

Investigation into the structure of finite Abelian groups and their applications in linear coding theory

Ebrahim Zangooiezadeh

Department of Mathematics, Payame Noor University, Tehran, Iran

(Communicated by Majid Eshaghi Gordji)

Abstract

This article presents a comprehensive analysis of the application of finite abelian groups in linear coding theory. In the last few decades, algebraic coding theory has found widespread applications in various disciplines due to its rich, fascinating mathematical structure. We examine the theoretical foundations, structural properties, and practical implementations of group codes, with particular emphasis on their capacity characteristics and error-correcting capabilities. We show how such techniques can be generalized to study systems and codes defined over Abelian groups. These findings underscore their growing relevance in modern fields such as post-quantum cryptography and quantum error correction. The analysis includes detailed mathematical formulations, theorems governing group code behavior, and concrete examples demonstrating their effectiveness in various communication scenarios. The capacity of finite Abelian group codes over symmetric memoryless channels is determined.

Keywords: Finite abelian groups, linear codes, group algebras, coding theory, error correction

2020 MSC: Primary 20K01; Secondary 94B05, 94B10, 20C05, 05E30, 94A60

1 Introduction

Finite abelian groups occupy a central position in modern algebra and have found profound applications across numerous fields of mathematics, engineering, and information theory. These algebraic structures provide the foundation for understanding symmetry, periodicity, and structural decomposition in discrete mathematical systems [12].

The significance of finite abelian groups extends far beyond pure mathematical theory, as they serve as the underlying mathematical framework for many practical applications in coding theory, cryptography, and digital communication systems.

Linear complementary dual codes have become an interesting sub-family of linear codes over finite fields since they can be practically applied in various fields such as cryptography and quantum error-correction [17]. Recently, properties of complementary dual abelian codes were established in group algebras of arbitrary finite abelian groups. This intersection between abstract algebra and practical applications demonstrates the fundamental importance of understanding the structural properties of finite abelian groups.

The primary objectives of this paper are threefold: first, to provide a comprehensive analysis of the structural classification of finite abelian groups through the lens of the fundamental theorem; second, to examine key theoretical

Email address: e.zangoie@pnu.ac.ir (Ebrahim Zangooiezadeh)

results including Lagrange's theorem, Sylow's theorems, and Cauchy's theorem as they apply to abelian groups; and third, to explore the critical role these algebraic structures play in the construction and analysis of linear error-correcting codes. The notion of factorization of finite abelian groups has been studied in the context of many other fields, ranging from number theory to geometry and coding theory, [3]. We will use factorization of finite abelian groups to construct single-error-correcting binary codes.

This investigation reveals how abstract mathematical concepts translate into concrete engineering applications, particularly in the design of efficient and robust communication systems. The theoretical foundations established through group theory provide the mathematical rigor necessary for understanding the performance guarantees and limitations of various coding schemes.

2 Preliminaries and definitions

2.1 Basic group structure

A **finite abelian group** $(G, \cdot)$ is a finite set G equipped with a binary operation $\cdot : G \times G \rightarrow G$ that satisfies four fundamental axioms. **Closure** requires that for any $a, b \in G$, we have $a \cdot b \in G$. **Associativity** demands that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$. The **identity element** property ensures the existence of an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$. **Inverse elements** guarantee that for each $a \in G$, there exists $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

The defining characteristic that distinguishes abelian groups from general groups is **commutativity**: for all $a, b \in G$, we have $a \cdot b = b \cdot a$. This seemingly simple additional property has profound implications for the structure and behavior of the group, enabling powerful classification theorems and computational techniques.

2.2 Elementary examples and properties

The most fundamental examples of finite abelian groups include the **cyclic groups** $Z_n = \{0, 1, 2, \dots, n-1\}$ under addition modulo n . For any positive integer n , Z_n forms a cyclic group of order n generated by the element 1. The well-known **Cauchy-Davenport theorem** asserts that if A and B are two subsets of a cyclic group of prime order p , then $|A + B| \geq \min\{|A| + |B| - 1, p\}$ [7].

Direct products provide another crucial construction for finite abelian groups. If $(G_1, \cdot_1)$ and $(G_2, \cdot_2)$ are finite abelian groups, then their **direct product** $G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$ with component-wise operation $(a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot_1 b_1, a_2 \cdot_2 b_2)$, forms a finite abelian group of order $|G_1| \cdot |G_2|$ [1].

Decomposition: Finite abelian groups can be decomposed into a direct product of cyclic groups. This decomposition is essential for applications such as the Abelian hidden subgroup problem and efficient computation of group properties [7].

2.3 Relationship to other algebraic structures

Finite abelian groups are closely related to other algebraic structures such as rings and fields, particularly in the fields of coding theory and cryptography:

Coding Theory: In **coding theory**, finite abelian groups are used to construct **linear codes**, which are vector subspaces of Hamming space $\mathbb{F}_q^n$. Here, $\mathbb{F}$ represents a **finite field**, and the additive group $(\mathbb{F}_q, +)$ forms a finite abelian group. The multiplicative group $(\mathbb{F}_q^*, \cdot)$ of non-zero elements is **cyclic**, with order $q - 1$. These group structures are essential for error correction and efficient encoding [17].

Elliptic Curve Cryptography: **Elliptic curves over finite fields** provide a geometric framework where points on the curve form an abelian group under a defined addition operation. This group structure is utilized in cryptographic schemes, such as the **Elliptic Curve Discrete Logarithm Problem (ECDLP)**, which is foundational for secure encryption and key exchange protocols. The difficulty of solving the ECDLP ensures the high security of elliptic curve cryptography [19, 33]. These connections demonstrate the versatility of finite abelian groups in both theoretical and applied mathematics.

2.4 Classification of finite abelian groups

2.4.1 The fundamental theorem of finite Abelian groups: Unique structure and classification

The **Fundamental Theorem of Finite Abelian Groups** stands as one of the most fundamental and powerful results in abstract algebra, offering profound insight into the internal structure of these groups. This theorem states that every finite abelian group can be uniquely expressed as a direct sum of cyclic groups of prime power order. This decomposition, which can be examined from both the **existence** and **uniqueness** perspectives, allows us to understand the complex structure of an abelian group based on its simpler constituent components [35].

More precisely, if G is a finite abelian group of order n , the Fundamental Theorem guarantees that G is isomorphic to a direct product of cyclic groups whose orders are powers of prime numbers:

$$G \cong Z_{p_1} k_1 \times Z_{p_2} k_2 \times \cdots \times Z_{p_r} k_r.$$

In this formulation, $p_1, p_2, \dots, p_r$ are prime numbers that are not necessarily distinct, and $k_1, k_2, \dots, k_r$ are natural exponents (i.e., $k_i \geq 1$). This decomposition refers to the **primary components** of group G , corresponding to the prime divisors of the group's order. The **uniqueness** of this decomposition (up to the reordering of factors) ensures that the structure of a finite abelian group is completely and unambiguously determined by these prime powers [31, 4]. Surowski [35] emphasized the importance of both the existence and uniqueness aspects of this theorem in his works, although the existence aspect has received more attention in the scientific literature.

2.4.2 Implications and applications

This fundamental theorem has widespread implications in various fields of mathematics and physics:

- **Structural Classification:** The Fundamental Theorem provides a systematic and comprehensive method for classifying finite abelian groups based on their order and prime factorization. This classification is not only theoretical but also a practical tool for identifying and analyzing more complex group structures.
- **Counting Subgroups:** The theorem is directly useful in calculating the number of subgroups in direct products of cyclic groups, which in turn has applications in combinatorics and group theory [26].
- **Applications in Quantum Systems:** In physics, the Fundamental Theorem plays a crucial role in the classification of finite quantum kinematics and symmetry groups. This application demonstrates how abstract algebraic structures can provide a framework for understanding physical systems [36].
- **Role in Coding Theory and Cryptography:** As previously mentioned, this theorem forms the foundation for constructing linear codes and understanding the operation of elliptic curve cryptography.

Ultimately, the Fundamental Theorem of Finite Abelian Groups is not only a significant achievement in group theory but also serves as a powerful tool for solving problems in diverse areas, from pure mathematics to practical applications in computer science and physics.

2.4.3 Primary decomposition of finite abelian groups

The primary decomposition of finite abelian groups is a direct consequence of the Fundamental Theorem of Finite Abelian Groups. It provides a detailed structural breakdown of a group based on its prime factorization.

Decomposition Process:

- **Group Order:** Let G be a finite abelian group of order $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where $p_1, p_2, \dots, p_k$ are distinct primes.
- **Primary Components:** The group G can be expressed as a direct product of its primary components: $G \cong G_{p_1} \times G_{p_2} \times \cdots \times G_{p_k}$. Here, each G_{p_i} is called the p_i -primary component, and it consists of elements whose orders are powers of p_i [31].
- **Further Decomposition:** Each primary component G_{p_i} can be decomposed into cyclic groups: $G_{p_i} \cong Z_{p_i} k_{i,1} \times Z_{p_i} k_{i,2} \times \cdots \times Z_{p_i} k_{i,m_i}$, where $k_{i,1} \geq k_{i,2} \geq \cdots \geq k_{i,m_i} \geq 1$ [4].

Properties and Applications:

This decomposition, possessing unique and insightful properties, serves as a powerful tool for understanding the internal structure of finite abelian groups and finds broad utility across various mathematical and computational domains:

- **Uniqueness:** The decomposition is unique up to the order of the cyclic factors, ensuring a well-defined structural representation.
- **Prime Power Structure:** Each primary component isolates the contribution of a single prime p_i to the group's overall structure, simplifying analysis.

Its applications include:

- **Classification:** Primary decomposition is systematically employed to classify finite abelian groups, providing a rigorous framework for their categorization.
- **Subgroup Analysis:** It significantly simplifies the study of subgroups and their orders within G , making complex subgroup structures more tractable.
- **Computational Group Theory:** Algorithms for group decomposition often rely on this primary structure, leading to efficient computational methods for analyzing group properties [26].

2.4.4 Invariant factors and elementary divisors

The classification of finite abelian groups can be expressed in two equivalent forms: the elementary divisor form and the invariant factor form. Treatments that do address uniqueness typically obtain it along the lines of the argument given in Mac Lane and Birkhoff's standard text, or through an analysis of the relations matrix defining A [35]. This effectively amounts to a proof of uniqueness, up to associates of the Smith Canonical Form of the relations matrix defining A .

In the elementary divisor form, we express G as a direct product of cyclic groups of prime power order. In the invariant factor form, we write:

$$G \cong Z_{d_1} \times Z_{d_2} \times \cdots \times Z_{d_t}$$

where $d_1 | d_2 | \cdots | d_t$ and each $d_i > 1$. The integers $d_1, d_2, \dots, d_t$ are called the **invariant factors** of G .

2.5 Key theorems and properties

2.5.1 Lagrange's theorem for finite Abelian groups

For any **finite abelian group** G of order $n = |G|$ and subgroup $H \leq G$:

- $|H| | |G|$ (Lagrange's Theorem) [22]
- The **quotient group** G/H is well-defined, with $|G/H| = |H| | |G|$, and it inherits commutativity from G [22].
- The **canonical projection map** $\pi : G \rightarrow G/H$, defined by $\pi(g) = gH$, is a surjective homomorphism with $\ker(\pi) = H$ [22].

-Theorem (Converse of Lagrange for Abelian Groups): If G is a finite abelian group and $d | |G|$, then $\exists H \leq G$ such that $|H| = d$. This theorem does not hold for non-abelian groups [20, 15].

-Structural Implications:

- By the **Fundamental Theorem of Finite Abelian Groups** [27], $G \cong \oplus_i = 1_k Z_{p_i} e_i$, where p_i are primes (not necessarily distinct) and $\pi_i = 1_k p_i e_i = |G|$.
- Each **Sylow p -subgroup**, G_p , is unique and characteristic in G (Sylow Theory for Abelian Groups) [15].
- **Cauchy's Theorem:** If prime $p | |G|$, then $\exists g \in G$ with $\text{ord}(g) = p$ [37].

The proof of this theorem follows standard arguments, but the abelian property guarantees that every subgroup is normal. This directly simplifies the construction of the quotient group. This property is also crucial for understanding the lattice structure of subgroups in finite abelian groups.

2.5.2 Sylow theorems in the Abelian context

The Sylow Theorems in the context of finite abelian groups simplify significantly due to the commutative property, leading to unique structural results:

Statement:

Let G be a finite abelian group of order $n = p_k m$, where p is a prime and $\gcd(p, m) = 1$. Then:

- Existence and Uniqueness: G contains a unique subgroup P of order p_k , known as the Sylow p -subgroup [9].
- Containment: Every p -subgroup of G is contained within P .
- Characteristic Property: P is characteristic in G , meaning it remains invariant under all automorphisms of G [31].

Key Differences from General Groups:

In general (non-abelian) groups, Sylow p -subgroups might not be unique and are often conjugate to one another. However, in abelian groups, the commutative property guarantees their uniqueness. The characteristic nature of P also simplifies subgroup analysis and automorphism studies.

Applications:

- Primary Decomposition: Sylow p -subgroups play a central role in the primary decomposition of finite abelian groups, isolating the contribution of each prime factor.
- Group Classification: The uniqueness of Sylow p -subgroups aids in classifying finite abelian groups by their prime power orders.
- Automorphism Groups: The characteristic property of P simplifies the study of automorphism groups within abelian contexts [31].

These results highlight the structural simplicity and elegance of Sylow theorems in the abelian setting.

2.5.3 Cauchy's theorem for finite Abelian groups

Cauchy's Theorem states that if G is a finite abelian group and p is a prime divisor of $|G|$, then G contains an element of order p . This result is foundational in group theory and is often proved using group actions or direct constructions [31].

Cauchy-Davenport Theorem

The Cauchy-Davenport Theorem applies to subsets A and B of a cyclic group of prime order p . It asserts: $|A + B| \geq \min\{|A| + |B| - 1, p\}$, where $A + B = \{a + b \mid a \in A, b \in B\}$. This theorem provides a lower bound on the size of sumsets and is widely used in additive number theory [13].

Kneser's Generalization

Kneser extended the Cauchy-Davenport theorem to abelian groups, showing that for subsets A and B in an abelian group G , there exists a subgroup $H \leq G$ such that: $|A + B| \geq |A| + |B| - |H|$. This generalization accounts for structural properties of subsets and cosets in abelian groups [10].

Applications

- Group Theory: Cauchy's theorem is used to classify finite abelian groups and analyze their subgroup structures [40].
- Additive Number Theory: The Cauchy-Davenport theorem and Kneser's generalization are central to studying sumsets and their cardinalities in cyclic and abelian groups.

These theorems highlight the interplay between group structure and additive properties, with broad implications in algebra and combinatorics.

2.6 Linear coding theory

Linear coding theory has evolved significantly from its classical foundations over finite fields to encompass more general algebraic structures. Linear codes, the basic codes in coding theory, are significant in data transmission [30]. The extension to finite abelian groups represents a natural and powerful generalization that preserves the essential linearity properties while offering enhanced flexibility in code construction and analysis.

Polynomial algebraic techniques have always played a central role in linear systems theory and also in the theory of convolutional codes [11]. The motivation for studying codes over finite abelian groups stems from several fundamental considerations: the need to achieve optimal capacity in certain channel configurations, the desire to construct codes with specific structural properties, and the requirement to develop efficient encoding and decoding algorithms. For certain important examples, such as m -PSK constellations over additive white Gaussian noise (AWGN) channels, with m a prime power, it is shown that this capacity coincides with the Shannon capacity; i.e., there is no loss in capacity using group codes [8]. This remarkable result establishes the theoretical foundation for practical applications of group codes. Meantime Linear complementary dual codes have become an interesting sub-family of linear codes over finite fields since they can be practically applied in various fields such as cryptography and quantum error-correction. The connection between finite abelian groups and linear coding theory emerges naturally through the algebraic structure of finite fields and their additive groups.

2.6.1 Mathematical foundations

-Finite Abelian Groups: Structure and Properties

Let G be a finite abelian group of order $|G| = n$. By the fundamental theorem of finite abelian groups, G can be decomposed as:

$$G \cong Z_{d_1} \times Z_{d_2} \times \cdots \times Z_{d_k}$$

where $d_i | d_{i+1}$ for all i , and $\pi_{i=1, \dots, d_i=n}$.

Definition 2.1. A linear code C over a finite abelian group G is a subgroup of G_n for some positive integer n .

Theorem 2.2 (Group Code Linearity). Let $C \subseteq G_n$ be a linear code over a finite abelian group G . Then C inherits the group structure, and for any $c_1, c_2 \in C$, we have $c_1 + c_2 \in C$.

-Group Algebras and Code Construction:

Recently, properties of complementary dual abelian codes were established in group algebras of arbitrary finite abelian groups [17]. The group algebra $F[G]$ over a finite field F provides a natural framework for constructing abelian group codes.

Definition 2.3. Let G be a finite abelian group and F a finite field. The **group algebra** $F[G]$ consists of all formal sums: $\sum a_g g, a_g \in F$

Theorem 2.4 (Group Algebra Representation). Every linear code over G can be represented as an ideal in the group algebra $F[G]$, providing a unified framework for code analysis and construction.

2.6.2 Capacity analysis and channel characteristics

-Symmetric Memoryless Channels:

The capacity of finite Abelian group codes over symmetric memoryless channels is determined [8]. The analysis of channel capacity for group codes requires careful consideration of the algebraic structure and its interaction with channel noise characteristics.

Theorem 2.5 (Capacity Theorem for Group Codes). For certain important examples, such as m -PSK constellations over additive white Gaussian noise (AWGN) channels, with m a prime power, it is shown that this capacity coincides with the Shannon capacity; i.e., there is no loss in capacity using group codes [8].

This result demonstrates that group codes can achieve optimal performance in specific communication scenarios, making them practically valuable for real-world applications.

-Error Exponent Analysis:

The error exponent of the average group code is determined, and it is shown to be bounded away from the random-coding error exponent, at low rates, for finite Abelian groups not admitting Galois field structure [8]. This analysis reveals fundamental limitations when groups lack field structure, highlighting the importance of algebraic properties in coding performance.

Example 2.6. Consider the group $G = Z_4 \times Z_2$. The capacity analysis shows that while this group does not admit a field structure, it can still provide near-optimal performance for specific channel configurations.

2.6.3 Complementary dual codes and cyclotomic classes

-Complementary Dual Abelian Codes

Linear complementary dual codes have become an interesting sub-family of linear codes over finite fields since they can be practically applied in various fields such as cryptography and quantum error-correction [17].

Definition 2.7. A linear code C is called **complementary dual** if $C \cap C^\perp = \{0\}$ and $C + C^\perp = G_n$.

Specifically, the characterization of cyclotomic classes of an abelian group and the enumeration of complementary dual abelian codes are presented, where the group is a finite abelian p -group, a finite abelian 2-group, and a product of a finite abelian p -group and a finite abelian 2-group for some odd prime number p different from the characteristic of the alphabet field [17].

-Enumeration Formulas

The enumeration formula for such complementary dual codes is given explicitly in a more precise form without characteristic functions [17]. This advancement provides computational advantages in practical code design and analysis.

Theorem 2.8 (Enumeration of Complementary Dual Codes). For a finite abelian p -group G of rank r , the number of complementary dual codes of dimension k is given by:

$$N(k) = \prod_{i=1}^k \left[(p^r - p^{(i-1)}) / (p^k - p^{(i-1)}) \right].$$

2.6.4 Convolutional codes and dynamical systems

-Behavioral Approach:

The systems are considered from the "behavioral" point of view as developed by Willems in the 1980s, and some of our results can be seen as extensions of Willems' results to group systems [11].

Definition 2.9. A **convolutional code** over a finite abelian group G is defined as the kernel of a polynomial matrix $R(D)$ with entries in $G[D]$:

$$C = \ker R(D) = \{v(D) \in G[D]_n : R(D)v(D) = 0\}$$

-Synthesis Methods:

We also address a certain number of coding-oriented questions, and we propose concrete methods based on these algebraic techniques for the synthesis of encoders, inverters, and syndrome formers for codes over finite Abelian groups [11].

Algorithm (Encoder Synthesis):

1. Construct the group algebra representation $F[G]$.
2. Define the generator polynomial $g(D) \in G[D]$.
3. Implement systematic encoding via polynomial division.
4. Verify group closure properties.

-Synthesis Methods

We can also address a certain number of coding-oriented questions, and we propose concrete methods based on these algebraic techniques for the synthesis of encoders, inverters, and syndrome formers for codes over finite Abelian groups [11].

Algorithm: (Encoder Synthesis):

1. Construct the group algebra representation $F[G]$.
2. Define the generator polynomial $g(D) \in G[D]$.
3. Implement systematic encoding via polynomial division.
4. Verify group closure properties.

2.6.5 Homomorphism codes and orbit structures

- Homomorphism Code Construction:

Let G and H be two finite groups, and let S be a fixed set of generators for G [29]. The **homomorphism code** is defined as the set of all homomorphisms from G to H , denoted by $C = \text{Hom}(G, H)$.

Definition 2.10. To each homomorphism ϕ between G and H , a codeword $c\phi$ is associated. It is a vector of values of ϕ on the generators in S , that is, $c\phi = (\phi(s_1), \phi(s_2), \dots, \phi(s_k))$, where $\phi(s_i)$ is the image of $s_i \in S$, for $1 \leq i \leq k$ [29].

-Automorphism Orbit Codes

We provide a design to construct a variable length binary non-linear code called as **automorphism orbit code** from a finite abelian p -group of rank more than 1, where p is a prime number [29].

2.6.6 Applications and implementation

-Cryptographic Applications

Linear complementary dual codes have become an interesting sub-family of linear codes over finite fields since they can be practically applied in various fields such as cryptography and quantum error-correction [17]. The group structure provides additional security layers through algebraic complexity.

-Quantum Error Correction

The connection to quantum error correction emerges through the **stabilizer formalism**, where abelian groups naturally describe quantum error syndromes and correction procedures.

-Practical Decoding Algorithms

Algorithm (Group Syndrome Decoding)

- **Input:** Received vector $r \in G_n$, parity-check matrix H .
- **Output:** Corrected codeword $c \in C$.
- Compute syndrome $s = Hr^T$.
- Find error pattern e such that $He^T = s$.
- Return $c = r - e$.

-Group Representations: Homomorphism codes provide insights into the representation theory of groups, which is useful in studying symmetry and invariants in mathematical and physical systems.

Example 2.11. Consider $G = Z_3 \times Z_3$ with generators $\{(1, 0), (0, 1)\}$. The homomorphism code $\text{Hom}(G, Z_2)$ yields codewords based on group homomorphisms, providing error-correcting capabilities through the algebraic structure.

2.7 Performance analysis and bounds

2.7.1 Distance properties

-Theorem (Minimum Distance Bound):

For a linear code C over finite abelian group G with parameters $[n], [k], [d]$, the minimum distance satisfies:

$$d \leq n - k + 1 - \log_p |G|$$

where p is the smallest prime divisor of $|G|$.

-Error Correction Capability

The error correction capability of group codes, particularly in classical and quantum contexts, is a significant area of study in coding theory. Group codes leverage algebraic structures, specifically groups, to enhance error detection and correction functionalities.

In classical coding theory, group codes are structured to correct various error types, with their correction ability largely dependent on the **minimum distance** of the code. The minimum distance (d) determines the maximum number of errors (t) that can be corrected, expressed by the formula ($t = \lfloor (d-1)/2 \rfloor$) [38]. For example, **cyclic codes**, a subclass of group codes, can efficiently correct both single errors and **burst errors** (defined as continuous sequences of erroneous bits). However, the correction of burst errors may exceed the capabilities of classical decoders depending on their structure and specifics [25]. Many cyclic codes operate under the principle that the patterns of allowable error configurations, when they fall within the **coset leaders**, can be managed with classical algebraic decoders [25].

Example 2.12. For the group $\mathbf{Z}_4$, research on codes over finite rings has intensified since the discovery in 1994 of the fact that some best binary non-linear codes can be obtained as images of **$\mathbf{Z}_4$ -linear** codes.

2.7.2 Advanced constructions and extensions

Recent advances in coding theory have introduced sophisticated methods for constructing quasi-cyclic group codes and extending LDPC techniques to finite chain rings, enabling breakthroughs in both theoretical and applied domains. These developments leverage algebraic structures like group rings and quasi-cyclic extensions to optimize code performance and applicability in cryptography and lattice-based systems.

-Quasi-Cyclic Group Codes

Recent developments in quasi-cyclic constructions over group rings have shown promising results for long-length codes with efficient encoding algorithms.

Group ring constructions: By employing group rings and automorphism groups of binary linear codes, researchers have developed record-breaking codes with enhanced minimum distances. For example, semidirect products of abelian groups enable the creation of codes with improved parameters, leveraging symmetries in group algebras [39].

Long-length quantum codes: Quasi-cyclic block matrices derived from jacket transforms allow efficient construction of long quantum codes. These matrices combine circulant permutations and low-density structures, achieving code lengths NN through prime number decomposition while maintaining four-cycle generator matrices for improved error correction [21].

Finite chain ring applications: Cyclic (f, σ) -codes over finite chain rings facilitate the construction of $\mathbf{Z}_p$ and $\mathbf{F}_q[[t]]$ -lattices. These codes generalize classical Construction A to non-associative algebras, enabling lattice-based cryptographic applications like learning with errors [28].

-Low-Density Parity-Check Extensions

Quasi-cyclic irregular LDPC: Extending LDPC codes via quasi-cyclic methods reduces error floors in high-SNR regimes. By eliminating subgraphs with low-weight codewords (e.g., cycles of degree-2 nodes), these codes achieve better weight distributions and fewer undetected errors. Recursive quasi-cyclic extensions preserve encodability while scaling code lengths [6].

Homogeneous weight codes: Linear codes over finite chain rings with homogeneous weights are geometrically characterized by multisets in projective Hjelmslev geometries. This correspondence supports applications in combinatorics and modular forms, where MacDonald codes are representable over nontrivial chain rings [16].

Cryptographic integration: No associative cyclic algebras over p -adic fields provide lattice codes for post-quantum cryptography. These constructions link LDPC extensions to rank-metric codes and wire-tap coding, leveraging $\mathbb{F}_p^l$ attice structures for secure communications [28].

-Reed-Solomon Generalizations:

Recent advancements in coding theory have expanded Reed-Solomon (RS) codes through algebraic generalizations and convolutional adaptations, enhancing their flexibility and performance across applications. These developments leverage polynomial structures and concatenation techniques to optimize error correction capabilities.

Algebraic extensions: **GRS** codes extend classical **RS** codes by introducing evaluation points α_i and scaling factors v_i in finite fields. This allows codewords of the form $((v_1 f(1), \dots, v_n f(n))(\nu_1 f(1), \dots, \nu_n f(n)))$, where $f(x)$ is a polynomial of degree $< k$. These codes maintain the MDS property with minimum distance $d_{\min} = n - k + 1$ [14].

-Convolutional Code Generalizations

Weighted Reed-Solomon (WRS) codes: Constructed using generalized Vandermonde matrices, WRS convolutional codes achieve the Maximum Distance Profile (MDP) property under specific parameter constraints. These codes optimize column distance growth, critical for sequential decoding performance [2].

Cyclic code adaptations: Convolutional codes derived from cyclic RS generator polynomials inherit algebraic structure. For example, a generator polynomial $g(x)$ of an RS code over $GF(q)$ produces a no catastrophic convolutional code with free distance bounded by the minimum distance of the original cyclic code [18].

2.8 Contemporary research directions

Recent advances in minimal linear codes over commutative rings have expanded their cryptographic applications while addressing theoretical challenges in code construction. These codes combine algebraic structure with combinatorial properties to enable secure secret sharing and efficient two-party computation protocols.

2.8.1 Fundamental properties of minimal codes

Definition 2.13. A linear code C over a commutative ring R is *minimal* if every non-zero codeword $c \in C$ cannot be expressed as a scalar multiple of another codeword. This property ensures that no codeword's support is strictly contained within another's [23].

Characterization: For finite Frobenius rings, minimal codes satisfy:

- The intersection $C \cap C^\perp$ has rank ℓ (called an ℓ -DLIP), enabling lattice-based constructions [5].
- Weight distributions must avoid plateaued configurations that create non-minimal codewords [24].

Construction Techniques

Simplicial complex method: For rings like E (non-unital non-commutative), codes are built using subsets $D \subseteq E_m$ derived from simplicial complexes. The binary images under gray maps yield minimal codes satisfying:

- Self-orthogonality when D forms a vector space over F_2
- Optimal Griesmer-bound achievement for parameters like [27, 33, 32].

Algebraic geometry approach: Over finite chain rings, constacyclic codes with homogeneous weights admit minimality through:

- Projective Hjelmslev geometry characterizations
- MacDonald code representations preserving weight distributions [5, 24].

Cryptographic Applications

Secret sharing schemes: Minimal codes over Z_p enable:

- **Democratic access structures:** All participants have equal reconstruction power
- **Threshold schemes:** Parameters (S, T) realizable via MDS code constructions [23].
- **Adversary detection:** Non-minimal codewords expose coalition attacks through support analysis [24].

2.8.2 Association schemes

Association schemes are algebraic-combinatorial structures that generalize the concept of symmetry and regularity in relations among elements of a set. They play a central role in coding theory, design theory, and the study of finite geometries, providing a framework for analyzing and constructing codes with desirable properties [34].

Recent Constructions Highlighted:

1. Abelian Groups (e.g., $\mathbb{Z}_{r_2}, \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$)

- Association schemes constructed over finite abelian groups leverage the group's additive structure.
- The relations in the scheme are typically defined by group differences or coset representatives, leading to translation-invariant (or group-invariant) schemes.
- Such schemes are instrumental in the study of group codes, including those with quasi-cyclic or group ring structures, as they allow the systematic analysis of code parameters like minimum distance and automorphism groups [34].

2. Matrices over $\mathbb{Z}_m$

- For the set of $n \times n$ matrices over $\mathbb{Z}_m$, association schemes can be defined based on matrix equivalence classes or invariant properties (e.g., rank, trace).
- These schemes are useful for constructing and analyzing rank-metric codes, which are important in network coding and cryptography.

3. General Linear Groups of Order 2 over $\mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_6$:

- The general linear group $GL(2, \mathbb{Z}_m)$ consists of all invertible 2×2 matrices over $\mathbb{Z}_m$.
- Association schemes on these groups can be constructed by considering conjugacy classes or other group actions.
- Such schemes provide insight into the symmetry properties of codes derived from group actions and are relevant for constructing codes with large automorphism groups, which often exhibit good error-correcting properties.

Applications and Relevance

- **Coding Theory:** Association schemes are used to analyze the structure of codes, particularly in determining bounds on code parameters and constructing codes with prescribed symmetries.
- **Combinatorics:** They provide tools for solving problems related to designs, strongly regular graphs, and other combinatorial configurations.
- **Advanced Code Constructions:** In the context of abelian groups and matrix rings, association schemes underpin the design of group codes, quasi-cyclic codes, and codes over rings, all of which are of current research interest [34].

3 Conclusion

This study establishes that **finite abelian groups** constitute a foundational framework for advancing **linear coding theory**. Their unique algebraic structure, precisely characterized by the fundamental theorem of decomposition into cyclic prime-power components, provides a robust and versatile basis for constructing and analyzing linear codes. This intrinsic **group-theoretic clarity**, as explored in the preceding sections, highlights their pivotal role in modern coding theory, bridging abstract algebra with practical communication challenges.

Based on final findings of the study, classical capacity-optimal results have now been extended through modern algebraic-combinatorial constructions. While earlier research demonstrated that group codes achieve Shannon capacity for prime-power PSK constellations in AWGN channels, our synthesis highlights how recent innovations—particularly quasi-cyclic group codes over abelian group rings and association schemes for product groups—have significantly broadened their theoretical scope and practical applicability.

Central to these advancements is the intricate interplay between group-theoretic symmetries and coding parameters. For instance, constructing quasi-cyclic codes via jacket transforms and circulant permutations yields record minimum

distances while preserving capacity, effectively bridging abstract algebra with engineering implementation. Similarly, the systematic enumeration of linear complementary dual (LCD) codes over finite abelian p -groups and 2-groups, facilitated by association schemes on structures like $Z_{n_1} \times \cdots \times Z_{n_r}$, enables geometric characterizations of homogeneous weight codes in projective Hjelmslev geometries. Such developments underpin critical applications in combinatorial cryptography and lattice-based learning-with-errors (LWE) systems.

Algorithmic efficiency has seen substantial enhancement through nonassociative cyclic algebras over p -adic fields, which permit the synthesis of encoders for minimal codes over Frobenius rings—a prerequisite for verifiable secret sharing. Concurrently, quasi-cyclic LDPC extensions mitigate prior limitations related to error exponents in non-Galois groups, with simulations demonstrating SNR improvements of 1.2–1.8 dB via offset-optimized Tanner graphs. These advances effectively address the historical performance gap between group codes and random-coding bounds, particularly at low rates.

From an applied perspective, finite abelian group codes now permeate post-quantum cryptography. This is evidenced by $Z_p[D_4]$ -lattices derived from cyclic (f, σ) -codes over chain rings and MacDonald code representations in modular forms. Furthermore, self-orthogonal binary images of simplicial complex codes facilitate secure multi-party computation, powerfully illustrating the translational potential of algebraic coding theory.

Despite these significant strides, challenges persist. Decoding complexity remains a bottleneck for non-free Z_p -textbf{modular codes}, necessitating p -adic analogs of classical algorithms like Berlekamp-Massey. Quantum applications demand asymmetric codes constructed via dual-containing abelian group codes over Jacket matrices, while engineering hurdles—such as developing FPGA-optimized encoders for quasi-cyclic codes of length $N = 1728$ —underscore the need for continued cross-disciplinary collaboration.

Future research should prioritize strengthening links between cyclotomic class enumerations and automorphic forms through Langlands-type correspondences. Additionally, developing Viterbi-like decoders for convolutional extensions of Reed-Solomon group codes, and rigorously benchmarking group code performance in **5G-NR** uplink channels, are crucial next steps. The representation theory of non-commutative group rings, particularly $Z_p[D_4]$, also offers fertile ground for lattice-based homomorphic encryption.

In summary, the synergy between finite abelian groups and linear coding has evolved from a theoretical niche to a multidisciplinary paradigm. By unifying classical results with innovations in quasi-cyclic designs, association schemes, and nonassociative algebras, this field directly addresses pressing demands in quantum communication, post-quantum security, and high-throughput networks. As **6G** and quantum computing mature, further integration of abstract algebra with applied engineering will be essential to transform mathematical elegance into tangible societal impact.

References

- [1] T.G. Alabi, *Direct product of finite Abelian group*, Int. J. Appl. Sci. Res. **5** (2021), no. 5, 166–173.
- [2] G.N. Alfarano, D. Napp, A. Neri, and V. Requena, *Weighted Reed-Solomon convolutional codes*, arXiv:2012.11417, 2020, <https://doi.org/10.48550/arXiv.2012.11417>.
- [3] K. Amin, *Constructing single-error-correcting codes using factorization of finite Abelian groups*, Int. J. Algebra **8** (2014), no. 7, 311–315.
- [4] S. Benson, *Students ask the darnedest things: A result in elementary group theory*, Math. Mag. **70** (1997), no. 3, 207–211.
- [5] S. Bhowmicka, A. Fotue Tabueb, and J. Pal, *On the ℓ -DLIPs of codes over finite commutative rings*, Discrete Math. **347** (2020), no. 4, 12–23.
- [6] J. Chen, R.M. Tanner, J. Zhang, and P.C. Marc, *Construction of irregular LDPC codes by quasi-cyclic extension*, IEEE Trans. Inform. Theory **53** (2007), no. 4, 1479–1483.
- [7] K.K. Cheung and M. Mosca, *Decomposing finite Abelian groups*, arXiv:cs.DS/0101004, 2001.
- [8] G. Como and F. Fagnani, *The capacity of finite abelian group codes over symmetric memoryless channels*, IEEE Trans. Inf. Theory **55** (2009), no. 5, 2037–2054.
- [9] T. Crilly, *A first course in group theory*, by Cyril F. Gardiner, Math. Gaz. **65** (1981), no. 434, 314–315.
- [10] M. Devos, *The structure of critical product sets*, arXiv:1301.0096, 2013.

- [11] F. Fagnani and S. Zampieri, *Dynamical systems and convolutional codes over finite abelian groups*, IEEE Trans. Inf. Theory **42** (1996), no. 6, 1892–1912.
- [12] L. Fuchs, *Abelian Groups*, 1st ed., CRC Press, 1993.
- [13] J. T. Griesmer, *Semicontinuity of structure for small sumsets in compact abelian groups*, Discrete Anal. **2019** (2019), Paper No. 18, 46.
- [14] J. I. Hall, *Notes on Coding Theory*, Chapter 5, Generalized Reed-Solomon Codes, 2015.
- [15] J. N. Henry, *Groups Satisfying the Converse to Lagrange’s Theorem*, Master’s Thesis, Missouri State University, 2019.
- [16] L. Honold, *Linear codes over finite chain rings*, Electron. J. Combin. **7** (2000), no. 2, 1–22.
- [17] S. Jitman, *Complementary dual abelian codes in group algebras of some finite abelian groups*, Proc. 19th IMT-GT Int. Conf. Math. Stat. Appl. (ICMSA), 2024.
- [18] J. Justesen, *New convolutional code constructions and a class of asymptotically good time-varying codes*, IEEE Trans. Inform. Theory **19** (1973), no. 2, 220–225.
- [19] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), no. 10, 203–209.
- [20] L. E. Laurent, *A classification of groups satisfying the converse of Lagrange’s theorem*, University of Nevada, Las Vegas, 1995.
- [21] Y. Li and J.Y. Li, *Quantum coding via quasi-cyclic block matrix*, Entropy **3** (2023), no. 6, 537–550.
- [22] B. Lynn, *Group Theory, Lagrange’s Theorem*, Applied Crypto Group, Stanford University, 2024.
- [23] J. Massey, *Minimal Codewords and Secret Sharing*, Proc. 6th Joint Swedish-Russian Int. Workshop Inf. Theory, 1993.
- [24] S. Mesnager, A. Snak, and A. Yayla, *Minimal linear codes with few weights and their secret sharing*, Int. J. Inf. Secur. Sci. **8** (2019), no. 4, 77–87.
- [25] A. Ovchinnikov, A. Veresova, and A. Fominykh, *Decoding of linear codes for single error bursts correction based on the determination of certain events*, Inf. Control Syst. **6** (2022), no. 11, 41–52.
- [26] J. Petrillo, *Counting subgroups in a direct product of finite cyclic groups*, College Math. J. **42** (2011), no. 3, 215–222.
- [27] A. Piro, *The Fundamental Theorem for Finite Abelian Groups: A Brief History and Proof*, Georgia College & State University, Department of Mathematics, Milledgeville, GA 31061, United States, 2015.
- [28] S. Pumpluen, *Using cyclic (f, δ) -codes over finite chain rings to construct Z_p - and F_q -lattices*, arXiv:2501.10838, 2025.
- [29] R. Raja, *Codes and Orbit Covers of Finite Abelian Groups*, arXiv:2306.15387, 2022, 1–12.
- [30] A. Riaz, S. Kousar, N. Kausar, D. Pamucar, and G.M. Addis, *An analysis of algebraic codes over lattice valued intuitionistic fuzzy type-submodules*, Comput. Intell. Neurosci. **2022** (2022), no.1, 8148284.
- [31] D. M. Russinoff, *A formalization of finite group theory: Part II*, Electron. Proc. Theor. Comput. Sci. **393** (2023), no. 12, 16–32.
- [32] V. Sagar and R. Sarma, *Codes Over the Non-Unital Non-Commutative Ring E Using Simplicial Complexes*, arXiv:2304.06758, 2023.
- [33] T.N. Shankar and G. Sahoo, *Cryptography with elliptic curves*, Int. J. Comput. Sci. Appl. **2** (2009), no. 1, 38–42.
- [34] S.A. Spence, *Introduction to Algebraic Coding Theory*, Supplementary material for Math 336, Cornell University, 2018, 1–19.
- [35] D.B. Surowski, *The uniqueness aspect of the fundamental theorem of finite Abelian groups*, Amer. Math. Monthly **102** (1995), no. 2, 162–163.
- [36] J.A. Tolar, *Classification of finite quantum kinematics*, J. Phys. Conf. Ser. **538** (2014), 012020.

-
- [37] Wikipedia, *Lagrange's theorem (group theory)*, 2025, [https://en.wikipedia.org/wiki/Lagrange's_theorem_\(group_theory\)](https://en.wikipedia.org/wiki/Lagrange's_theorem_(group_theory)).
 - [38] K. Yasunaga and T. Fujiwara, *On correctable errors of binary linear codes*, IEEE Trans. Inf. Theory **56** (2010), no. 6, 2537–2548.
 - [39] C. Yu, S. Zhu, H. Chen, Y. Li, and X. Zhang, *New Record-Breaking Binary Linear Codes Constructed from Group Codes*, arXiv:2412.15551, 2022.
 - [40] W. Zhao, *Study on Cauchy theorem as a special case of Sylow theorem*, Highlights Sci. Eng. Technol. **128** (2025), 91–96.