Table 6.2, offering a compact representation of the submodules in terms of coding theory.

Table 6.2: Binary Linear codes of small dimension from 21 Permutation Module

Name	Dimension	parameters
$C_{21,1}$	9	$[21, 9, 8]_2$
$C_{21,2}$	10	$[21, 10, 7]_2$
$C_{21,3}$	10	$[21, 10, 6]_2$
$C_{21,4}$	10	$[21, 10, 5]_2$
$C_{21,5}$	11	$[21, 11, 6]_2$
$C_{21,6}$	11	$[21, 11, 6]_2$
$C_{21,7}$	11	$[21, 11, 5]_2$
$C_{21,8}$	12	$[21, 12, 5]_2$
$C_{21,9}$	20	$[21, 20, 2]_2$

We conducted a detailed analysis of the codes derived from the submodules. The following properties were observed and rigorously examined:

For $C_{21,1}$:

i . The weight enumerator polynomial of $C_{21,1}$ is $W(x) = 1 + 210x^8 + 280x^{12} + 21x^{16}$. We observed that all non-zero weights (8, 12, and 16) are divisible by 4.

ii . The dual code $C_{21,1}^{\perp}$ has a minimum weight of 5.

iii . $C_{21,1}$ contains only the trivial submodule.

Proposition 6.1.1. *Let G be a primitive group of degree 21 of the extension group $L_3(4)$: 2. The code $C_{21,1}$ possesses the following characteristics:*

i. It is doubly even.

ii. It is projective.

iii. It is irreducible.

Proof.

i. To show $C_{21,1}$ is doubly even, we examine its weight polynomial $W(x) = 1+210x^8+280x^{12}+21x^{16}$. All non-zero weights (8, 12, and 16) are divisible by 4, satisfying the definition of a doubly even code.

ii. To establish projectivity, we observe that the dual code $C_{21,1}^{\perp}$ exhibits a minimum weight of 5. This property satisfies the criterion for projectivity. Consequently, we can conclude that $C_{21,1}$ is indeed projective.

iii. To prove irreducibility, we examine the submodule lattice in Figure 6.1. We observe that $C_{21,1}$, which corresponds to the submodule of dimension 9, has no proper non-zero submodules. This lack of proper submodules is the definition of irreducibility for codes.

□

For $C_{21,2}$, $C_{21,4}$, $C_{21,6}$, $C_{21,7}$, and $C_{21,8}$
The dual codes $C_{21,2}^{\perp}$, $C_{21,4}^{\perp}$, $C_{21,6}^{\perp}$, $C_{21,7}^{\perp}$, and $C_{21,8}^{\perp}$ have minimum weights of 6, 6, 7, 6, and 8 respectively.

Proposition 6.1.2. *Let G be a primitive group of degree 21 of the extension group $L_3(4):2$. The codes $C_{21,2}$, $C_{21,4}$, $C_{21,6}$, $C_{21,7}$, and $C_{21,8}$ are projective.*

Proof. A linear code is projective if and only if its dual code has minimum distance at least 3. We have observed that the minimum weights of the dual codes are 6, 6, 7, 6, and 8 respectively, all of which are greater than 3. Therefore, by definition, these codes are projective. □

For $C_{21,3}$:

i The weight enumerator polynomial of $C_{21,3}$ is $W(x) = 1+56x^6+210x^8+336x^{10}+280x^{12}+120x^{14}+21x^{16}$. We observed that all weights are divisible by 2.

ii The dual code $C_{21,3}^{\perp}$ has a minimum weight of 5.

iii $C_{21,3}$ contains two non-trivial submodules of dimensions 9 and 1.

Proposition 6.1.3. *Let G be a primitive group of degree 21 of the extension group $L_3(4)$: 2. The code $C_{21,3}$ possesses the following characteristics:*

i. It is even.

ii. It is projective.

iii. It is decomposable.

Proof.

i. To prove $C_{21,3}$ is even, we examine its weight enumerator polynomial. All weights (6, 8, 10, 12, 14, 16) are divisible by 2, satisfying the definition of an even code.

ii. For projectivity, we note that $C_{21,3}^{\perp}$ has a minimum weight of 5. As this is greater than 3, $C_{21,3}$ is projective by definition.

iii. The structural property of decomposability for $C_{21,3}$ is evident from its possession of two non-trivial submodules. This characteristic aligns with the formal definition of decomposability. The identification of these two non-trivial submodules within $C_{21,3}$ firmly establishes its decomposable nature.

□

For $C_{21,5}$ and $C_{21,9}$:

i The weights of the codewords of both codes are divisible by 2.

ii $C_{21,5}^{\perp}$ and $C_{21,9}^{\perp}$ have minimum weights of 5 and 21 respectively.

Proposition 6.1.4. *Let G be a primitive group of degree 21 of the extension group $L_3(4)$: 2. The codes $C_{21,5}$ and $C_{21,9}$ possess the following characteristics:*

i. They are even.

ii. They are projective.

Proof.

i. For both $C_{21,5}$ and $C_{21,9}$, all codeword weights are divisible by 2. This property, by definition, makes these codes even.

ii. The dual codes $C_{21,5}^{\perp}$ and $C_{21,9}^{\perp}$ have minimum weights of 5 and 21 respectively. Both of these values exceed 3, which is the threshold for projectivity. Therefore, both $C_{21,5}$ and $C_{21,9}$ are projective.

□

Combinatorial Designs from Minimum Weight Codewords in Codes $C_{21,i}$

We determined designs formed by the set of coordinate positions of codewords with minimum weight wm in the codes $C_{21,i}$. Table 6.3 provides information about these designs in four columns:

i . Column 1: The code $C_{21,i}$ containing codewords of weight m.

ii . Column 2: The parameters of the 1-design D_{wm} formed by the supports of minimum weight codewords.

iii . Column 3: The number of blocks in the design D_{wm}.

iv . Column 4: Whether the design D_{wm} is primitive or not under the action of the automorphism group $\mathrm{Aut}(C_{21,i})$ of the code.

Table 6.3: Combinatorial Designs from Minimum Weight Codewords in Codes $C_{21,i}$

Code	Design	Number of blocks	Primitive
$21,9,8]_2$	1-(21,8,80)	210	no
$[21,10,7]_2$	1-(21,7,40)	120	Yes
$[21,10,6]_2$	1-(21,6,16)	56	Yes
$[21,10,5]_2$	1-(21,5,5)	21	Yes
$[21,11,6]_2$	1-(21,6,48)	168	No
$[21,11,6]_2$	1-(21,6,16)	56	Yes
$[21,11,5]_2$	1-(21,5,5)	21	Yes
$[21,12,5]_2$	1-(21,5,5)	21	Yes
$[21,20,2]_2$	1-(21,2,20)	210	No

Remark 6.1.5. *From our analysis of the designs derived from the minimum weight codewords, we observe:*

i . *The designs 1-(21,7,40), 1-(21,6,16), and 1-(21,5,5) exhibit primitive structure under the action of their respective code automorphism groups.*

ii . *In contrast, the designs 1-(21,8,80), 1-(21,6,48), and 1-(21,2,20) are not primitive under this action.*

iii . *Notably, the codes* $[21,10,5]_2$*,* $[21,11,5]_2$*, and* $[21,12,5]_2$*, despite having different parameters, all generate the same design 1-(21,5,5).*

Theorem 6.1.6. *Let G denote the extension group $L_3(4):2$, and Ω represent the primitive G-set of size 21, defined by G's action on the cosets of its maximal subgroup* $2:A_5:2^4$*. We consider the significant binary codes $C_{21,1}, C_{21,2}, \ldots, C_{21,8}$ derived from the 21-dimensional permutation module. These codes exhibit the following characteristics:*

i . *The code $C_{21,1}$ is a self-orthogonal, geometrically significant, linear error-correcting code with parameters* $[21,9,8]$ *over the binary field. Its dual code has parameters* $[21,12,5]$*. Furthermore, $C_{21,1}$ possesses the property of irreducibility.*

ii . *The codes $C_{21,2}, C_{21,4}, C_{21,6}, C_{21,7}$, and $C_{21,8}$ are projective binary codes with parameters* $[21,10,7]$*,* $[21,10,5]$*,* $[21,11,6]$*,* $[21,11,5]$*, and* $[21,12,5]$ *respectively. Their* *corresponding dual codes have parameters* $[21, 11, 6]$, $[21, 11, 6]$, $[21, 10, 7]$, $[21, 10, 6]$, *and* $[21, 9, 8]$.

iii . *The code* $C_{21,3}$ *is an even and projective* $[21, 10, 6]$ *binary code. Its dual code has parameters* $[21, 11, 5]$. *Furthermore,* $C_{21,3}$ *is decomposable.*

iv . *The codes* $C_{21,5}$ *and* $C_{21,9}$ *are even and projective binary codes with parameters* $[21, 11, 6]$ *and* $[21, 20, 2]$ *respectively. Their dual codes have parameters* $[21, 10, 5]$ *and* $[21, 1, 21]$.

v . *The codes* $C_{21,2}, C_{21,3}, C_{21,4}, C_{21,6}, C_{21,7}$, *and* $C_{21,8}$ *generate primitive symmetric 1-designs with parameters 1-(21,7,40), 1-(21,6,16), 1-(21,5,5), 1-(21,6,16), 1-(21,5,5), and 1-(21,5,5) respectively.*

6.2 Analysis of the 56-Dimensional Representation

We developed a 56-dimensional permutation module that remains unchanged when subjected to the transformations induced by a symmetry-preserving algebraic structure G operating on a discrete collection of elements Ω containing 56 distinct members. This permutation module served as our primary object of study, and we systematically identified all its submodules through recursive analysis.

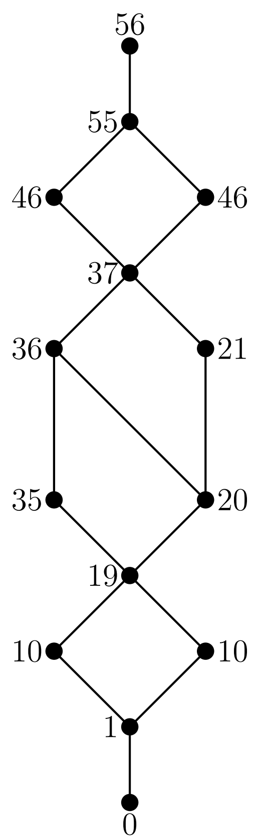
Our investigation revealed that this permutation module decomposes into a total of 14 distinct submodules. Table 6.4 provides a comprehensive overview of these submodules. In this table, the column labeled m denotes the dimension of each submodule, while the column labeled # indicates the frequency of submodules with that dimension.

Table 6.4: Submodules from 56 Permutation Module of $L_3(4):2$

m	#	m	#
0	1	35	1
1	1	36	1
10	2	37	1
19	1	46	2
20	1	55	1
21	1	56	1

The submodules identified from the decomposition of the 56-dimensional permutation module serve as the fundamental components for constructing a submodule lattice. Figure 6.2 presents a visual representation of this lattice, illustrating the hierarchical relationships between the submodules.

Figure 6.2: Lattice diagram depicting the submodule structure of the permutation module of degree 56



Through careful examination of the lattice diagram, we identify that the submodule of dimension one exhibits the property of irreducibility. This observation has significant implications for understanding the fundamental building blocks of the module's structure. To further elucidate the properties of these submodules, we generate binary linear codes corresponding to each submodule. These codes are presented in Table 6.5, offering a compact representation of the submodules in terms of coding theory.

Table 6.5: Binary Linear codes of small dimensions of degree 56 of $L_3(4):2$.

Name	Dimension	parameters
$C_{56,1}$	10	$[56,10,16]_2$
$C_{56,2}$	19	$[56,19,16]_2$
$C_{56,3}$	20	$[56,20,10]_2$
$C_{56,4}$	21	$[56,21,10]_2$

We conducted a detailed analysis of the properties of selected codes derived from the submodules. Our findings are as follows:

For codes $C_{56,1}$ and $C_{56,2}$:

i . All codeword weights are divisible by 4.

ii . The dual codes $C_{56,1}^{\perp}$ and $C_{56,2}^{\perp}$ have minimum weights of 4 and 6 respectively.

Proposition 6.2.1. *Let G be a primitive group of degree 56 of the extension group $L_3(4):2$. Then the codes $C_{56,1}$ and $C_{56,2}$ are:*

i . Doubly even

ii . Projective

Proof.

i . To establish the doubly even nature of $C_{56,1}$ and $C_{56,2}$, we note a fundamental characteristic of their codewords: the weight of each codeword is invariably a multiple of 4. This property aligns precisely with the defining criterion for doubly even codes.

ii . For projectivity, we note that the dual codes have minimum weights of 4 and 6 respectively. By definition, a code is projective if its dual code has minimum distance at least 3. Both 4 and 6 exceed this threshold, thus $C_{56,1}$ and $C_{56,2}$ are projective.

□

For codes $C_{56,3}$ and $C_{56,4}$:

i . All codeword weights are divisible by 2.

ii . The dual codes $C_{56,3}^{\perp}$ and $C_{56,4}^{\perp}$ have minimum weights of 6 and 8 respectively.

Proposition 6.2.2. *Let G be a primitive group of degree 56 of the extension group $L_3(4):2$. Then the codes $C_{56,3}$ and $C_{56,4}$ are:*

i . Even

ii . Projective

Proof.

i . To prove that $C_{56,3}$ and $C_{56,4}$ are even, we observe that all codeword weights are divisible by 2, which is the definition of an even code.

ii . For projectivity, we note that the dual codes have minimum weights of 6 and 8 respectively. As both these values exceed 3, $C_{56,3}$ and $C_{56,4}$ are projective by the same reasoning as in the previous proposition.

□

Combinatorial Designs Derived from Minimum Weight Codewords in $C_{56,i}$

In our analysis, we focused on the combinatorial structures that emerge from the minimum weight codewords in the codes $C_{56,i}$. Specifically, we examined the designs formed by the support sets of these codewords. Our findings are presented in Table 6.6, which is organized into four columns. The first column identifies the code $C_{56,i}$ and its corresponding weight m. Column 2 delineates the defining characteristics of the emergent 1-design D_{wm}, encapsulating its structural properties in a concise parametric form. The subsequent column, Column 3, enumerates the total number of blocks constituting each design D_{wm}, offering insight into its combinatorial complexity. Finally, the fourth column indicates whether the design D_{wm} exhibits primitivity under the action of the code's automorphism group Aut(C).

Table 6.6: Combinatorial Designs Derived from Minimum Weight Codewords in $C_{56,i}$

Code	Design	Number of blocks	Primitive
$[56, 10, 16]_2$	1-(56,16,6)	21	Yes
$[56, 19, 16]_2$	1-(56,16,492)	1722	No
$[56, 20, 10]_2$	1-(56,10,10)	56	Yes
$[56, 21, 10]_2$	1-(56,10,10)	56	Yes
$[56, 35, 8]_2$	1-(56,8,405)	2835	No

Remark 6.2.3. *The analysis of designs derived from our codes revealed several noteworthy characteristics:*

i. The designs 1-(56,16,6) and 1-(56,10,10) exhibit primitive properties.

ii. Conversely, the designs 1-(56,16,492) and 1-(56,8,405) lack primitivity.

iii. The code $[56, 10, 16]_2$ *generates the design 1-(56,16,6), while both codes* $[56, 20, 10]_2$ *and* $[56, 21, 10]_2$ *produce an identical design, 1-(56,10,10).*

Theorem 6.2.4. *Let G symbolize the extension group $L_3(4) : 2$, and Ω denote a primitive algebraic structure of order 56, arising from the group G's transformations on the quotient space formed by the cosets of $2 : A_6$. We examine the significant binary codes $C_{56,1}, C_{56,2}, C_{56,3}, C_{56,4}$, and $C_{56,5}$ derived from the 56-dimensional permutation module. These codes exhibit the following notable characteristics:*

i. $C_{56,1}$ *and* $C_{56,2}$ *are doubly even and projective binary codes with parameters* $[56, 10, 16]$ *and* $[56, 19, 16]$ *respectively. Their corresponding dual codes have parameters* $[56, 46, 4]$ *and* $[56, 37, 6]$.

ii. $C_{56,3}$ *and* $C_{56,4}$ *are even and projective binary codes with parameters* $[56, 20, 10]$ *and* $[56, 21, 10]$ *respectively. Their dual codes have parameters* $[56, 36, 6]$ *and* $[56, 35, 8]$.

iii. $C_{56,1}, C_{56,3}$*, and* $C_{56,4}$ *each generate primitive symmetric 1-designs: 1-(56,16,6), 1-(56,10,10), and 1-(56,10,10) respectively.*

6.3 Analysis of the 120-Dimensional Representation

Our investigation focused on a 120-dimensional permutation module. This module remains unchanged when subjected to the transformations induced by a symmetry-preserving algebraic structure G operating on a discrete collection of elements Ω containing 120 distinct members. Our investigation focused on this permutation module as our principal subject of inquiry, and we methodically uncovered its complete submodule structure through an iterative decomposition process.

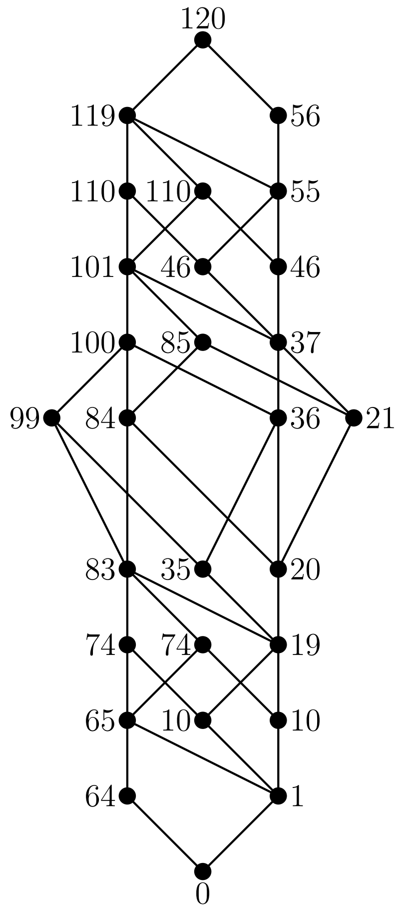
Our investigation revealed that this permutation module decomposes into a total of 28 distinct submodules. To provide a clear overview of this decomposition, we present the dimensions of these submodules along with their respective frequencies in Table 6.7.

Table 6.7: Submodules from 120 Permutation Module of $L_3(4):2$

m	#	m	#	m	#
0	1	37	1	84	1
1	1	46	2	85	1
10	2	55	1	99	1
19	1	56	1	100	1
20	1	64	1	101	1
21	1	65	1	110	1
35	1	74	2	119	1
36	1	83	1	120	1

In Table 6.7, the column labeled m denotes the dimension of each submodule, while the column labeled # indicates the frequency of submodules with that dimension. To provide a visual representation of the hierarchical relationships between these submodules, we present a lattice diagram in Figure 6.3.

Figure 6.3: Lattice diagram depicting the submodule structure of the permutation module of degree 120



Through careful examination of the lattice diagram, we identify that the submodules of dimensions 64 and 1 exhibit the property of irreducibility. This observation has significant implications for understanding the fundamental building blocks of the module's structure. To further elucidate the properties of these submodules, we generate binary linear codes corresponding to each submodule. These codes are presented in Table 6.8, offering a compact representation of the submodules in terms of coding theory.

Table 6.8: Binary Linear codes of small dimensions of 120 permutation Module of $L_3(4):2$

Name	Dimension	parameters
$C_{120,1}$	10	$[120, 10, 40]_2$
$C_{120,2}$	19	$[120, 19, 32]_2$
$C_{120,3}$	20	$[120, 20, 30]_2$
$C_{120,4}$	21	$[120, 21, 30]_2$

We now examine the properties of codes $C_{120,1}$, $C_{120,2}$, $C_{120,3}$, and $C_{120,4}$:

For $C_{120,1}$ and $C_{120,2}$:

i . All codeword weights are divisible by 4.

ii . The dual codes $C_{120,1}^{\perp}$ and $C_{120,2}^{\perp}$ have minimum weights of 4 and 6 respectively.

Proposition 6.3.1. *Let G be a primitive group of degree 120 of the extension group $L_3(4):2$. Then $C_{120,1}$ and $C_{120,2}$ are:*

i . Doubly even

ii . Projective

Proof.

i . To establish the doubly even nature of $C_{120,1}$ and $C_{120,2}$, we note a fundamental characteristic of their codewords: the weight of each codeword is invariably a multiple of 4. This property aligns precisely with the defining criterion for doubly even codes.

ii . For projectivity, we note that the dual codes have minimum weights of 4 and 6 respectively. By definition, a code is projective if its dual code has minimum distance at least 3. Both 4 and 6 exceed this threshold, thus $C_{120,1}$ and $C_{120,2}$ are projective.

□

For $C_{120,3}$ and $C_{120,4}$:

i . All codeword weights are divisible by 2.

ii . The dual codes $C_{120,3}^{\perp}$ and $C_{120,4}^{\perp}$ have minimum weights of 6 and 8 respectively.

Proposition 6.3.2. *Let G be a primitive group of degree 120 of the extension group $L_3(4):2$. Then $C_{120,3}$ and $C_{120,4}$ are:*

i . Even

ii . Projective

Proof.

i . To prove that $C_{120,3}$ and $C_{120,4}$ are even, we observe that all codeword weights are divisible by 2, which is the definition of an even code.

ii . For projectivity, we note that the dual codes have minimum weights of 6 and 8 respectively. As both these values exceed 3, $C_{120,3}$ and $C_{120,4}$ are projective by the same reasoning as in the previous proposition.

□

Combinatorial Designs from Minimum Weight Codewords in Codes $C_{120,i}$

We determined designs formed by the set of coordinate positions of codewords with minimum weight wm in the codes $C_{120,i}$. Table 6.9 provides information about these designs in four columns:

i. Column 1: The code $C_{120,i}$ containing codewords of weight m.

ii. Column 2: The parameters of the 1-design D_{wm} formed by the supports of minimum weight codewords.

iii. Column 3: The number of blocks in the design D_{wm}.

iv. Column 4: Whether the design D_{wm} is primitive or not under the action of the automorphism group $\mathrm{Aut}(C_{120,i})$ of the code.

Table 6.9: Combinatorial Designs from Minimum Weight Codewords in Codes $C_{120,i}$ of $L_3(4):2$

Code	Design	Number of blocks	Primitive
$[120, 10, 40]_2$	1-(120,40,7)	21	Yes
$[120, 19, 32]_2$	1-(120,32,28)	105	No
$[120, 20, 30]_2$	1-(120,30,14)	56	Yes
$[120, 21, 30]_2$	1-(120,30,14)	56	Yes

Remark 6.3.3. *From our analysis of the designs derived from the minimum weight codewords, we observe:*

i. The designs 1-(120,40,7) and 1-(120,30,14) exhibit primitive structure under the action of their respective code automorphism groups.

ii. In contrast, the design 1-(120,32,28) is not primitive under this action.

iii. Notably, the codes $[120, 20, 30]_2$ *and* $[120, 21, 30]_2$*, despite having different parameters, both generate the same design 1-(120,30,14).*

Theorem 6.3.4. *Let G be the extension group* $L_3(4) : 2$ *and* Ω *be the primitive G-set of size 120 defined by the action of G on the cosets of its maximal subgroup* $L_2(7) : 2$*. Consider the non-trivial binary codes* $C_{120,1}, C_{120,2}, C_{120,3}$ *and* $C_{120,4}$ *obtained from the permutation module of degree 120. The following properties hold:*

i. The codes $C_{120,1}$ *and* $C_{120,2}$ *are doubly even and projective binary codes with parameters* $[120, 10, 40]$ *and* $[120, 19, 32]$ *respectively. Their corresponding dual codes have parameters* $[120, 110, 4]$ *and* $[120, 101, 6]$.

ii. The codes $C_{120,3}$ *and* $C_{120,4}$ *are even and projective binary codes with parameters* $[120, 20, 30]$ *and* $[120, 21, 30]$ *respectively. Their dual codes have parameters* $[120, 100, 6]$ *and* $[120, 99, 6]$.

iii. Furthermore, $C_{120,1}$*,* $C_{120,3}$*, and* $C_{120,4}$ *generate primitive symmetric 1-designs with parameters 1-(120, 40, 7), 1-(120,30,14), and 1-(120,30,14) respectively.*

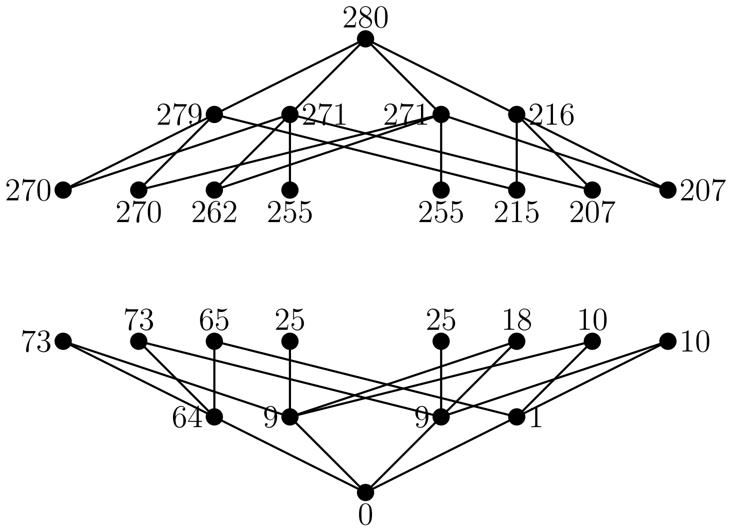
6.4 Analysis of the 280-Dimensional Representation

We developed a 280-dimensional permutation module that remains unchanged when subjected to the transformations induced by a symmetry-preserving algebraic structure G operating on a discrete collection of elements Ω containing 280 distinct members. This permutation module was chosen as the primary object of study, and a recursive process was employed to identify all its submodules. The decomposition revealed that this 280-dimensional permutation module splits into a total of 2604 distinct submodules. Table 6.10 provides a summary of these submodules, where the column labeled m indicates the dimension of each submodule, and the column # specifies the count of submodules corresponding to each dimension.

Table 6.10: Submodules from 280 Permutation Module of $L_3(4):2:2$

m	#	m	#	m	#	m	#	m	#	m	#
0	1	69	3	108	20	144	39	178	6	220	2
1	1	70	9	109	46	145	45	179	21	223	2
9	2	71	29	110	53	146	17	180	1	224	7
10	2	72	7	111	35	147	3	181	31	225	19
18	1	73	4	112	7	150	2	182	9	226	7
19	3	74	2			151	3	187	1	227	3
20	3	78	2	113	1	152	9	188	9	228	3
21	1	79	6	114	7	153	49	189	53	229	3
25	2	80	32	115	21	154	67	190	63	230	1
26	2	81	16	116	45	155	59	191	51	234	10
34	3	82	9	117	21	156	11	192	7	235	10
35	13	83	3	118	11	157	1	193	1	236	6
36	9	84	3	119	19	159	2	195	1	243	3
37	3	85	1	120	7	160	7	196	3	244	9
44	6	87	1	121	2	161	19	197	3	245	13
45	10	88	7	123	1	162	13	198	9	246	3
46	10	89	51	124	11	163	21	199	16	254	2
50	1	90	63	125	59	164	45	200	32	255	2
51	3	91	53	126	67	165	22	201	6	259	1
52	3	92	9	127	49	166	7	202	2	260	3
53	3	93	1	128	9	167	1	206	2	261	3
54	7	98	9	129	3	168	7	207	4	262	1
55	19	99	31	130	2	169	35	208	7	270	2
56	7	100	51	133	3	170	53	209	29	271	2
57	2	101	21	134	17	171	46	210	9	279	1
60	2	102	6	135	45	172	20	211	3	280	1
61	6	103	1	136	39	173	36	214	2		
62	6	104	7	137	8	174	43	215	3		
64	3	105	35	138	2	175	35	216	3		
65	3	106	43	142	2	176	7	218	6		
66	2	107	36	143	8	177	1	219	6		

Figure 6.4: Lattice diagram portraying a subset of the submodule structure for the permutation module of dimension 280



Examination of the partial lattice diagram revealed that the submodules with dimensions 64, 9, and 1 exhibit the property of irreducibility. Table 6.11 presents the binary linear codes derived from the submodules of smaller dimensions within the 280-dimensional permutation module of the group extension $L_3(4):2$.

Table 6.11: Low-dimensional binary linear codes obtained from the permutation module of degree 280 associated with $L_3(4):2$

Name	Dimension	Parameters	Name	Dimension	Parameters
$C_{280,1}$	9	$[280,9,136]_2$	$C_{280,9}$	21	$[280,21,84]_2$
$C_{280,2}$	10	$[280,10,120]_2$	$C_{280,10}$	25	$[280,25,64]_2$
$C_{280,3}$	18	$[280,18,112]_2$	$C_{280,11}$	26	$[280,26,64]_2$
$C_{280,4}$	19	$[280,19,84]_2$			
$C_{280,5}$	19	$[280,19,100]_2$			
$C_{280,6}$	19	$[280,19,88]_2$			
$C_{280,7}$	20	$[280,20,84]_2$			
$C_{280,8}$	20	$[280,20,84]_2$			

For the codes $C_{280,1}$ through $C_{280,16}$:

i. The weights of all codewords in these sixteen codes are divisible by 4.

ii. The dual codes $C_{280,1}^{\perp}$, $C_{280,2}^{\perp}$, $\cdots$, $C_{280,16}^{\perp}$ have minimum weights of 3, 3, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4 and 4 respectively.

Proposition 6.4.1. *Consider G as a fundamental symmetry group of order 280 embedded within the larger algebraic structure* $L_3(4) : 2$*. The linear codes* $C_{280,1}$, $C_{280,2}$, $\cdots$, $C_{280,16}$ *derived from this group exhibit the following notable characteristics:*

i. They are doubly even.

ii. They are projective.

Proof.

i. To prove that $C_{280,1}, C_{280,2}, \cdots, C_{280,16}$ are doubly even, we observe that all codeword weights are divisible by 4, which satisfies the definition of a doubly even code.

ii. For projectivity, we note that the dual codes $C^{\perp}_{280,1}, C^{\perp}_{280,2}, \cdots, C^{\perp}_{280,16}$ have minimum weights of at least 3. By Definition, a code is projective if its dual code has a minimum distance of at least 3. Therefore, $C_{280,1}, C_{280,2}, \cdots, C_{280,16}$ are projective.

□

Proposition 6.4.2. *Consider G as a fundamental symmetry group of order 280 embedded within the larger algebraic structure* $L_3(4) : 2$*. The dual codes* $C^{\perp}_{280,1}$ *and* $C^{\perp}_{280,2}$ *possess error-correcting capabilities allowing them to rectify up to 1 error, whereas the dual codes* $C^{\perp}_{280,1}$, $C^{\perp}_{280,2}$, $\cdots$, $C^{\perp}_{280,16}$ *demonstrate enhanced robustness, with the ability to correct up to 1.5 errors.*

Proof.

By applying Theorem 1.2.12, which states that a code with minimum distance d can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors, we obtain the following: For $C^{\perp}_{280,1}$ and $C^{\perp}_{280,2}$: The minimum distance $d = 3$. Thus, $\lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{3-1}{2} \rfloor = \lfloor 1 \rfloor = 1$. For $C^{\perp}_{280,3}, \cdots, C^{\perp}_{280,16}$: The minimum distance $d = 4$. Thus, $\lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{4-1}{2} \rfloor = \lfloor 1.5 \rfloor = 1$. Therefore, $C^{\perp}_{280,1}$ and $C^{\perp}_{280,2}$ can correct up to 1 error, while $C^{\perp}_{280,3}, \cdots, C^{\perp}_{280,16}$ can correct up to 1 error (as the floor function rounds down 1.5 to 1). □

6.5 Combinatorial Designs from Minimum Weight Codewords in Codes $C_{280,i}$

We examined the combinatorial designs formed by the supports of the codewords with minimum weight wm in the codes $C_{280,i}$. Table 6.12 presents the properties of these designs, with each column providing the following information:

i. Column 1: The code $C_{280,i}$ containing the codewords of weight m.

ii. Column 2: The parameters of the 1-design D_{wm} formed by the supports of the minimum weight codewords.

iii. Column 3: The number of blocks in the design D_{wm}.

iv. Column 4: An indication of whether the design D_{wm} is primitive or not under the action of the automorphism group $\mathrm{Aut}(C_{280,i})$ of the code.

Table 6.12: Combinatorial Designs from Minimum Weight Codewords in Codes $C_{280,i}$ of $L_3(4):2$

Code	Design	Number of blocks	Primitive
$[280, 9, 136]_2$	1-(280,136,136)	280	Yes
$[280, 10, 120]_2$	1-(280,120,9)	21	Yes
$[280, 18, 112]_2$	1-(280,112,1179)	2940	No
$[280, 19, 84]_2$	1-(280,84,36)	120	Yes
$[280, 19, 100]_2$	1-(280,100,240)	672	No
$[280, 19, 88]_2$	1-(280,88,33)	105	No
$[280, 20, 84]_2$	1-(280,84,108)	360	No
$[280, 20, 84]_2$	1-(280,84,36)	120	Yes
$[280, 21, 84]_2$	1-(280,84,108)	360	No
$[280, 25, 64]_2$	1-(280,64,72)	315	No
$[280, 26, 64]_2$	1-(280,64,72)	315	No

Remark 6.5.1. *From our analysis of the designs derived from the minimum weight codewords, we observe:*

i. The designs 1-(280,136,136), 1-(280,120,9), and 1-(280,84,36) exhibit primitive structure under the action of their respective code automorphism groups.

ii. *In contrast, the designs 1-(280,112,1179), 1-(280,100,240), 1-(280,88,33), 1-(280,84,108), and 1-(280,64,72) are not primitive under this action.*

iii. *The codes* $[280, 19, 84]_2$ *and* $[280, 20, 84]_2$*, despite having different parameters, both generate the same design 1-(280,84,36). Similarly, the codes* $[280, 25, 64]_2$ *and* $[280, 26, 64]_2$ *yield the identical design 1-(280,64,72).*

Theorem 6.5.2. *Let* G *be the extension group* $L_3(4) : 2$*, and let* Ω *be the primitive* G*-set of size 280 defined by the action of* G *on the cosets of its maximal subgroup* $2^4 \times 3^2$*. Consider the non-trivial binary codes* $C_{280,1}, C_{280,2}, \ldots, C_{280,11}$ *obtained from the permutation module of degree 280. The following properties hold:*

i. *The codes* $C_{280,1}$ *through* $C_{280,11}$ *are doubly even and projective binary codes with parameters* $[280, 9, 136]$, $[280, 10, 120]$, $[280, 18, 112]$, $[280, 19, 84]$, $[280, 19, 100]$, $[280, 19, 88]$, $[280, 20, 84]$, $[280, 20, 84]$, $[280, 21, 84]$, $[280, 25, 64]$, *and* $[280, 26, 64]$ *respectively. Their corresponding dual codes have parameters* $[280, 271, 3]$, $[280, 270, 4]$, $[280, 262, 4]$, $[280, 261, 4]$, $[280, 261, 4]$, $[280, 261, 4]$, $[280, 260, 4]$, $[280, 260, 4]$, $[280, 259, 4]$, $[280, 255, 4]$, *and* $[280, 254, 4]$.

ii. *The codes* $C_{280,1}, C_{280,2}, C_{280,4}$*, and* $C_{280,8}$*, with parameters* $[280, 9, 136]$, $[280, 10, 120]$, $[280, 19, 84]$, *and* $[280, 20, 84]$ *respectively, generate primitive symmetric 1-designs with parameters 1-(280,136,136), 1-(280,120,9), 1-(280,84,36), and 1-(280,84,36).*

Chapter 7

Representations of Maximal Subgroups of $L_3(4) : 2^2$

In this chapter, we explored the representations of the extension group $L_3(4) : 2^2$. Our investigation focused on five specific representations, corresponding to the degrees 56, 105, 120, 280, and 336. The key findings from our analysis are encapsulated in a comprehensive theorem presented at the conclusion of each representation.

7.1 Analysis of the 56-Dimensional Representation

We developed a 56-dimensional permutation module that remains unchanged when subjected to the transformations induced by a symmetry-preserving algebraic structure G operating on a discrete collection of elements Ω containing 56 distinct members. This permutation module served as our principal subject of inquiry, and we methodically uncovered its complete submodule structure through an iterative decomposition process. Our investigation revealed that this permutation module decomposes into a total of 10 distinct submodules. Table 7.1 provides an overview of these submodules, where the column labeled m denotes the dimension of each submodule, and the column labeled # indicates the frequency of submodules with that dimension.

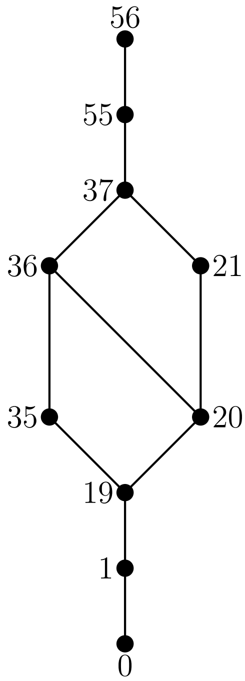
Table 7.1: Submodules derived from the permutation module of degree 56 associated with $L_3(4) : 2^2$

m	#	m	#
0	1	36	1
1	1	37	1
19	1	55	1
20	1	56	1
21	1		
35	1		

Figure 7.1 presents a visual representation of the lattice diagram, illustrating the hierar-

chical relationships between the submodules derived from the 56-dimensional permutation module.

Figure 7.1: Lattice diagram portraying the submodule structure of the permutation module of degree 56



Through careful examination of the hierarchical structure depicted in the lattice diagram, we identify that the one-dimensional submodule possesses the fundamental characteristic of irreducibility. Table 7.2 presents the binary linear codes corresponding to the submodules, offering a compact representation of these structures.

Table 7.2: Low-dimensional binary linear codes derived from the submodules of the permutation module associated with $L_3(4) : 2^2$

Name	Dimension	parameters
$C_{56,1}$	19	$[56, 19, 16]_2$
$C_{56,2}$	20	$[56, 20, 10]_2$
$C_{56,3}$	21	$[56, 21, 10]_2$

We analyzed the properties of several codes derived from the submodules. The following observations were made:

For code $C_{56,1}$:

i . All codeword weights are divisible by 4.

ii . The dual code $C_{56,1}^{\perp}$ has a minimum weight of 6.

Proposition 7.1.1. *Consider G as a fundamental symmetry group of order 56 embedded within the larger algebraic structure $L_3(4) : 2^2$. The linear code $C_{56,1}$ derived from this group exhibits the following notable characteristics:*

i . It is doubly even.

ii . It is projective.

Proof.

i . To prove $C_{56,1}$ is doubly even, we examine its weight distribution. All non-zero weights are divisible by 4, satisfying the definition of a doubly even code.

ii . For projectivity, we note that $C_{56,1}^{\perp}$ has a minimum weight of 6. As this exceeds 3, $C_{56,1}$ is projective by definition.

□

For codes $C_{56,2}$ and $C_{56,3}$:

i . Every codeword in this code exhibits a weight that is invariably an even integer.

ii . The dual codes $C_{56,2}^{\perp}$ and $C_{56,3}^{\perp}$ have minimum weights of 6 and 8 respectively.

Proposition 7.1.2. *Let G be a primitive group of degree 56 of the extension group $L_3(4) : 2^2$. The codes $C_{56,2}$ and $C_{56,3}$ have the following properties:*

i . They are even.

ii . They are projective.

Proof.

i . For both $C_{56,2}$ and $C_{56,3}$, all codeword weights are divisible by 2. This property, by definition, makes these codes even.

ii . The dual codes $C_{56,2}^{\perp}$ and $C_{56,3}^{\perp}$ have minimum weights of 6 and 8 respectively. Both of these values exceed 3, which is the threshold for projectivity. Therefore, both $C_{56,2}$ and $C_{56,3}$ are projective.

□

Combinatorial Designs Derived from Minimum Weight Codewords in $C_{56,i}$

In our analysis, we focused on the combinatorial structures that emerge from the minimum weight codewords in the codes $C_{56,i}$. Specifically, we examined the designs formed by the support sets of these codewords. Our findings are presented in Table 7.3, which is organized into four columns. The first column identifies the code $C_{56,i}$ and its corresponding weight m. Column 2 delineates the defining characteristics of the emergent 1-design D_{wm}, encapsulating its structural properties in a concise parametric form. The subsequent column, Column 3, enumerates the total number of blocks constituting each design D_{wm}, offering insight into its combinatorial complexity. Finally, the fourth column indicates whether the design D_{wm} exhibits primitivity under the action of the code's automorphism group Aut(C).

Table 7.3: Combinatorial Designs Derived from Minimum Weight Codewords in $C_{56,i}$ of $L_3(4) : 2^2$

Code	Design	Number of blocks	Primitive
$[56, 19, 16]_2$	1-(56,16,492)	1722	No
$[56, 20, 10]_2$	1-(56,10,10)	56	Yes
$[56, 21, 10]_2$	1-(56,10,10)	56	Yes

Remark 7.1.3. *The analysis of designs derived from our codes revealed several noteworthy characteristics:*

i. The design 1-(56,10,10) exhibits primitive properties and is generated by two distinct codes: $[56, 20, 10]_2$ *and* $[56, 21, 10]_2$.

ii. In contrast, the design 1-(56,16,492) lacks primitivity.

Theorem 7.1.4. *Let G symbolize the extension group* $L_3(4) : 2^2$*, and* Ω *denote a primitive algebraic structure of order 56, arising from the group G's transformations on the quotient space formed by the cosets of* $A_6 : 2^2$. *We examine the significant binary codes* $C_{56,1}$, $C_{56,2}$, *and* $C_{56,3}$ *derived from the 56-dimensional permutation module. These codes exhibit the following notable characteristics:*

i. The code $C_{56,1}$ *is a self-orthogonal, geometrically significant linear error-correcting code with parameters* $[56, 19, 16]$ *over the binary field.*

ii. $C_{56,2}$ *and* $C_{56,3}$ *are even and projective binary codes with parameters* $[56, 20, 10]$ *and* $[56, 21, 10]$ *respectively. Their corresponding dual codes have parameters* $[56, 36, 6]$ *and* $[56, 35, 8]$. *Moreover, these two codes each generate a primitive symmetric 1-design with parameters 1-(56,10,10).*

7.2 Analysis of the 105-Dimensional Representation

We developed a 105-dimensional permutation module that remains unchanged when subjected to the transformations induced by a symmetry-preserving algebraic structure G operating on a discrete collection of elements Ω containing 105 distinct members. This permutation module served as our principal subject of inquiry, and we methodically uncovered its complete submodule structure through an iterative decomposition process.

Our analysis revealed that this representation space decomposes into a total of 52 distinct invariant subspaces. Table 7.4 provides a comprehensive list of the invariant submodules of the permutation module over the finite field $\mathbb{F}_2$ for the representation of degree

105. The table categorizes these submodules based on their size. The m column specifies the size of each submodule category, while the # column reports how many submodules belong to each size category.

Table 7.4: Submodules from 105 Permutation Module

m	#	m	#
0	1	64	1
1	1	65	1
18	1	82	1
19	3	83	3
20	7	84	7
21	7	85	7
22	3	86	3
23	1	87	1
40	1	104	1
41	1	105	1

To further elucidate the properties of these submodules, we generated binary linear codes corresponding to each submodule. Table 7.5 presents these codes, focusing on those of smaller dimensions. This compact representation offers insight into the coding-theoretic aspects of the submodules derived from the 105-dimensional permutation module.

Table 7.5: Low-dimensional binary linear codes derived from the 105 permutation module

Name	Dimension	parameters
$C_{105,1}$	18	$[105, 18, 32]_2$
$C_{105,2}$	19	$[105, 19, 32]_2$
$C_{105,3}$	19	$[105, 19, 32]_2$
$C_{105,4}$	19	$[105, 19, 25]_2$
$C_{105,5}$	20	$[105, 20, 28]_2$
$C_{105,6}$	20	$[105, 20, 28]_2$
$C_{105,7}$	20	$[105, 20, 25]_2$
$C_{105,8}$	21	$[105, 21, 28]_2$
$C_{105,9}$	21	$[105, 21, 28]_2$
$C_{105,10}$	21	$[105, 21, 28]_2$
$C_{105,11}$	21	$[105, 21, 25]_2$
$C_{105,12}$	22	$[105, 22, 28]_2$
$C_{105,13}$	22	$[105, 22, 25]_2$
$C_{105,14}$	23	$[105, 23, 25]_2$

We conducted a detailed analysis of the properties of selected codes derived from the submodules. Our findings are as follows:

For codes $C_{105,1}$, $C_{105,2}$, and $C_{105,5}$:

i . All codeword weights are divisible by 4.

ii . The dual codes $C^{\perp}_{105,1}$, $C^{\perp}_{105,2}$, and $C^{\perp}_{105,5}$ have minimum weights of 5 each.

Proposition 7.2.1. *Consider a particular group G, which is an extension of the group $L_3(4) : 2^2$ acting on a set of 105 elements. Under this setup, the codes $C_{105,1}$, $C_{105,2}$, and $C_{105,5}$ possess the following properties:*

i . Doubly even

ii . Projective

Proof.

i . To show that $C_{105,1}$, $C_{105,2}$, and $C_{105,5}$ are doubly even, we note that each codeword in these codes has a weight (i.e., the number of non-zero elements) that is a multiple of 4. This property of all weights being divisible by 4 is precisely what characterizes a doubly even code.

ii . For projectivity, we note that the dual codes have minimum weights of 5. By definition, a code is projective if its dual code has minimum distance at least 3. As 5 exceeds this threshold, $C_{105,1}$, $C_{105,2}$, and $C_{105,5}$ are projective.

□

For codes $C_{105,10}$ and $C_{105,12}$:

i . All codeword weights are divisible by 2.

ii . $C^{\perp}_{105,10}$ and $C^{\perp}_{105,12}$ have minimum weights of 5 each.

Proposition 7.2.2. *Let G be a primitive group of degree 105 of the extension group $L_3(4) : 2^2$. Then $C_{105,10}$ and $C_{105,12}$ are:*

i . Even

ii . Projective

Proof.

i . To prove that $C_{105,10}$ and $C_{105,12}$ are even, we observe that all codeword weights are divisible by 2, which is the definition of an even code.

ii . For projectivity, we note that the dual codes have minimum weights of 5. As this exceeds 3, $C_{105,10}$ and $C_{105,12}$ are projective by the same reasoning as in the previous proposition.

□

For codes $C_{105,3}$, $C_{105,4}$, $C_{105,6}$, $C_{105,7}$, $C_{105,8}$, $C_{105,9}$, $C_{105,11}$, and $C_{105,13}$: The dual codes $C^{\perp}_{105,3}$, $C^{\perp}_{105,4}$, $C^{\perp}_{105,6}$, $C^{\perp}_{105,7}$, $C^{\perp}_{105,8}$, $C^{\perp}_{105,9}$, $C^{\perp}_{105,11}$, and $C^{\perp}_{105,13}$ all have minimum weights of 6.

Proposition 7.2.3. *Let G be a primitive group of degree 105 of the extension group $L_3(4)$: 2^2. Then $C_{105,3}$, $C_{105,4}$, $C_{105,6}$, $C_{105,7}$, $C_{105,8}$, $C_{105,9}$, $C_{105,11}$, and $C_{105,13}$ are projective.*

Proof.

For each code $C_{105,i}$ in this set, its dual code $C_{105,i}^{\perp}$ has a minimum weight of 6. By definition, a code is projective if its dual code has a minimum distance of at least 3. As 6 exceeds this threshold, all these codes are projective. □

Combinatorial Designs Derived from Minimum Weight Codewords in $C_{105,i}$

We examined the combinatorial designs formed by the supports of the codewords with minimum weight wm in the codes $C_{105,i}$. Table 7.6 presents the properties of these designs, with each column providing the following information:

i. Column 1: The code $C_{105,i}$ containing the codewords of weight m.

ii. Column 2: The parameters of the 1-design D_{wm} formed by the supports of the minimum weight codewords.

iii. Column 3: The number of blocks in the design D_{wm}.

iv. Column 4: Specifies whether the design D_{wm} retains a high degree of symmetry (i.e., is primitive) or exhibits reduced symmetry (i.e., is not primitive) when the code's symmetry group, denoted $\mathrm{Aut}(C)$, is applied to it.

Table 7.6: Combinatorial Designs from Minimum Weight Codewords in Codes $C_{105,i}$

Code	Design	Number of blocks	Primitive
$[105, 18, 32]_2$	1-(105,32,32)	105	Yes
$[105, 19, 32]_2$	1-(105,28,32)	120	Yes
$[105, 19, 32]_2$	1-(105,32,32)	105	Yes
$[105, 19, 25]_2$	1-(105,25,10)	42	No
$[105, 20, 28]_2$	1-(105,28,32)	120	Yes
$[105, 20, 28]_2$	1-(105,28,32)	120	Yes
$[105, 20, 25]_2$	1-(105,25,10)	42	No
$[105, 21, 28]_2$	1-(105,28,32)	120	Yes
$[105, 21, 28]_2$	1-(105,28,96)	360	No
$[105, 21, 28]_2$	1-(105,28,96)	360	No
$[105, 21, 25]_2$	1-(105,25,10)	42	No
$[105, 22, 28]_2$	1-(105,28,96)	360	No
$[105, 22, 25]_2$	1-(105,25,10)	42	No
$[105, 23, 25]_2$	1-(105,25,10)	42	No

Remark 7.2.4. *Our analysis of the designs derived from the codes revealed several notable patterns:*

i. The designs 1-(105,32,32) and 1-(105,28,32) exhibit primitive structure.

ii. In contrast, the designs 1-(105,25,10) and 1-(105,28,96) lack primitivity.

iii. Multiple codes generate identical designs:

- *The codes* $[105, 18, 32]_2$ *and* $[105, 19, 32]_2$ *both produce the design 1-(105,32,32).*
- *The codes* $[105, 19, 32]_2$, $[105, 20, 28]_2$, *and* $[105, 21, 28]_2$ *all generate the design 1-(105,28,32).*

Theorem 7.2.5. *Let G be the group $L_3(4) : 2^2$ extended by another group, and let Ω be a special set of 105 elements on which G acts. This set Ω is constructed by dividing the group $2^8 \times 3$ into equally-sized subsets, called cosets, and considering the action of G on these cosets. From this setup, we obtain the important binary codes $C_{105,1}, C_{105,2}, \ldots, C_{105,13}$ by studying the permutations of the 105 elements induced by the action of G. These codes have the following notable properties:*

i. $C_{105,1}$*,* $C_{105,2}$*, and* $C_{105,3}$ *are doubly even and projective binary codes with parameters* $[105, 18, 32]$*,* $[105, 19, 32]$*, and* $[105, 20, 28]$ *respectively. Their corresponding dual codes have parameters* $[105, 87, 5]$*,* $[105, 86, 5]$*, and* $[105, 85, 5]$*.*

ii. $C_{105,10}$ *and* $C_{105,12}$ *are even and projective binary codes with parameters* $[105, 21, 28]$ *and* $[105, 22, 28]$*. Their dual codes have parameters* $[105, 84, 5]$ *and* $[105, 83, 5]$ *respectively.*

iii. The codes $C_{105,3}$*,* $C_{105,4}$*,* $C_{105,5}$*,* $C_{105,6}$*,* $C_{105,7}$*,* $C_{105,8}$*,* $C_{105,9}$*,* $C_{105,11}$*, and* $C_{105,13}$ *are projective with varying parameters. Their dual codes all have minimum distance 6.*

iv. The codes $C_{105,1}$*,* $C_{105,2}$*,* $C_{105,3}$*,* $C_{105,5}$*,* $C_{105,6}$*, and* $C_{105,8}$ *generate primitive symmetric 1-designs with parameters 1-(105, 32, 32) or 1-(105, 28, 32).*

7.3 Analysis of the 120-Dimensional Representation

We built a mathematical structure called a permutation module, which has 120 dimensions. This module has a special property: it remains unchanged when a certain group of permutations, denoted by G, rearranges the elements of a set Ω that contains 120 objects. We focused our attention on this permutation module and systematically broke it down into smaller, more manageable pieces called submodules. To do this, we applied a step-by-step process that gradually unveiled all the submodules hiding within the larger structure.

Our investigation revealed that this permutation module decomposes into a total of 20 distinct submodules. To provide a clear overview of this decomposition, we present the dimensions of these submodules along with their respective frequencies in Table 7.7.

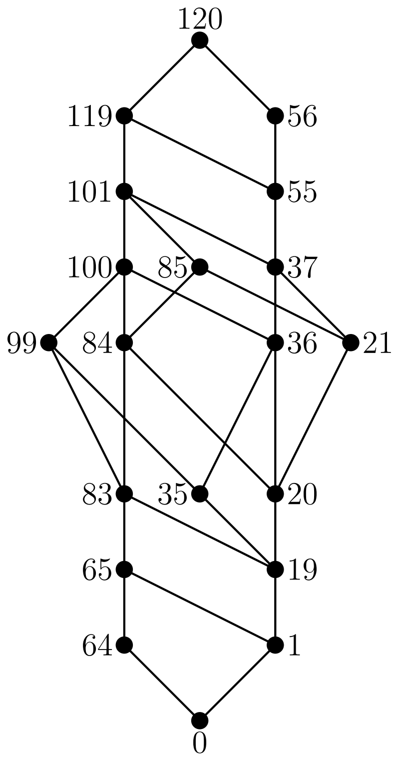
Table 7.7: Submodules from 120 Permutation Module of $L_3(4) : 2^2$

m	#	m	#
0	1	64	1
1	1	65	1
19	1	83	1
20	1	84	1
21	1	85	1
35	1	99	1
36	1	100	1
37	1	101	1
55	1	119	1
56	1	120	1

The submodules identified from the decomposition of the 120-dimensional permutation module serve as the fundamental components for constructing a submodule lattice. Figure 7.2 presents a visual representation of this lattice, illustrating the hierarchical relationships between the submodules.

.

Figure 7.2: Lattice diagram depicting the submodule structure of the permutation module of degree 120



Through careful examination of the lattice diagram, we identify that the submodules of dimensions 64 and 1 exhibit the property of irreducibility. This observation has significant implications for understanding the fundamental building blocks of the module's structure. To further elucidate the properties of these submodules, we generate binary linear codes corresponding to each submodule. These codes are presented in Table 7.8, offering a compact representation of the submodules.

Table 7.8: Low-dimensional binary linear codes derived from the 120-dimensional permutation module of $L_3(4) : 2^2$

Name	Dimension	parameters
$C_{120,1}$	19	$[120, 19, 32]_2$
$C_{120,2}$	20	$[120, 20, 30]_2$
$C_{120,3}$	21	$[120, 21, 30]_2$

We now examine the properties of codes $C_{120,1}$, $C_{120,2}$, and $C_{120,3}$:

For $C_{120,1}$:

i . All codeword weights are divisible by 4.

ii . The dual code $C_{120,1}^{\perp}$ has a minimum weight of 6.

Proposition 7.3.1. *Let G be a primitive group of degree 120 of the extension group $L_3(4) : 2^2$. Then $C_{120,1}$ is:*

i . Doubly even

ii . Projective

Proof.

i . To show that $C_{120,1}$ is doubly even, we note that the weight of each codeword (i.e., the number of non-zero elements in the codeword) is always a multiple of 4. This property of all weights being divisible by 4 is precisely what defines a doubly even code.

ii . For projectivity, we note that the dual code has minimum weight of 6. By definition, a code is projective if its dual code has minimum distance at least 3. As 6 exceeds this threshold, $C_{120,1}$ is projective.

□

For $C_{120,2}$ and $C_{120,3}$:

i . All codeword weights are divisible by 2.

ii . The dual codes $C_{120,2}^{\perp}$ and $C_{120,3}^{\perp}$ have minimum weights of 6 each.

Proposition 7.3.2. *Let G be a primitive group of degree 120 of the extension group $L_3(4) : 2^2$. Then $C_{120,2}$ and $C_{120,3}$ are:*

i . Even

ii . Projective

Proof.

i . To prove that $C_{120,2}$ and $C_{120,3}$ are even, we observe that all codeword weights are divisible by 2, which is the definition of an even code.

ii . For projectivity, we note that the dual codes have minimum weights of 6. As both these values exceed 3, $C_{120,2}$ and $C_{120,3}$ are projective by the same reasoning as in the previous proposition.

□

Combinatorial Designs from Minimum Weight Codewords in Codes $C_{120,i}$

We determined designs formed by the set of coordinate positions of codewords with minimum weight wm in the codes $C_{120,i}$. Table 7.9 provides information about these designs in four columns:

i . Column 1: The code $C_{120,i}$ containing codewords of weight m.

ii . Column 2: The parameters of the 1-design D_{wm} formed by the supports of minimum weight codewords.

iii . Column 3: The number of blocks in the design D_{wm}.

iv . Column 4: Whether the design D_{wm} is primitive or not under the action of the automorphism group $\mathrm{Aut}(C_{120,i})$ of the code.

Table 7.9: Combinatorial Designs from Minimum Weight Codewords in Codes $C_{120,i}$ of $L_3(4) : 2^2$

Code	Design	Number of blocks	Primitive
$[120, 19, 32]_2$	1-(120,32,28)	105	Yes
$[120, 20, 30]_2$	1-(120,30,14)	56	Yes
$[120, 21, 30]_2$	1-(120,30,14)	56	Yes

Remark 7.3.3. *From our analysis of the designs derived from the minimum weight codewords, we observe:*

i. The designs 1-(120,32,28) and 1-(120,30,14) exhibit primitive structure under the action of their respective code automorphism groups.

ii. Notably, the codes $[120, 20, 30]_2$ and $[120, 21, 30]_2$, despite having different parameters, both generate the same design 1-(120,30,14).

Theorem 7.3.4. *Let G be the extension group $L_3(4) : 2^2$ and Ω be the primitive G-set of size 120 defined by the action of G on the cosets of its maximal subgroup $L_2(7) : 2^2$. Consider the non-trivial binary codes $C_{120,1}$, $C_{120,2}$, and $C_{120,3}$ obtained from the permutation module of degree 120. The following properties hold:*

i. The code $C_{120,1}$ is a doubly even and projective $[120, 19, 32]$ binary code. Its dual code has parameters $[120, 101, 6]$.

ii. The codes $C_{120,2}$ and $C_{120,3}$ are even and projective binary codes with parameters $[120, 20, 30]$ and $[120, 21, 30]$ respectively. Their corresponding dual codes have parameters $[120, 100, 6]$ and $[120, 99, 6]$.

iii. Furthermore, $C_{120,1}$, $C_{120,2}$ and $C_{120,3}$ generate primitive symmetric 1-designs with parameters 1-(120, 32, 28), 1-(120,30,14), and 1-(120,30,14) respectively.

7.4 Analysis of the 280-Dimensional Representation

We created a mathematical object called a permutation module, which has 280 dimensions. This module has an interesting property: it stays the same even when a specific group of permutations, called G, shuffles around the elements of a set Ω that has 280 items. We decided to focus our attention on this permutation module and investigate its internal structure. To do this, we used a method that allowed us to gradually uncover all the smaller pieces, known as submodules, that make up the larger module.

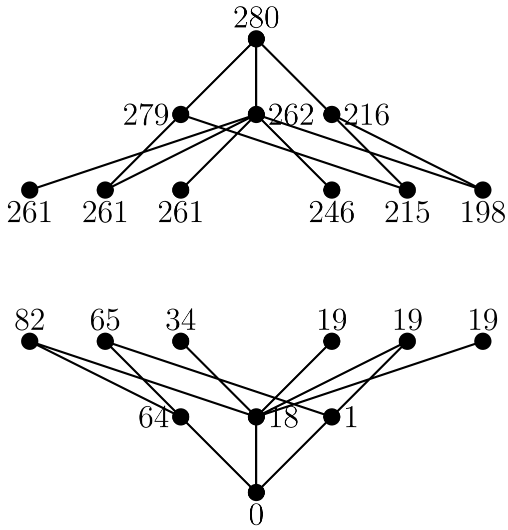
Our investigation revealed that this permutation module decomposes into a total of 516 distinct submodules. Table 7.10 provides a comprehensive overview of these submodules. In this table, the column labeled m denotes the dimension of each submodule, while the column labeled # indicates the frequency of submodules with that dimension.

Table 7.10: Submodules derived from the 280-dimensional permutation module of $L_3(4) : 2^2$

m	#	m	#	m	#	m	#	m	#
0	1	91	13	129	1	175	11	243	1
1	1	92	3	133	1	176	3	244	3
18	1	93	1	134	3	177	1	245	3
19	3	98	1	135	5	179	1	246	1
20	3	99	3	136	1	180	3	259	1
21	1	100	3	144	1	181	3	260	3
34	1	101	3	145	5	182	1	261	3
35	3	103	1	146	3	187	1	262	1
36	3	104	3	147	1	188	3	279	1
37	1	105	11	151	1	189	13	280	1
50	1	106	11	152	3	190	13		
51	3	107	12	153	13	191	13		
52	3	108	6	154	13	192	3		
53	1	109	12	155	13	193	1		
54	1	110	11	156	3	195	1		
55	3	111	11	157	1	196	3		
56	1	112	3	160	1	197	3		
64	1	113	1	161	3	198	1		
65	1	114	1	162	1	208	1		
69	1	115	3	163	1	209	5		
70	3	116	3	164	3	210	3		
71	5	117	1	165	3	211	1		
72	1	118	1	166	1	215	1		
82	1	119	3	167	1	216	1		
83	3	120	1	168	3	224	1		
84	3	123	1	169	11	225	3		
85	1	124	3	170	11	226	1		
87	1	125	13	171	12	227	1		
88	3	126	13	172	6	228	3		
89	13	127	13	173	12	229	3		
90	13	128	3	174	11	230	1		

To visualize the complex relationships between these submodules, we constructed a partial lattice diagram. Figure 7.3 presents this diagram, offering insights into the hierarchical structure of the submodules within the 280-dimensional permutation module.

Figure 7.3: Lattice diagram portraying a subset of the submodule structure for the permutation module of dimension 280



To further elucidate the properties of these submodules, we generated binary linear codes corresponding to each submodule. Table 7.11 presents a selection of these codes, focusing on those of smaller dimensions. This compact representation offers insight into the coding-theoretic aspects of the submodules derived from the 280-dimensional permutation module.

Table 7.11: Low-dimensional binary linear codes obtained from the permutation module of degree 280 associated with $L_3(4) : 2^2$

Name	Dimension	Parameters
$C_{280,1}$	18	$[280, 18, 112]_2$
$C_{280,2}$	19	$[280, 19, 100]_2$
$C_{280,3}$	19	$[280, 19, 88]_2$
$C_{280,4}$	19	$[280, 19, 84]_2$
$C_{280,5}$	20	$[280, 20, 84]_2$
$C_{280,6}$	20	$[280, 20, 84]_2$
$C_{280,7}$	21	$[280, 21, 84]_2$
$C_{280,8}$	34	$[280, 34, 64]_2$

For the codes $C_{280,1}$ through $C_{280,8}$:

i . The weights of all codewords in these eight codes were divisible by 4.

ii . The dual codes $C^{\perp}_{280,1}$, $C^{\perp}_{280,2}$, $\cdots$, $C^{\perp}_{280,8}$ each had a minimum weight of 4.

iii . The dual codes $C^{\perp}_{280,1}$, $C^{\perp}_{280,2}$, $\cdots$, $C^{\perp}_{280,8}$ were capable of correcting up to 1.5 errors.

Proposition 7.4.1. *Consider a group G that has a highly symmetric action on a set of 280 elements. This group G is related to another group called $L_3(4) : 2^2$, its extension. For this particular setup, the codes $C_{280,1}$, $C_{280,2}$, $\cdots$, $C_{280,8}$ have the following interesting properties:*

i . They are doubly even.

ii . They are projective and can correct up to 1.5 errors.

Proof. The doubly even property and the projectivity along with the error-correcting capability of the codes can be deduced from the fundamental properties of linear codes and their duals. □

Combinatorial Designs Derived from Minimum Weight Codewords in $C_{280,i}$

We examined the combinatorial designs formed by the supports of the codewords with minimum weight wm in the codes $C_{280,i}$. Table 7.12 presents the properties of these designs, with each column providing the following information:

i . Column 1: The code $C_{280,i}$ containing the codewords of weight m.

ii . Column 2: The parameters of the 1-design D_{wm} formed by the supports of the minimum weight codewords.

iii . Column 3: The number of blocks in the design D_{wm}.

iv . Column 4: An indication of whether the design D_{wm} is primitive or not under the action of the automorphism group $\mathrm{Aut}(C_{280,i})$ of the code.

Table 7.12: Combinatorial Designs from Minimum Weight Codewords in Codes $C_{280,i}$ of $L_3(4) : 2^2$

Code	Design	Number of blocks	Primitive
$[280, 18, 112]_2$	1-(280,112,1176)	2940	No
$[280, 19, 100]_2$	1-(280,100,136)	672	No
$[280, 19, 88]_2$	1-(280,88,33)	105	Yes
$[280, 19, 84]_2$	1-(280,84,36)	120	Yes
$[280, 20, 84]_2$	1-(280,84,36)	120	Yes
$[280, 20, 84]_2$	1-(280,84,108)	360	No
$[280, 21, 84]_2$	1-(280,84,108)	360	No

Remark 7.4.2. *The analysis of designs derived from the codes revealed several noteworthy characteristics:*

i . *The designs 1-(280,88,33) and 1-(280,84,36) exhibit primitive properties.*

ii . *In contrast, the designs 1-(280,112,1179), 1-(280,100,240), and 1-(280,84,108) lack primitivity.*

iii . *The codes* $[280, 19, 84]_2$ *and* $[280, 20, 84]_2$ *generate the same design, 1-(280,84,36). Similarly, the codes* $[280, 20, 84]_2$ *and* $[280, 21, 84]_2$ *produce the identical design, 1-(280,84,108).*

Theorem 7.4.3. *Let G be the group* $L_3(4) : 2^2$ *extended by another group, and let* Ω *be a special set of 280 elements that G acts on in a highly symmetric way. This set* Ω *is constructed by dividing the group* $2^5 \times 3^2$ *into equally-sized subsets called cosets and considering the action of G on these cosets. By studying the way G permutes the 280 elements of* Ω*, we can construct important binary codes* $C_{280,1}$, $C_{280,2}$, $\cdots$, $C_{280,7}$. *These codes have the following notable properties:*

i . $C_{280,1}$ *through* $C_{280,7}$ *are doubly even and projective binary codes with parameters* $[280, 18, 112]$, $[280, 19, 100]$, $[280, 19, 88]$, $[280, 19, 84]$, $[280, 20, 84]$, $[280, 20, 84]$, *and* $[280, 21, 84]$ *respectively. Their corresponding dual codes have parameters* $[280, 262, 4]$, $[280, 261, 4]$, $[280, 261, 4]$, $[280, 261, 4]$, $[280, 260, 4]$, $[280, 260, 4]$, *and* $[280, 259, 4]$.

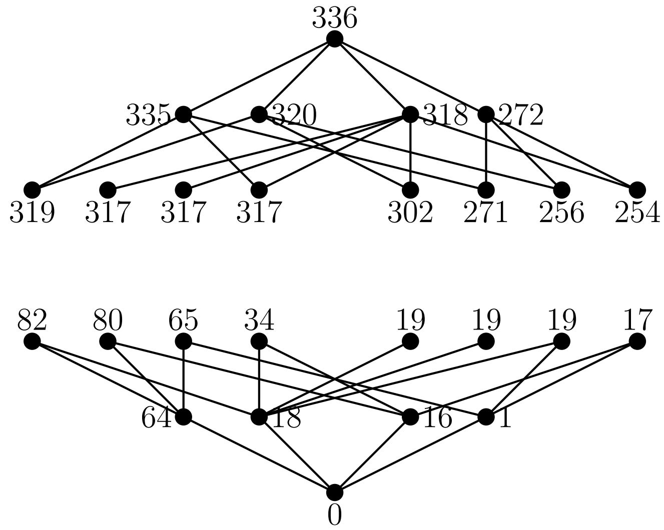
ii . The codes $C_{280,3}$*,* $C_{280,4}$*, and* $C_{280,5}$*, with parameters* $[280, 19, 88]$*,* $[280, 19, 84]$*, and* $[280, 20, 84]$ *respectively, generate primitive symmetric 1-designs with parameters 1-(280,88,33), 1-(280,84,36), and 1-(280,84,36).*

7.5 Analysis of the 336-Dimensional Representation

We created a mathematical object called a permutation module, which has 336 dimensions. This module has an interesting property: it stays the same even when a specific group of permutations, called G, shuffles around the elements of a set Ω that has 336 items. This permutation module served as our primary object of study, and we systematically identified all its submodules through recursive analysis.

Our investigation revealed that this 336-dimensional permutation module decomposes into a total of 5188 distinct submodules. To visualize the complex relationships between these submodules, we constructed a partial lattice diagram, presented in Figure 7.4. This diagram offers insights into the hierarchical structure of a subset of the submodules within the 336-dimensional permutation module.

Figure 7.4: Lattice diagram portraying a subset of the submodule structure for the permutation module of dimension 336



Combinatorial Designs Derived from Minimum Weight Codewords in $C_{336,i}$

In our analysis, we focused on the combinatorial structures that emerge from the minimum weight codewords in the codes $C_{336,i}$. Specifically, we examined the designs formed by the support sets of these codewords. Our findings are presented in Table 7.13, which is organized into five columns. The first column identifies the code $C_{336,i}$. The second column identifies the code's parameters. Column 3 delineates the defining characteristics of the emergent 1-design D_{wm}, encapsulating its structural properties in a concise parametric form. The subsequent column, Column 4, enumerates the total number of blocks constituting each design D_{wm}, offering insight into its combinatorial complexity. Finally, the fifth column indicates whether the design D_{wm} exhibits primitivity under the action of the code's automorphism group Aut(C).

Table 7.13: Combinatorial Designs Derived from Minimum Weight Codewords in $C_{336,i}$ of $L_3(4):2^2$

Code	Parameter	Design	Number of blocks	Primitive
$C_{336,1}$	$[336,16,120]_2$	1-(336,120,120)	336	Yes
$C_{336,2}$	$[336,17,120]_2$	1-(336,120,120)	336	Yes
$C_{336,3}$	$[336,18,120]_2$	1-(336,120,120)	336	Yes
$C_{336,4}$	$[336,19,120]_2$	1-(336,120,120)	336	Yes
$C_{336,5}$	$[336,19,80]_2$	1-(336,80,10)	42	No
$C_{336,6}$	$[336,19,120]_2$	1-(336,120,140)	392	No
$C_{336,7}$	$[336,20,120]_2$	1-(336,120,180)	504	No
$C_{336,8}$	$[336,20,120]_2$	1-(336,120,140)	392	No
$C_{336,9}$	$[336,20,112]_2$	1-(336,112,80)	240	No
$C_{336,10}$	$[336,20,80]_2$	1-(336,80,10)	42	No
$C_{336,11}$	$[336,20,96]_2$	1-(336,96,32)	112	No
$C_{336,12}$	$[336,21,96]_2$	1-(336,96,32)	112	No
$C_{336,13}$	$[336,21,112]_2$	1-(336,112,80)	240	No
$C_{336,14}$	$[336,21,80]_2$	1-(336,80,10)	42	No
$C_{336,15}$	$[336,22,96]_2$	1-(336,96,96)	336	Yes
$C_{336,16}$	$[336,22,96]_2$	1-(336,96,32)	112	No
$C_{336,17}$	$[336,22,80]_2$	1-(336,80,10)	42	No
$C_{336,18}$	$[336,23,80]_2$	1-(336,80,10)	42	No

We analyzed the codes and designs derived from the permutation module of degree 336. Our findings are as follows:

For the codes $C_{336,1}$ through $C_{336,18}$

i . All codeword weights in these 18 codes were divisible by 4.

ii . The dual codes $C_{336,1}^{\perp}$, $C_{336,2}^{\perp}$, $\cdots$, $C_{336,18}^{\perp}$ had minimum weights of 3, 4, $\cdots$, 4 respectively.

iii . The dual codes $C_{336,1}^{\perp}$, $C_{336,2}^{\perp}$, $\cdots$, $C_{336,18}^{\perp}$ were capable of correcting up to 1 error.

Proposition 7.5.1. *Consider a group G that has a highly symmetric action on a set of 336 elements. This group G is related to another group called $L_3(4):2^2$, its extension. Then the codes $C_{336,1}$, $C_{336,2}$, $\cdots$, $C_{336,18}$ possess the following properties:*

i . They are doubly even.

ii . *They are projective, and all can correct up to 1.5 errors, except* $C_{336,1}$ *which can correct up to 1 error.*

Proof.

i . To prove that $C_{336,1}$, $C_{336,2}$, $\cdots$, $C_{336,18}$ are doubly even, we observe that all codeword weights are divisible by 4. This property, by definition, makes these codes doubly even.

ii . For projectivity, we note that the dual codes $C_{336,1}^{\perp}$, $C_{336,2}^{\perp}$, $\cdots$, $C_{336,18}^{\perp}$ have minimum weights of at least 3. A linear code is projective if and only if its dual code has minimum distance at least 3. Therefore, these codes are projective. For the error-correcting capability, we apply the result that a code with minimum distance d can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors. The dual codes have minimum weights of 3 or 4, so they can correct up to 1 or 1.5 errors respectively. Thus, all codes except $C_{336,1}$ can correct up to 1.5 errors, while $C_{336,1}$ can correct up to 1 error.

□

Remark 7.5.2. *The analysis of designs derived from the codes revealed several noteworthy characteristics:*

i . *The designs 1-(336,120,120) and 1-(336,96,96) exhibit primitive properties.*

ii . *Multiple codes generate identical designs:*

The codes $[336,16,120]_2$*,* $[336,17,120]_2$*,* $[336,18,120]_2$*, and* $[336,19,120]_2$ *all produce the design 1-(336,120,120). The codes* $[336,19,80]_2$*,* $[336,20,80]_2$*,* $[336,21,80]_2$*,* $[336,22,80]_2$*, and* $[336,23,80]_2$ *yield the design 1-(336,80,10). The codes* $[336,19,120]_2$ *and* $[336,20,120]_2$ *generate the design 1-(336,120,140). The codes* $[336,20,96]_2$*,* $[336,21,96]_2$*, and* $[336,22,96]_2$ *result in the design 1-(336,96,32). The codes* $[336,20,112]_2$ *and* $[336,21,112]_2$ *produce the design 1-(336,112,80).*

Theorem 7.5.3. *Let G be the group $L_3(4) : 2^2$ extended by another group, and let Ω be a special set of 336 elements that G acts on in a highly symmetric way. This set Ω is constructed by dividing the group $2^2 : A_5$ into equally-sized subsets called cosets and considering the action of G on these cosets. By studying the way G permutes the 336 elements of Ω, we can construct important binary codes $C_{336,1}$, $C_{336,2}$, $\cdots$, $C_{336,18}$. These codes have the following notable properties:*

i . *$C_{336,1}$ through $C_{336,18}$ are doubly even and projective binary codes with parameters $[336, 16, 120]$, $[336, 17, 120]$, $\cdots$, $[336, 23, 80]$ respectively. Their corresponding dual codes have parameters $[336, 320, 3]$, $[336, 319, 4]$, $\cdots$, $[336, 313, 4]$.*

ii . *The codes $C_{336,1}$, $C_{336,2}$, $C_{336,3}$, $C_{336,4}$, and $C_{336,15}$, with parameters $[336, 16, 120]$, $[336, 17, 120]$, $[336, 18, 120]$, $[336, 19, 120]$, and $[336, 22, 96]$ respectively, generate primitive symmetric 1-designs with parameters 1-(336,120,120), 1-(336,120,120), 1-(336,120,120), 1-(336,120,120), and 1-(336,96,96).*

Chapter 8

Representations of Maximal Subgroups of $L_3(3):2$

In this chapter, we explored the representations of the extension group $L_3(3):2$. Our investigation focused on four specific representations, corresponding to the degrees 52, 117, 144, and 234. The key findings from our analysis are encapsulated in a comprehensive theorem presented at the conclusion of each representation.

8.1 Analysis of the 52-Dimensional Representation

We created a mathematical object called a permutation module, which has 52 dimensions. This module has an interesting property: it stays the same even when a specific group of permutations, called G, shuffles around the elements of a set Ω that has 52 items. This permutation module served as our primary object of study, and we systematically identified all its submodules through recursive analysis.

Our investigation revealed that this permutation module decomposes into a total of 12 distinct submodules. To provide a clear overview of this decomposition, we present the dimensions of these submodules along with their respective frequencies in Table 8.1.

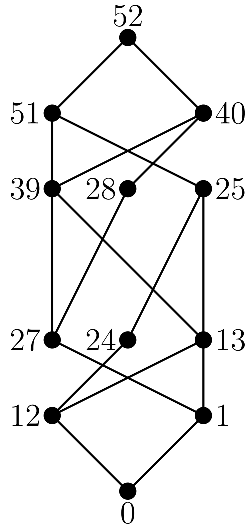
Table 8.1: Submodules derived from the 52-dimensional permutation module

m	#	m	#
0	1	27	1
1	1	28	1
12	1	39	1
13	1	40	1
24	1	51	1
25	1	52	1

The submodules identified from the decomposition of the 52-dimensional permutation module serve as the fundamental components for constructing a submodule lattice. Figure

8.1 presents a visual representation of this lattice, illustrating the hierarchical relationships between the submodules.

Figure 8.1: Lattice diagram portraying the submodule structure for the permutation module of dimension 52



Through careful examination of the lattice diagram, we identify that the submodules of dimensions 12 and 1 exhibit the property of irreducibility. This observation has significant implications for understanding the fundamental building blocks of the module's structure. To further elucidate the properties of these submodules, we generate binary linear codes corresponding to each submodule. These codes are presented in Table 8.2, offering a compact representation of the submodules in coding science.

Table 8.2: Low-dimensional binary linear codes obtained from the permutation module of degree 52

Code Name	Dimension	parameters
$C_{52,1}$	12	$[52, 12, 16]_2$
$C_{52,2}$	13	$[52, 13, 12]_2$
$C_{52,3}$	24	$[52, 24, 6]_2$
$C_{52,4}$	25	$[52, 25, 4]_2$
$C_{52,5}$	27	$[52, 27, 6]_2$
$C_{52,6}$	28	$[52, 28, 6]_2$

We now examine the properties of these codes.

For the codes $C_{52,1}$ and $C_{52,2}$:

i . All codeword weights were divisible by 4.

ii . The dual codes $C_{52,1}^{\perp}$ and $C_{52,2}^{\perp}$ each had a minimum weight of 4.

iii . $C_{52,1}$ contained no non-trivial submodules, while $C_{52,2}$ had two submodules of dimensions 12 and 1.

Proposition 8.1.1. *Let G be a primitive group of degree 52 in the extension group $L_3(3)$: 2. Then the codes $C_{52,1}$ and $C_{52,2}$ possess the following properties:*

i . They are doubly even.

ii . They are projective.

iii . $C_{52,1}$ is irreducible, while $C_{52,2}$ is decomposable.

Proof.

i . To prove that $C_{52,1}$ and $C_{52,2}$ are doubly even, we observe that all codeword weights are divisible by 4. This property, by definition, makes these codes doubly even.

ii . For projectivity, we note that the dual codes $C_{52,1}^{\perp}$ and $C_{52,2}^{\perp}$ have minimum weights of 4. A linear code is projective if and only if its dual code has minimum distance at least 3. As 4 exceeds this threshold, $C_{52,1}$ and $C_{52,2}$ are projective.

iii . The irreducibility of $C_{52,1}$ and the decomposability of $C_{52,2}$ can be deduced from the submodule structure depicted in Figure 8.1. $C_{52,1}$ has no non-trivial submodules, implying irreducibility, while $C_{52,2}$ has two proper submodules, confirming decomposability.

□

For the codes $C_{52,3}$, $C_{52,4}$, and $C_{52,5}$:

i . All codeword weights were divisible by 2.

ii . The dual codes $C_{52,3}^{\perp}$, $C_{52,4}^{\perp}$, and $C_{52,5}^{\perp}$ had minimum weights of 6, 6, and 4 respectively.

iii . The dual code $C_{52,5}^{\perp}$ was capable of correcting up to 1 error.

Proposition 8.1.2. *Let G be a primitive group of degree 52 in the extension group $L_3(3):2$. Then the codes $C_{52,3}$, $C_{52,4}$, and $C_{52,5}$ possess the following properties:*

i . They are even.

ii . They are projective.

iii . $C_{52,5}$ can correct up to 1.5 errors.

Proof.

i . To prove that $C_{52,3}$, $C_{52,4}$, and $C_{52,5}$ are even, we observe that all codeword weights are divisible by 2. This property, by definition, makes these codes even.

ii . For projectivity, we note that the dual codes $C_{52,3}^{\perp}$, $C_{52,4}^{\perp}$, and $C_{52,5}^{\perp}$ have minimum weights of 6, 6, and 4 respectively. As these values exceed 3, the codes are projective.

iii . The error-correcting capability of $C_{52,5}$ follows from the fact that its dual code $C_{52,5}^{\perp}$ has a minimum weight of 4. Applying the result that a code with minimum distance d can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors, we find that $C_{52,5}^{\perp}$ can correct up to $\lfloor \frac{4-1}{2} \rfloor = 1.5$ errors. Consequently, $C_{52,5}$ can correct up to 1.5 errors.

□

For the code $C_{52,6}$:

i . The dual code $C_{52,6}^{\perp}$ had a minimum weight of 6.

Proposition 8.1.3. *Let G be a primitive group of degree 52 in the extension group $L_3(3)$: 2. Then the code $C_{52,6}$ is projective.*

Proof.

To prove the projectivity of $C_{52,6}$, we observe that its dual code $C_{52,6}^{\perp}$ has a minimum weight of 6. As this value exceeds 3, $C_{52,6}$ is projective by the definition of projective codes. □

Combinatorial Designs Derived from Minimum Weight Codewords in $C_{52,i}$

We examined the combinatorial designs formed by the supports of the codewords with minimum weight wm in the codes $C_{52,i}$. Table 8.3 presents the properties of these designs, with each column providing the following information:

i . Column 1: The code $C_{52,i}$ containing the codewords of weight m.

ii . Column 2: The parameters of the 1-design D_{wm} formed by the supports of the minimum weight codewords.

iii . Column 3: The number of blocks in the design D_{wm}.

iv . Column 4: An indication of whether the design D_{wm} is primitive or not under the action of the automorphism group $\text{Aut}(C_{52,i})$ of the code.

Table 8.3: Combinatorial Designs from Minimum Weight Codewords in Codes $C_{52,i}$

Code	Design	Number of blocks	Primitive
$[52, 12, 16]_2$	1-(52,16,36)	117	Yes
$[52, 13, 12]_2$	1-(52,12,6)	26	No
$[52, 24, 6]_2$	1-(52,6,6)	52	Yes
$[52, 25, 4]_2$	1-(52,4,2)	26	No
$[52, 27, 6]_2$	1-(52,6,27)	234	Yes
$[52, 28, 6]_2$	1-(52,6,27)	234	Yes

Remark 8.1.4. *i . The designs 1-(52,16,36),1-(52,6,6) and 1-(52,6,27) are primitive.*

ii . The designs 1-(52,12,6) and 1-(52,4,2) are not primitive.

iii . The codes $[52, 27, 6]_2$ *and* $[52, 28, 6]_2$ *generate same design,1-(52,6,27).*

Theorem 8.1.5. *Let G be a group of extension* $L_3(3) : 2$ *and* Ω *be the primitive G-set of size 52 defined by the action on the maximal subgroup of* $2^3 \times 3^2$*. Consider the following non-trivial binary codes obtained from the permutation module of degree 52:* $C_{52,1}, C_{52,2}, C_{52,3}, C_{52,4}, C_{52,5}$ *and* $C_{52,6}$.

i . $C_{52,1}$ *is a doubly even and projective [52, 12, 16] binary code. Its dual code is [52, 40 , 4]. Furthermore ,* $C_{52,1}$ *is irreducible .*

ii . $C_{52,2}$ *is a doubly even and projective [52, 13, 12] binary code. Its dual code is [52, 39 , 4] . Furthermore ,* $C_{51,2}$ *is decomposable .*

iii . $C_{52,3}, C_{52,4}$ *and* $C_{52,5}$ *are even and projective [52,24, 6] , [52, 25, 4] and [52,27, 6] binary codes. Their dual codes are [52,28, 6] , [52, 27, 6] and [52,25, 4], respectively.*

iv . $C_{52,6}$ *is a projective [52, 28, 6] binary code. Its dual is [52, 24 , 6].*

v . Furthermore, $C_{52,1}, C_{52,3}, C_{52,5}$ *and* $C_{52,6}$ *are binary codes with parameters [52,12, 16] , [52, 24, 6] , [52,27, 6] and [52, 28,6] respectively . They generate primitive* *symmetric -1- designs 1-(52, 16, 36), 1-(52, 6, 6), 1-(52, 6, 27) and 1-(52, 6, 27) respectively, within the G-set Ω defined by the action on the maximal subgroup of* $2^3 \times 3^2$.

8.2 Analysis of the 117-Dimensional Representation

We created a mathematical object called a permutation module, which has 117 dimensions. This module has an interesting property: it stays the same even when a specific group of permutations, called G, shuffles around the elements of a set Ω that has 117 items. This permutation module served as our primary object of study, and we systematically identified all its submodules through recursive analysis.

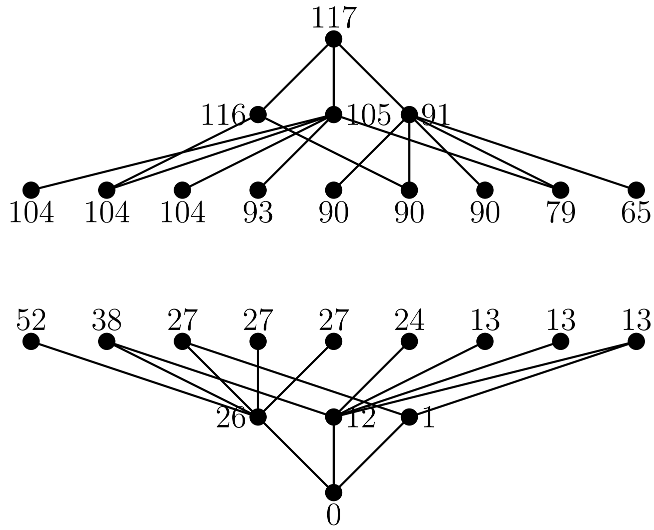
Our investigation revealed that this permutation module decomposes into a total of 108 distinct submodules. To provide a clear overview of this decomposition, we present the dimensions of these submodules along with their respective frequencies in Table 8.4.

Table 8.4: Submodules from 117 Permutation Module

m	#	m	#	m	#
0	1	41	1	78	7
1	1	50	1	79	1
12	1	51	7	89	1
13	3	52	8	90	3
14	1	53	4	91	2
24	1	54	1	92	3
25	3	63	1	93	1
26	2	64	4	103	1
27	3	65	8	104	3
28	1	66	7	105	1
38	1	67	1	116	1
39	7	76	1	117	1
40	7	77	7		

To provide a visual representation of the hierarchical relationships between these submodules, we present a subset of the submodule structure in Figure 8.2.

Figure 8.2: Lattice diagram portraying a subset of the submodule structure for the permutation module of dimension 117



Some binary linear codes of small dimensions of this representation are given in the Table 8.5.

Table 8.5: Some Binary Linear codes of small dimensions of degree 117

Code Name	Dimension	Parameters
$C_{117,1}$	12	$[117, 12, 36]_2$
$C_{117,2}$	13	$[117, 13, 36]_2$
$C_{117,3}$	13	$[117, 13, 36]_2$
$C_{117,4}$	13	$[117, 13, 36]_2$
$C_{117,5}$	14	$[117, 14, 36]_2$
$C_{117,6}$	24	$[117, 24, 16]_2$
$C_{117,7}$	25	$[117, 25, 16]_2$
$C_{117,8}$	25	$[117, 25, 9]_2$
$C_{117,9}$	26	$[117, 26, 9]_2$
$C_{117,10}$	26	$[117, 26, 24]_2$
$C_{117,11}$	27	$[117, 27, 24]_2$
$C_{117,12}$	27	$[117, 27, 24]_2$
$C_{117,13}$	28	$[117, 28, 24]_2$

The codes $C_{117,2}$, $C_{117,3}$, and $C_{117,4}$ were found to be isomorphic and generated the same codes. Despite this isomorphism, $C_{117,2}$ possessed an additional property that distinguished it from the other two codes, as demonstrated in the following propositions.

For the codes $C_{117,1}$ and $C_{117,10}$:

i . All codeword weights were divisible by 4.

ii . The dual codes $C_{117,1}^{\perp}$ and $C_{117,10}^{\perp}$ had minimum weights of 3 and 6 respectively.

iii . Both $C_{117,1}$ and $C_{117,10}$ contained no non-trivial submodules.

iv . The dual code $C_{117,1}^{\perp}$ had a minimum weight of 3.

Proposition 8.2.1. *Let G be a primitive group of degree 117 in the extension group $L_3(3):2$. Then the codes $C_{117,1}$ and $C_{117,10}$ possess the following properties:*

i . They are doubly even.

ii . They are projective.

iii . They are irreducible.

iv . $C_{117,1}$ can correct up to 1 error.

Proof.

i . To prove that $C_{117,1}$ and $C_{117,10}$ are doubly even, we observe that all codeword weights are divisible by 4. This property, by definition, makes these codes doubly even.

ii . For projectivity, we note that the dual codes $C^{\perp}_{117,1}$ and $C^{\perp}_{117,10}$ have minimum weights of 3 and 6 respectively. As these values exceed 3, the codes $C_{117,1}$ and $C_{117,10}$ are projective.

iii . The irreducibility of $C_{117,1}$ and $C_{117,10}$ follows from the absence of non-trivial submodules, as evident from their submodule structure.

iv . The error-correcting capability of $C_{117,1}$ is a consequence of its dual code $C^{\perp}_{117,1}$ having a minimum weight of 3. Applying the result that a code with minimum distance d can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors, we find that $C^{\perp}117, 1$ can correct up to $\lfloor \frac{3-1}{2} \rfloor = 1$ error. Consequently, $C_{117,1}$ can correct up to 1 error.

□

For the codes $C_{117,2}$, $C_{117,6}$, and $C_{117,7}$:

i . All codeword weights were divisible by 2.

ii . The dual codes $C^{\perp}_{117,2}$, $C^{\perp}_{117,6}$, and $C^{\perp}_{117,7}$ each had a minimum weight of 4.

Proposition 8.2.2. *Let G be a primitive group of degree 117 in the extension group $L_3(3) : 2$. Then the codes $C_{117,2}$, $C_{117,6}$, and $C_{117,7}$ possess the following properties:*

i . They are even.

ii . They are projective and can correct up to 1.5 errors.

Proof.

i . To prove that $C_{117,2}$, $C_{117,6}$, and $C_{117,7}$ are even, we observe that all codeword weights are divisible by 2. This property, by definition, makes these codes even.

ii . For projectivity and error-correcting capability, we note that the dual codes $C^{\perp}_{117,2}$, $C^{\perp}_{117,6}$, and $C^{\perp}_{117,7}$ have minimum weights of 4. As this value exceeds 3, the codes are projective. Moreover, a code with minimum distance 4 can correct up to $\lfloor \frac{4-1}{2} \rfloor = 1.5$ errors.

□

For the code $C_{117,11}$:

i . All codeword weights were divisible by 2.

ii . The dual code $C^{\perp}_{117,11}$ had a minimum weight of 6.

iii . $C_{117,11}$ had two submodules of dimensions twenty six and one.

Proposition 8.2.3. *Consider a group G that has a highly symmetric action on a set of 117 elements. This group G is related to another group called $L_3(3):2$, its extension. For this particular setup, the code $C_{117,11}$ has the following interesting properties:*

i . It is even.

ii . It is projective.

iii . It is decomposable.

Proof.

i . To prove that $C_{117,11}$ is even, we observe that all codeword weights are divisible by 2. This property, by definition, makes this code even.

ii . For projectivity, we note that the dual code $C^{\perp}_{117,11}$ has a minimum weight of 6. As this value exceeds 3, $C_{117,11}$ is projective.

iii . The decomposability of $C_{117,11}$ follows from the presence of two non-trivial submodules of dimensions 26 and 1, as evident from its submodule structure depicted in Figure 8.2.

□

For the codes $C_{117,3}$, $C_{117,4}$, $C_{117,5}$, $C_{117,8}$, $C_{117,12}$, an $C_{117,13}$:

i . The dual codes $C^{\perp}_{117,3}$, $C^{\perp}_{117,4}$, $C^{\perp}_{117,5}$, $C^{\perp}_{117,8}$, $C^{\perp}_{117,12}$, and $C^{\perp}_{117,13}$ each had a minimum weight of 4.

Proposition 8.2.4. *Let G be a primitive group of degree 117 in the extension group $L_3(3):2$. Then the codes $C_{117,3}$, $C_{117,4}$, $C_{117,5}$, $C_{117,8}$, $C_{117,12}$, and $C_{117,13}$ are projective and can correct up to 1.5 errors.*

Proof.

To prove the projectivity and error-correcting capability of these codes, we observe that their dual codes have a minimum weight of 4. As this value exceeds 3, the codes are projective. Moreover, a code with minimum distance 4 can correct up to $\lfloor \frac{4-1}{2} \rfloor = 1.5$ errors. □

For the code $C_{117,9}$:

i . The dual code $C^{\perp}_{117,9}$ had a minimum weight of 4.

ii . $C_{117,9}$ contained no submodules.

Proposition 8.2.5. *Let G be a primitive group of degree 117 in the extension group $L_3(3):2$. Then the code $C_{117,9}$ possesses the following properties:*

i . It is projective and can correct up to 1.5 errors.

ii . It is irreducible.

Proof.

i . The projectivity and error-correcting capability of $C_{117,9}$ follow from its dual code $C_{117,9}^{\perp}$ having a minimum weight of 4. As this value exceeds 3, $C_{117,9}$ is projective. Moreover, a code with minimum distance 4 can correct up to $\lfloor \frac{4-1}{2} \rfloor = 1.5$ errors.

ii . The irreducibility of $C_{117,9}$ is evident from the absence of non-trivial submodules in its structure.

□

Combinatorial Designs Derived from Minimum Weight Codewords in $C_{117,i}$

We examined the combinatorial designs formed by the supports of the codewords with minimum weight wm in the codes $C_{117,i}$. Table 8.6 presents the properties of these designs, with each column providing the following information:

i . Column 1: The code $C_{117,i}$ containing the codewords of weight m.

ii . Column 2: The parameters of the 1-design D_{wm} formed by the supports of the minimum weight codewords.

iii . Column 3: The number of blocks in the design D_{wm}.

iv. Column 4: Specifies whether the design D_{wm} retains a high degree of symmetry (i.e., is primitive) or exhibits reduced symmetry (i.e., is not primitive) when the code's symmetry group, denoted $\mathrm{Aut}(C)$, is applied to it.

Table 8.6: Combinatorial Designs from Minimum Weight Codewords in Codes $C_{117,i}$

Code	Design	Number of blocks	Primitive
$[117, 12, 36]_2$	1-(117,36,16)	52	Yes
$[117, 13, 36]_2$	1-(117,36,16)	52	Yes
$[117, 14, 36]_2$	1-(117,36,16)	52	Yes
$[117, 24, 36]_2$	1-(117,16,16)	117	Yes
$[117, 25, 36]_2$	1-(117,25,16)	117	Yes
$[117, 25, 9]_2$	1-(117,9,2)	26	No
$[117, 26, 9]_2$	1-(117,9,2)	26	No
$[117, 26, 24]_2$	1-(117,24,80)	390	No
$[117, 27, 24]_2$	1-(117,24,80)	390	No
$[117, 28, 24]_2$	1-(117,24,80)	390	No

Remark 8.2.6.

i .The designs 1-(117,36,16),1-(117,16,16) and 1-(117,25,16) are primitive.

ii . The designs 1-(117,9,2) and 1-(117,24,80) are not primitive.

iii . The codes $[117, 12, 36]_2$, $[117, 13, 36]_2$ *and* $[117, 14, 36]_2$ *generate same design,1-(117,36,16). The codes* $[117, 25, 9]_2$ *and* $[117, 26, 9]_2$ *generate same design,1-(117,9,2).The codes* $[117, 26, 24]_2$, $[117, 27, 24]_2$ *and* $[117, 28, 24]_2$ *generate same design,1-(117,24,80).*

Theorem 8.2.7. *Let G be a group of extension $L_3(3) : 2$ and Ω be the primitive G- set of degree 117 defined by the action on the maximal subgroup of $2^5 \times 3$. Consider the following non-trivial binary codes obtained from the permutation module of degree 117: $C_{117,1}$ through $C_{117,13}$.*

i . $C_{117,1}$ and $C_{117,10}$ are doubly even and projective [117, 12, 36] and [117, 26 ,24] binary codes , respectively. Their dual codes are [117, 105, 3] and [117, 91, 6]. Furthermore, $C_{117,1}$ and $C_{117,10}$ are irreducible .

ii . $C_{117,2}, C_{117,6}$ and $C_{117,7}$ are even and projective [117, 13, 36] , [117, 24, 16] and [117, 25 ,16] binary codes , respectively. Their dual codes are [117, 104, 4] , [117,93,4] and [117, 92, 4].

iii . $C_{117,11}$ is even and projective [117, 27, 24] binary code. Its dual code is [117, 90 , 6] . Furthermore , $C_{117,11}$ is decomposable .

iv . $C_{117,3}, C_{117,4}, C_{117,5}, C_{117,8}, C_{117,12}$ and $C_{117,13}$ are projective [117, 13, 36] , [117, 13, 36] , [117, 14 ,36] , [117, 25, 9] , [117, 27, 24] and [117, 28 ,24] binary codes , respectively. Their dual codes are [117, 104, 3] , [117,104,4] , [117,103, 4],[117,92,4] , [117, 90,6] , [117, 89, 6].

v . $C_{117,9}$ is a projective [117, 26, 9] binary code. Its dual codes is [117, 91, 4]. Furthermore , $C_{117,9}$ is irreducible .

iv . Additionally, $C_{117,1}$ through $C_{117,7}$ are binary codes with parameters [117, 12, 36], [117, 13, 36] , [117, 13, 36] , [117, 13, 36] ,[117, 14 ,36] , [117, 24, 16] and [117, 25, 16] respectively. They generate primitive symmetric -1- designs 1-(117, 36, 16), 1-(117, 36, 16), 1-(117, 36, 16), 1-(117, 36, 16), 1-(117, 36, 16), 1-(117, 16, 16), and 1-(117, 16, 16) respectively, within the G-set Ω defined by the action on the maximal subgroup of $2^5 \times$ *3 .*

8.3 Analysis of the 144-Dimensional Representation

We created a mathematical object called a permutation module, which has 144 dimensions. This module has an interesting property: it stays the same even when a specific group of permutations, called G, shuffles around the elements of a set Ω that has 144 items.

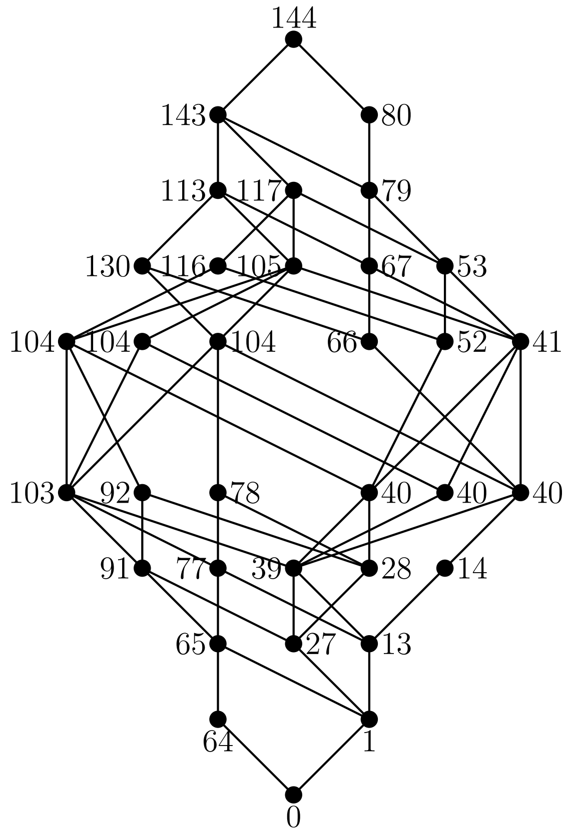
This permutation module served as our primary object of study, and we systematically identified all its submodules through recursive analysis. Our investigation revealed that this 144-dimensional permutation module decomposes into a total of 34 distinct submodules. To provide a clear overview of this decomposition, we present the dimensions of these submodules along with their respective frequencies in Table 8.7.

Table 8.7: Submodules from 144 Permutation Module

m	#	m	#	m	#
0	1	53	1	92	1
1	1	64	1	103	1
13	1	65	1	104	3
14	1	66	1	105	1
27	1	67	1	116	1
28	1	77	1	117	1
39	1	78	1	130	1
40	3	79	1	131	1
41	1	80	1	143	1
52	1	91	1	144	1

To provide a visual representation of the hierarchical relationships between these submodules, we present the submodule structure in Figure 8.3.

Figure 8.3: Lattice diagram portraying the submodule structure for the permutation module of dimension 144



Some binary linear codes of small dimensions of this representation are given in Table 8.8.

Table 8.8: Some Binary Linear codes of small dimensions of degree 144

Code Name	Dimension	Parameters
$C_{144,1}$	13	$[144, 13, 48]_2$
$C_{144,2}$	14	$[144, 14, 48]_2$
$C_{144,3}$	27	$[144, 27, 40]_2$
$C_{144,4}$	28	$[144, 28, 36]_2$

We analyzed the properties of several codes derived from the representation of degree 144. For the codes $C_{144,1}$, $C_{144,3}$, and $C_{144,4}$:

i . All codeword weights were divisible by 4.

ii . The codes $C_{144,1}$, $C_{144,3}$, and $C_{144,4}$ had minimum weights of 4, 6, and 6 respectively.

Proposition 8.3.1. *Let G be a primitive group of degree 144 in the extension group $L_3(3):2$. Then the codes $C_{144,1}$, $C_{144,3}$, and $C_{144,4}$ possess the following properties:*

i . They are doubly even.

ii . They are projective.

Proof.

i . To prove that $C_{144,1}$, $C_{144,3}$ and $C_{144,4}$ are doubly even, we observe that all codeword weights are divisible by 4. This property, by definition, makes these codes doubly even.

ii . For projectivity, we note that the dual codes have minimum weights of 4, 6, and 6 respectively. As these values exceed 3, the codes are projective.

□

For the code $C_{144,2}$:

i . All codeword weights were divisible by 2.

ii . The dual code $C_{144,2}^{\perp}$ had a minimum weight of 4.

Proposition 8.3.2. *Let G be a primitive group of degree 144 in the extension group $L_3(3):2$. Then the code $C_{144,2}$ possesses the following properties:*

i . It is even.

ii . It is projective.

Proof.

i . To prove that $C_{144,2}$ is even, we observe that all codeword weights are divisible by 2. This property, by definition, makes this code even.

ii . For projectivity, we note that the dual code $C_{144,2}^{\perp}$ has a minimum weight of 4. As this value exceeds 3, $C_{144,2}$ is projective.

□

Combinatorial Designs Derived from Minimum Weight Codewords in $C_{144,i}$

We examined the combinatorial designs formed by the supports of the codewords with minimum weight wm in the codes $C_{144,i}$. Table 8.9 presents the properties of these designs, with each column providing the following information:

i . Column 1: The code $C_{144,i}$ containing the codewords of weight m.

ii . Column 2: The parameters of the 1-design D_{wm} formed by the supports of the minimum weight codewords.

iii . Column 3: The number of blocks in the design D_{wm}.

iv . Column 4: Specifies whether the design D_{wm} retains a high degree of symmetry (i.e., is primitive) or exhibits reduced symmetry (i.e., is not primitive) when the code's symmetry group, denoted $\mathrm{Aut}(C)$, is applied to it..

Table 8.9: Combinatorial Designs from Minimum Weight Codewords in Codes $C_{144,i}$

Code	Design	No. of blocks	Primitive
$[144, 13, 48]_2$	1-(144,48,39)	117	Yes
$[144, 14, 48]_2$	1-(144,48,39)	117	Yes
$[144, 27, 40]_2$	1-(144,40,455)	1638	No
$[144, 28, 36]_2$	1-(144,36,13)	52	Yes

Remark 8.3.3.

i .The designs 1-(144,48,39) and 1-(144,36,13) are primitive.

ii .The designs 1-(144,40,455) is not primitive.

iii . The codes $[144, 13, 48]_2$ *and* $[144, 14, 48]_2$ *generate same design,1-(144, 48,39).*

Theorem 8.3.4. *Let G be the group* $L_3(3) : 2$ *extended by another group, and let* Ω *be a special set of 144 elements that G acts on in a highly symmetric way. This set* Ω *is constructed by dividing the group* $2 \times 3 \times 13$ *into equally-sized subsets called cosets and considering the action of G on these cosets. By studying the way G permutes the 144 elements of* Ω*, we can construct important binary codes* $C_{144,1}, C_{144,2}, C_{144,3}$ *and* $C_{144,4}$*. These codes have the following notable properties:*

i . $C_{144,1}, C_{144,3}$ *and* $C_{144,4}$ *are doubly even and projective [144, 13, 48] , [144, 27, 40] and [144, 28,36] binary codes, respectively . Their dual codes are [144, 131, 4] , [144, 117, 6] and [144, 116,6] respectively.*

ii . $C_{144,2}$ *is an even and projective [144, 14, 48] binary code. Its dual code is [144, 130, 4] .*

iii . Furthermore, $C_{144,1}, C_{144,3}$ *and* $C_{144,4}$ *are binary codes that generate primitive symmetric -1- designs 1-(144, 48, 39), 1-(144, 48, 39) and 1-(144, 36, 13),* *respectively, within the G-set Ω defined by the action on the maximal subgroup of* $2 \times 3 \times 13$.

8.4 Analysis of the 234-Dimensional Representation

We created a mathematical object called a permutation module, which has 234 dimensions. This module has an interesting property: it stays the same even when a specific group of permutations, called G, shuffles around the elements of a set Ω that has 234 items. This permutation module served as our primary object of study, and we systematically identified all its submodules through recursive analysis.

Our investigation revealed that this 234-dimensional permutation module decomposes into a total of 1608 distinct submodules. To provide a clear overview of this decomposition, we present the dimensions of these submodules along with their respective frequencies in Table 8.10.

Table 8.10: Smaller modules from 234 Permutation Module

m	#	m	#	m	#	m	#
0	1	81	3	144	18	221	3
1	1	88	1	145	6	222	1
12	1	89	6	146	1	233	1
13	3	90	18	153	3	234	1
14	1	91	37	154	14		
24	1	92	59	155	28		
25	3	93	31	156	57		
26	4	94	3	157	34		
27	9	102	4	158	4		
28	3	103	40	166	1		
38	3	104	76	167	19		
39	21	105	35	168	55		
40	21	106	6	169	33		
41	3	107	1	170	7		
50	3	114	3	171	1		
51	21	115	22	179	1		
52	24	116	35	180	11		
53	18	117	36	181	18		
54	11	118	35	182	24		
55	1	119	22	183	21		
63	1	120	3	184	3		
64	7	127	1	193	3		
65	33	128	6	194	21		
66	55	129	35	195	21		
67	19	130	76	196	3		
68	1	131	40	206	3		
76	4	132	4	207	9		
77	34	140	3	208	4		
78	57	141	31	209	3		
79	28	142	59	210	1		
80	14	143	36	220	1		

Some binary linear codes of small dimensions and designs of this representation are given in Table 8.11.

Combinatorial Designs from Minimum Weight Codewords in Codes $C_{234,i}$

We determined designs held by the support of codewords of minimum weight wm in $C_{234,i}$. In table 8.11, columns one, two, three, four and five respectively represent the codes $C_{234,i}$

of weight m , parameters of the code, the parameters of the 1-designs D_{wm}, the number of blocks of D_{wm}, and tests whether or not a design D_{wm}, is primitive under the action of Aut(C).

Table 8.11: Combinatorial Designs from Minimum Weight Codewords in Codes $C_{234,i}$.

Code	Parameter	Design	Number of blocks	Primitive
$C_{234,1}$	$[234, 12, 72]_2$	1-(234,72,8)	26	No
$C_{234,2}$	$[234, 13, 72]_2$	1-(234,72,8)	26	No
$C_{234,3}$	$[234, 13, 72]_2$	1-(234,72,8)	26	No
$C_{234,4}$	$[234, 14, 72]_2$	1-(234,72,8)	26	No
$C_{234,5}$	$[234, 24, 54]_2$	1-(234,54,12)	52	Yes
$C_{234,6}$	$[234, 25, 54]_2$	1-(234,54,18)	78	No
$C_{234,7}$	$[234, 25, 54]_2$	1-(234,54,12)	52	Yes
$C_{234,8}$	$[234, 26, 54]_2$	1-(234,54,18)	78	No
$C_{234,9}$	$[234, 26, 36]_2$	1-(234,36,12)	78	No
$C_{234,10}$	$[234, 26, 52]_2$	1-(234,52,96)	432	No
$C_{234,11}$	$[234, 26, 56]_2$	(234,56,56)	234	Yes
$C_{234,12}$	$[234, 27, 27]_2$	1-(234,27,6)	52	Yes
$C_{234,13}$	$[234, 27, 36]_2$	1-(234,36,12)	78	No
$C_{234,14}$	$[234, 27, 52]_2$	1-(234,52,96)	432	No
$C_{234,15}$	$[234, 27, 52]_2$	1-(234,52,96)	432	No
$C_{234,16}$	$[234, 27, 52]_2$	1-(234,52,96)	432	No
$C_{234,17}$	$[234, 27, 56]_2$	1-(234,56,56)	234	Yes
$C_{234,18}$	$[234, 27, 56]_2$	1-(234,56,56)	234	Yes
$C_{234,19}$	$[234, 27, 56]_2$	1-(234,56,56)	234	Yes
$C_{234,20}$	$[234, 27, 36]_2$	1-(234,36,12)	78	No

Our analysis of the 234-dimensional permutation module yielded several codes and designs. The results are as follows:

Examining $C_{234,1}$, $C_{234,9}$, $C_{234,10}$, $C_{234,11}$ and $C_{234,19}$, we found:

1. All codewords in these five codes have weights divisible by 4.
2. The dual codes $C_{234,1}^{\perp}$, $C_{234,9}^{\perp}$, $C_{234,10}^{\perp}$, $C_{234,11}^{\perp}$, and $C_{234,19}^{\perp}$ all possess a minimum weight of 3.

Proposition 8.4.1. *For a primitive group G of degree 234 in the extension group $L_3(3):2$, the codes $C_{234,1}$, $C_{234,9}$, $C_{234,10}$, $C_{234,11}$ and $C_{234,19}$ exhibit the following properties:*

i . They are doubly even.

ii . They are projective with the ability to correct up to 1 error.

Proof.

i . The doubly even property is confirmed by the fact that all codeword weights are multiples of 4.

ii . Projectivity is established by the minimum weight of 3 in their dual codes. The error correction capability follows from the relation $\lfloor (d-1)/2 \rfloor = \lfloor (3-1)/2 \rfloor = 1$, where d is the minimum distance.

□

For the codes $C_{234,2}$, $C_{234,3}$, $C_{234,4}$, $C_{234,5}$, $C_{234,6}$, $C_{234,7}$, $C_{234,8}$, $C_{234,13}$, $C_{234,14}$, $C_{234,17}$ and $C_{234,18}$, we observed:

i . All codewords in these eleven codes have weights divisible by 2.

ii . Their respective dual codes have minimum weights of 4, 3, 4, 4, 4, 4, 4, 4, 4, 3, and 4.

Proposition 8.4.2. *Given a primitive group G of degree 234 in $L_3(3):2$, the aforementioned codes possess the following characteristics:*

i . They are even.

ii . They are projective.

Proof.

i . The even property is evident from the divisibility of all codeword weights by 2.

ii . Projectivity is confirmed by the minimum weights of their dual codes, which are all at least 3.

□

Regarding $C_{234,12}$, $C_{234,15}$, $C_{234,16}$ and $C_{234,20}$:

Their dual codes exhibit minimum weights of 3, 3, 4, and 4 respectively.

Proposition 8.4.3. *For a primitive group G of degree 234 in* $L_3(3):2$, *the codes* $C_{234,12}$, $C_{234,15}$, $C_{234,16}$ *and* $C_{234,20}$ *are projective.*

Proof. The projectivity of these codes is established by the minimum weights of their dual codes, which are all at least 3. □

Theorem 8.4.4. *Let G be an extension group* $L_3(3):2$ *and* Ω *be the primitive G-set of degree 234 defined by its action on the maximal subgroup* $2^4 \times 3$. *The non-trivial binary codes* $C_{234,1}$ *through* $C_{234,20}$, *derived from the 234-dimensional permutation module, exhibit the following properties:*

i . $C_{234,1}$, $C_{234,9}$, $C_{234,10}$, $C_{234,11}$ *and* $C_{234,19}$ *are doubly even and projective binary codes with parameters [234, 12, 72], [234, 26, 36], [234, 26, 52], [234, 26, 56], and [234, 27, 56] respectively. Their dual codes have parameters [234, 222, 3], [234, 208, 3], [234, 208, 3], [234, 208, 3], and [234, 207, 4].*

ii . $C_{234,2}$, $C_{234,3}$, $C_{234,4}$, $C_{234,5}$, $C_{234,6}$, $C_{234,7}$, $C_{234,8}$, $C_{234,13}$, $C_{234,14}$, $C_{234,17}$ *and* $C_{234,18}$ *are even and projective binary codes. Their parameters and those of their dual codes are as listed previously.*

iii . $C_{234,12}$, $C_{234,15}$, $C_{234,16}$ *and* $C_{234,20}$ *are projective binary codes with parameters [234, 27, 27], [234, 27, 52], [234, 27, 52], and [234, 27, 36] respectively. Their dual codes have parameters [234, 207, 3], [234, 207, 3], [234, 207, 4], and [234, 207, 4].*

iv . *Within* Ω, *the codes* $C_{234,5}$, $C_{234,7}$, $C_{234,11}$, $C_{234,12}$, $C_{234,17}$, $C_{234,18}$ *and* $C_{234,19}$ *generate primitive symmetric 1-designs with parameters 1-(234, 54, 12), 1-(234, 54, 12), 1-(234, 56, 56), 1-(234, 27, 6), 1-(234, 56, 56), 1-(234, 56, 56), and 1-(234, 56, 56) respectively.*

Chapter 9

Conclusions, Recommendations, and Future Research Directions

9.1 Overview

This chapter summarizes the key findings, offers recommendations based on our research, and proposes avenues for future investigation.

9.2 Key Findings

Our research successfully classified the maximal subgroups of four extension groups using the Modular Representation Method and MAGMA computational tool. We identified:

i . 8 subgroups for $O_8^+(2):2$

ii . 4 subgroups for $L_3(4):2$

iii . 5 subgroups for $L_3(4):2^2$

iv . 4 subgroups for $L_3(3):2$

The varying number and structure of these subgroups highlight the distinct algebraic properties of each group.

We then enumerated submodules derived from these maximal subgroups. Notable results include:

i . For $O_8^+(2):2$: 12, 28, and 106 submodules for permutation modules of degrees 120, 135, and 960 respectively.

ii . For $L_3(4):2$: 12, 14, 28, and 2604 submodules for degrees 21, 56, 120, and 280 respectively.

iii . For $L_3(4):2^2$: 10, 52, 20, 516, and 5188 submodules for degrees 56, 105, 120, 280, and 336 respectively.

iv . For $L_3(3) : 2$: 12, 108, 34, and 1608 submodules for degrees 52, 117, 144, and 234 respectively.

The construction of submodule lattices revealed intricate internal structures and relationships between invariant subspaces, allowing us to deduce properties such as irreducibility and decomposability of the corresponding codes.

Our analysis using the Modular Representation Method and MAGMA yielded doubly even, projective, irreducible, and decomposable codes with robust error-correcting capabilities. We also discovered numerous combinatorial designs from the minimum weight codewords, many of which exhibited primitive properties, indicating rich symmetrical structures.

9.3 Recommendations

i . We strongly recommend that stakeholders in the communication sector consider adopting our constructed codes for their robust error detection and correction capabilities.

ii . We encourage computer scientists and engineers in communication and data storage fields to explore our findings for deeper insights into both theoretical aspects and practical applications of these codes and designs.

9.4 Future Research Directions

i . Expansion to larger groups: Apply the modular representation method to more extensive and complex group structures to further our understanding of their properties and potential applications.

ii . Cryptographic applications: Investigate the potential of this method in developing or enhancing secure cryptographic schemes.

iii . Symmetry analysis: Delve deeper into the symmetry properties exhibited by group actions on these linear codes and designs, exploring their implications for coding theory, design theory, and related mathematical fields.

iv . Interdisciplinary connections: Explore links between this work and other areas of mathematics such as algebraic number theory, algebraic geometry, and representation theory.

v . Method generalization: Extend the modular representation method to other types of groups and mathematical objects, broadening its applicability in various areas of mathematics and engineering.

References

Baylis, D. J. (1997). *Error correcting codes: A mathematical introduction* (Vol. 15). CRC Press.

Berlekamp, E. R. (2015). *Algebraic coding theory* (revised edition). World Scientific.

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

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

Davey, M. C., & MacKay, D. J. (1998). Low density parity check codes over GF (q). In *1998 Information Theory Workshop* (Cat. No. 98EX131) (pp. 70-71). IEEE.

Fletcher, C. R. (1984). [Review of the book *Finite fields*, by R. Lidl & H. Niederreiter]. *The Mathematical Gazette*, 68(446), 306-307.

Grossman, J. (2008). Coding theory: Introduction to linear codes and applications. *Insight: River Academic Journal*, 4(2), 1-17.

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

Kananu, R. L. (2019). *Codes, designs and graphs obtained from some projective symplectic group* [Doctoral dissertation, Kibabii University].

Kariuki, Y. W. (2019). *On some ternary linear codes and designs obtained from the projective special linear group $PSL_3(4)$* [Master's dissertation, Kibabii University].

Maina, J. L. (2019). *2-Modular representations of unitary group $U_3(4)$ as linear codes* [Master's dissertation, Kibabii University].

Marani, V. N. (2019). *Some linear codes, graphs and designs from Mathieu groups M_{24} and M_{23}* [Doctoral dissertation, Kibabii University].

Peterson, W. W., & Weldon, E. J. (1972). *Error-correcting codes.* MIT Press.

Pham, D. M., Premkumar, A. B., & Madhukumar, A. S. (2011). Error detection and correction in communication channels using inverse gray RSNS codes. *IEEE Trans-*

actions on Communications, 59(4), 975-986.

Richardson, T., & Urbanke, R. (2008). *Modern coding theory.* Cambridge University Press.

Rodrigues, B. G. (2002). *Codes of designs and graphs from finite simple groups.* University of Natal, Pietermaritzburg.

Ryan, W., & Lin, S. (2009). *Channel codes: Classical and modern.* Cambridge University Press.

Sadiki, F., Alit, I., Agan, B., & Florinda, I. (n.d.). *Some properties of projective geometry in coding theory* [Professional paper]. UDC: 514.16:519.854.

Sayed, M. (2016). Binary linear codes and symmetric generation of finite simple groups. *International Journal of Algebra*, 10(7), 299-311.

Appendix

REPRESENTATION OF GROUP $S_6 2$

$G < x, y >$:=PermutationGroup $<$ 28|\| [1,3,2,4,5,7,6,8,10,9,11,14,13,12,15,16,19,18,17,22,21,\

[2,3,4,5,6,8,9,1,11,12,13,15,16,7,17,18,20,14,21,19,23,24,25,26,27,28,22]

$>$;

print "Group G is $S_6(2) < Sym(28)$"

REPRESENTATION OF GROUP $L_3(4)$

$G < xy >$:=PermutationGroup $<$ |\|120 [1,4,6,2,9,3,12 10,5,8,17,7,20,21,23,24,11,27,29,13,14

\

[2,5,1,7,3,10,13,4,14,16,6,18,8,22,9,11,25,28,12,30,23,15,34,35,38, 17,39,19,42,45,20,21,48,32,51,2

36,70,72,37,59,40,46,55,41,47,43,78,44,73,75,81,49,83,50,85,52,54,57,89,60, 91,76,63,93,80,67,82

103,106,101,113,94,95,107,97,115,98,116,100,105,114,110,112,119,117,120,118]

$>$;

print "Group G is $L_3(4) < sym(120)$"

REPRESENTATION OF GROUP $L_3(3)$.

$G < xy >$:=PermutationGroup <144 |\| [2,1,5,6,3,4,11,12,13,14,7,8, 9,10, 23,24,25,26,27,28,29

\ [

,\[1,3,4,2,7,9,8,5,10,6,15,17,19,21,16,11,18,12,20,13,22,14,23,31,33, 34,36,25,38,40,32,24,28,35,26,37,2

65,67,50,43,56,44,58,46,60,47,62,48,64,49,66,51,68,52,83,85,87,89,91,74,93, 95,96,97,99,101,76,

102, 80, 115, 117, 118, 119, 121, 105, 110, 112, 123, 109, 125, 104, 116, 103, 114, 108, 120, 106, 122, 107, 12

113,127,133,129,130,135,137,134,128,136,131,138,132,141,139,140,143,144,142]

$>$;

print "Group G is $L_3(4) < sym(144)$" CODES FROM MAXIMAL SUBGROUPS

M:=MaximalSubgroups(G);M; H:=M[1]'subgroup;

a1,a2,a3:=CosetAction(G,H); g1:=PermutationModule(a2,GF(2)); g1;

SubmoduleLattice(g1);

m:=Submodules(g1);m;

m

[#m[i]: i in [1.. # m]];

c1:=LinearCode(Morphism(m[1],g1));

c2:=LinearCode(Morphism(m[2],g1));

c3:=LinearCode(Morphism(m[3],g1));

c4:=LinearCode(Morphism(m[4],g1));

```
c5:=LinearCode(Morphism(m[5],g1));
c6:=LinearCode(Morphism(m[6],g1));
c7:=LinearCode(Morphism(m[7],g1));
c8:=LinearCode(Morphism(m[8],g1));
c9:=LinearCode(Morphism(m[9],g1));
c10:=LinearCode(Morphism(m[10],g1));
c11:=LinearCode(Morphism(m[11],g1));
c12:=LinearCode(Morphism(m[12],g1));
c13:=LinearCode(Morphism(m[13],g1));
c14:=LinearCode(Morphism(m[14],g1));
c15:=LinearCode(Morphism(m[15],g1)); A:=c3;

C:=AutomorphismGroup(A);
CompositionFactors(C);

orbs:=Orbits(C); # orbs;
N:=MaximalSubgroups(C);N; P:=N[2]`subgroup; CompositionFactors(P);

SubmoduleLattice (N);
N:=MaximalSubgroups(C);N; P:=N[2]`subgroup;
a1,a2,a3:=CosetAction(C,P);
g1:=PermutationModule(a2,GF(2) ); g1;
SubmoduleLattice(g1); SubmoduleLattice(g1);

m:=Submodules(g1);m;

#m;

[#m[i]: i in [1..#m]];

c1:=LinearCode(Morphism(m[1],g1));
c2:=LinearCode(Morphism(m[2],g1));
c3:=LinearCode(Morphism(m[3],g1));
c4:=LinearCode(Morphism(m[4],g1));
c5:=LinearCode(Morphism(m[5],g1));
c6:=LinearCode(Morphism(m[6],g1));
c7:=LinearCode(Morphism(m[7],g1));
c8:=LinearCode(Morphism(m[8],g1));
c9:=LinearCode(Morphism(m[9],g1));
```

c10:=LinearCode(Morphism(m[10],g1));

A:=c1; [Length(A), Dimension(A),
MinimumDistance(A)]; B:=Dual(c1); [Length(B),
Dimension(B), MinimumDistance(B)];
WeightDistribution(A);

DESIGNS FROM CODES USING MINIMUM DISTANCE

wt:=WeightDistribution(A); wt:=36;

wt;

wds := Words(A, wt);

/wds;

D:= Design 1,Length (A) — wds ; D;