Journal of Mathematical Problems, Equations and Statistics

E-ISSN: 2709-9407
P-ISSN: 2709-9393
JMPES 2025; 6(1): 162-167

www.mathematicaljournal.com
Received: 01-04-2025
Accepted: 04-05-2025

Dr. Anju Sharma
BRCM College of Engineering and Technology, Bahal, Bhiwani, Haryana, India

Corresponding Author:
Dr. Anju Sharma
BRCM College of Engineering and Technology, Bahal, Bhiwani, Haryana, India

A description of the class of composite length cyclic codes

Anju Sharma

DOI: https://www.doi.org/10.22271/math.2025.v6.i1b.240

Abstract
In this study, a novel subclass of cyclic codes with composite length is constructed. In order to efficiently encode and decode data, we offer the generator matrix for the built cyclic codes. This research focuses on creating a new kind of cyclic code with lengths that are not prime, by developing a generator matrix for efficient coding and then analyzing its weight distribution to better understand its error correction capabilities. We also demonstrate a few findings about their weight distribution. Our results advance the theory of cyclic codes and may find use in a number of domains, including cryptography, error-correcting codes, and communication systems.

Keywords: Novel construction, cyclic codes, cryptography, communication systems

1. Introduction
In this paper, we present the mathematical features of coding theory, including definitions, fundamental findings, and coding theory examples that are frequently used to prepare and prove findings in the proposed study's subsequent research. A brief history of codes over mathematical structures is also presented. In any digital communication over a noisy channel, codes are helpful. Errors are inevitable during the transmission process since the information is encoded as a codeword and sent over a noisy channel. Our objective is to find the mistakes, fix them, and retrieve the original data.
This method will involve a variety of parameters, bounds, and algorithms. Codes, linear codes, and the parameters that improve a code are defined in this study. The abbreviation "channel" refers to the information transmission channel. Commonly used channels include carrier lines, cable, optical fiber, radio wave transmission mediums, tape, optical disks, etc. The physical circumstances allowing social information to travel across time and space are made up of the channel. A piece of social information, including data, pictures, and different languages, should also be shared across time and distance. The fundamental technical tool for this is information coding. Information coding: what is it? It is, in essence, the process of digitizing various types of social data. Digitization is full of deep mathematical concepts and exquisite mathematical technology rather than just being a digital replacement of social knowledge. For instance, the source code used for data storage and compression attaches the necessary statistical properties to social information using the probability statistics concept; so, the source code is also known as random code. The third method for overcoming channel interference is called "channel coding." This kind of code is full of beautiful algebra, geometry and many mathematical approaches in combinatorics, in order to improve the accuracy of information transmission, hence the channel coding is also called algebraic combinatorial code. One intriguing subset of linear codes is cyclic codes. Because of their effective encoding and decoding methods, they are widely used in storage and communication systems, even if their error-correcting capabilities may not be as powerful as those of generic linear codes.
Among the well-known families of cyclic codes are binary Hamming codes, quadratic residue codes, BCH codes, and Golay codes. The creation of cyclic codes with advantageous parameters and characteristics is still a fascinating problem even after much research, especially in light of their recent uses in the creation of convolutional and locally recoverable codes. In this work, we concentrate on building cyclic codes for composite lengths with favorable characteristics and properties. Let's look at a finite field F_q of order q, where q is a quadratic residue for both n and r, and n and r are different odd primes that fulfill $\gcd(nr, q) = 1$. Ding *et al.* (2011) used quadratic residue codes of lengths n and r

independently to demonstrate three designs of cyclic codes of length nr and dimensions $\frac{(nr+1)}{2}$ over F_q. Maosheng *et al.* (2001) expanded on Ding's work by offering a comprehensive theory for cyclic codes of composite length nr and offering a partial explanation for the comparatively high minimum distance of cyclic codes derived from Ding's constructs. On the basis of quadratic residue codes of length n, they also presented a comprehensive construction of cyclic codes of length nr and dimension $\frac{(n+1)r}{2}$. Cyclic codes, which are linear error-correcting codes that are frequently employed in information and communication technology, are introduced in the second portion of this research study. We use the theory of finite fields to explore their algebraic structure and properties. Concatenated codes (Forney, 1965) and their characteristics are briefly reviewed in the third section. A building method for a certain class of cyclic codes with composite length is presented in the fourth section.

Verma and Sharma (2024) [1] The design of additive complementary dual (ACD) codes over finite fields Fq2 with respect to the trace inner products, where q is a prime power, is examined in this paper. Initially, we link a generating matrix a matrix to an additive code. Next, we give generating matrices for the trace Hermitian and the trace Euclidean inner products to represent ACD codes. Using these techniques, we create a variety of trace Euclidean and trace Hermitian ACD codes with better parameters than the most well-known linear codes over F9 and F4 of the same length and dimension.

Zhang and Liao (2022) [2] examined the fixed points of q-element involutions over the finite field. In order to derive a necessary and sufficient condition that the composite function $f_1 \circ f_2(x)$ is also an involution over the finite field, this work also examines the relationship between the fixed points set and the non-fixed points set of two involutions $f_1(x)$ and $f_2(x)$. Specifically, a unique class of involutions over certain finite fields is fully identified.

Guo *et al.* (2014) [10] proposed concatenating an outer Tanner code of length 155 with an inner polar code of length 4096, taking into account the presence of intermediate channels. The outer Tanner code was applied to the intermediate channels to offer additional protection.

Hamada (2008) [7] A concatenation technique for quantum error correcting codes is introduced. The technique works with a broad class of Calderbank Shor-Steane (CSS) codes, which are quantum error-correcting codes. Consequently, codes that are decodable in polynomial time and attain a high rate in the Shannon theoretic sense are introduced. The rate is the highest that CSS codes are known to be able to achieve. Additionally, the best known bound on the smallest distance of codes that can be constructed in polynomial time is enhanced for a variety.

Ling, S., and Sole, P. (2001) [5] present a novel algebraic method for quasi-cyclic codes. A quasi-cyclic code over a field should be viewed as a linear code over an auxiliary ring. That ring can be broken down into a direct product of fields using the Discrete Fourier Transform (DFT) or the Chinese Remainder Theorem (CRT). Constructions for quinting and septing are presented. The ring decomposition also allows for a trace representation that generalizes the one for cyclic codes and a characterization of self-dual quasi-cyclic codes.

Niu *et al.* (2020) [6] Permutations whose compositional inverses are they are called involutions over finite fields. Applications for involutions, particularly over Fq with q, are numerous and include coding theory and cryptography. Since the paper for binary fields, a lot of effort has been paid to the explicit study of involutions (including their fixed points). In this research, we propose an involutory variant of the AGW Criterion to examine constructions of involutions over finite fields. We analyze polynomials of various kinds to illustrate our generic building strategy.

Rabet *et al.* (2023) [4] the finite Euclidean and Projective geometry codes are the most known among One-Step Majority-Logic Decodable codes that are Low-Density Parity-Check codes as well. To offer a bigger range of possible alphabets for each code, we propose new construction by redefining the incidence vector of the lines of Euclidean and projective geometries over finite fields.

Assmus *et al.* (1976) [3] the majority decoding method, which is somewhat different from Massey's threshold decoding, uses the primary characteristics of the generalized t-designs that were introduced. The article also includes a list of codes that our technology can decode as well as several findings regarding the presence of such designs in codes.

Xiao *et al.* (2017) [8] In this study, we present a concatenated coding scheme that consists of an inner Finite Field low-density parity check (LDPC) code of medium length and high rate, and an outside Reed-Muller (RM) code. It reduces the inner Finite Field LDPC code's error floor. This concatenation approach is simple to use and allows for design flexibility. Furthermore, there are no dangerous trapping sets of size lower than the minimum distance of the outer code, and the decoding operates in a serial turbo way. According to the simulation results, the inner Finite Field LDPC code's dominant trapping sets can be removed using the suggested serial concatenation. Recently, there has been a lot of interest in concatenating LDPC codes with various error correction codes.

In order to reduce the error floor, Eslami *et al.* (2013) [9] concatenated a long polar code of length 32768 as the outside code on a long inner LDPC code of length 34493 for the Optical Transport Network. The generator matrix for the generated cyclic code, an essential tool for the encoding and decoding procedures, is then given in the fifth part. Proving conclusions pertaining to the weight distribution of the built cyclic code—a crucial indicator of its error-correcting ability—is the main goal of the sixth segment. The final section wraps up the study paper by providing a summary of the key discoveries and contributions. We offer future study topics in the realm of coding theory and talk about possible uses for the developed cyclic code.

2. Objectives of the study

- To Description of the Class of Composite Length Cyclic Codes
- To design composite length codes that perform as well as or better than existing codes of the same length and dimension, as determined by their minimum distance and error-correcting capabilities.
- To create codes that can be encoded and decoded efficiently using algorithms that exploit their algebraic structure, making them practical for real-world systems.

3. Scope of the study

Composite length cyclic codes are a class of error-correcting codes whose length is a composite number, often formed by combining shorter cyclic codes, such as those derived from quadratic residues. Their scope involves constructing codes with desirable properties like high minimum distance and efficiency in communication and storage systems, with objectives to enhance error correction capabilities and enable practical implementation through efficient encoding and decoding algorithms.

- The primary goal is to construct codes that offer robust error correction, often aiming for a minimum distance that approaches theoretical bounds, such as the square-root bound for binary codes.
- There is ongoing theoretical research to understand their algebraic properties, develop better constructions, and derive lower bounds on their minimum distance.

4. Data analysis and Discussions

A common type of linear error-correcting code in information and communication technology is the cyclic code. They have a unique algebraic structure that makes encoding and decoding processes more effective. We provide a summary of the basic ideas behind cyclic coding in this section. Let a finite field with q elements be represented by $\mathbb{F}_q$. The linear code C that demonstrates the cyclic shift property is a cyclic code of length n over $\mathbb{F}_q$. This characteristic suggests that if a codeword $c = (c_0, c_1, \dots, c_{n-1})$ is a member of C, then so is its cyclic shift $c_{n-1}, c_0, c_1, \dots, c_{n-2}$). In essence, cyclic codes do not change when their code words undergo cyclic shifts. The generator polynomial g(x), a divisor of the polynomial $x^n - 1$in the polynomial ring $\mathbb{F}_q[x]$, can be used to build cyclic codes.

In particular, the code C, which is represented as $C = \{f(x) \in \mathbb{F}_q[x] \mid g(x)$ divides f(x), contains all polynomials that are divisible by g(x). The generating polynomial g(x) has degree k, where k is the dimension of the code. The code's generator matrix, represented by G, is constructed with the help of the generator polynomial g(x). The coefficients of the polynomial $x^{i-1}g(x)$ for $1 \leqslant i \leqslant k$ are represented by the *i-th* row of this $k \times n$ matrix. The matrix vector multiplication c = mG, where m is a message vector of length k, can therefore be used to obtain any codeword c from the code C.

Furthermore, the generator polynomial $g(x)$ can be used to determine the parity check matrix H of the code C. The coefficients of the polynomial $x^{i-1}(x^n - 1)/g(x)$ for $1 \leqslant i \leqslant n - k$ are represented by the rows of this matrix, which has dimensions $(n - k) \times n$. Interestingly, the equation $cH^T = 0$, where H^T is the transpose of H, is satisfied by any codeword c from the code C. Cyclic codes are useful for error correction because of a number of their characteristics. For example, the generator polynomial approach can be used to find the minimal distance of a cyclic code. The roots of g(x) over an extension field of $\mathbb{F}_q$ must be calculated. Furthermore, methods like the Reed-Solomon algorithm and the Berlekamp Massey algorithm can be used to effectively encode and decode cyclic codes. These characteristics make cyclic codes effective instruments in the study of coding theory.

4.1 Concatenation for Cyclic Code

In this section, we review the definition and fundamental characteristics of concatenated codes. $\mathbb{F}_q$, where q is a prime power, represents the finite field with q elements throughout the text. Let $\mathbb{F}_{q^k}$ and $\mathbb{F}_{q}{}^{n}$ represent the degree k extension of $\mathbb{F}_q$ and an n-dimensional vector space over $\mathbb{F}_q$, respectively, for positive integers $k \leqslant n$.

Definition: Let C be a linear code over $\mathbb{F}_{q^k}$ with parameters $[N, K, d(C)$. Set $A := \text{im}(\pi) = \pi(\mathbb{F}_{q^k})$, which is a $[n, k, d(A)]$ linear code over $\mathbb{F}_q$, and let $\pi: \mathbb{F}_{q^k} \to \mathbb{F}_q^n$ be an $\mathbb{F}_q$–linear injection. Next, the set

$$\pi(C) := \{(\pi(c_1), \dots, \pi(c_N)) : (c_1, \dots, c_N) \in C\} \quad \dots. (1)$$

is also known as a concatenated code, and it is represented by the symbol $A \in C$. In this case, A is referred to as inner code, and C as exterior code. When π's domain is expanded to $\mathbb{F}_{q^k}^N$, it becomes injective. Thus, π(C) is a linear code over $\mathbb{F}_q$ with parameters $[nN, kK]$. The smallest distance d(π(C)) is clearly smaller than the bounded distance d(A)d(C).

In this example, we will use concatenated code to create cyclic code with greater parameters than previous codes. In particular, we will provide the precise minimum distance of the created cyclic code, which aids in determining its precise error-correcting and detection capabilities. In section 3, we continue the definition and notation, specifically referring to the map π.

Theorem 1: Consider the linear code $C = \{(\alpha, \alpha, \dots, \alpha) : \alpha \in \mathbb{F}_{q^k}\}$ with parameters [N,1,N] over $\mathbb{F}_{q^k}$ and the cyclic code $A = \text{im}(\pi) = \pi(\mathbb{F}_{q^k})$ with parameters $[n, k, d(A)]$ over $\mathbb{F}_q$. Then, the parameters $[nN, k, d(A)N]$ over $\mathbb{F}_q$ make up the cyclic code A∈C.

Proof: Consider the linear code $C = \{(\alpha, \alpha, \dots, \alpha) : \alpha \in \mathbb{F}_{q^k}\}$ with parameters [N,1,N] over $\mathbb{F}_{q^k}$ and the cyclic code $A = \text{im}(\pi) = \pi(\mathbb{F}_{q^k})$with parameters $[n, k, d(A)]$ over $\mathbb{F}_q$.

∴ The linear code $A \in C = \{(\pi(\alpha), \dots, \pi(\alpha)) : \alpha \in \mathbb{F}_{q^k}\}$ has parameters $[nN, k, d(A \in C)]$, where $d(A \in C) \geqslant Nd(A)$. To determine A's precise minimum distance from C:

$$d(A \in C) = \min\{d((\pi(\alpha), \dots, \pi(\alpha)), (\pi(\beta), \dots, \pi(\beta))) : \alpha, \beta \in \mathbb{F}_{q^k}\}$$
$$\therefore d(A \in C) = \min\{d(A)d(\pi(\alpha), (\pi(\beta)) : \alpha, \beta \in \mathbb{F}_{q^k}\} \quad \dots. (2)$$

$$\therefore d(A \in C) = d(A) \times \min\{d(\pi(\alpha), (\pi(\beta)): \alpha, \beta \in \mathbb{F}_{q^k}\}$$
$$\therefore d(A \in C) = d(A)d(C) = d(A)N \quad \ldots. (3)$$

$\therefore$ With parameters $[n, k, d(A)]$ over $\mathbb{F}_q, A \in C$ is a linear code. To demonstrate that $A \in C$ is cyclic code:
Reflect on

$$(\underbrace{c_1, c_2, \ldots, c_n}_{1}, \underbrace{c_{n+1}, \ldots, c_{2n}}_{2}, \ldots, \underbrace{c_{(N-1)n+1}, \ldots, c_{Nn}}_{N}) \in A \in C \quad \ldots. (4)$$

$\therefore \exists \alpha \in \mathbb{F}_{q^k} \ldots (5)$
s.t.

$$\pi(\alpha) = (c_1, c_2, \ldots, c_n) = (c_{n+1}, \ldots, c_{2n}) = \cdots = (c_{(N-1)n+1}, \ldots, c_{Nn}) \in A$$

$$\therefore c_1 = c_{n+1} = \cdots = c_{(N-1)n+1}, c_2 = c_{n+2} = \cdots = c_{(N-1)n+2}, \cdots, c_n = c_{2n} = \cdots = c_{Nn} \quad \ldots. (6)$$

Since we know that A is cyclic code, we obtain

$$(c_n, c_1, \ldots, c_{n-1}) \in A$$
$$\therefore \exists \beta \in \mathbb{F}_{q^k} \text{ s.t. } \pi(\beta) = (c_n, c_1, \ldots, c_{n-1})$$
$$\therefore \pi(\beta) = (c_{Nn}, c_1, \ldots, c_{n-1}) = (c_n, c_{n+1}, \ldots, c_{2n-1}) = \cdots = (c_{(N-1)n}, c_{(N-1)n+1}, \ldots, c_{Nn-1})$$
$$\therefore \left(\underbrace{c_{Nn}, c_1, \ldots, c_{n-1}}_{1}, \underbrace{c_n, c_{n+1}, \ldots, c_{2n-1}}_{2}, \ldots, \underbrace{c_{(N-1)n}, c_{(N-1)n+1}, \ldots, c_{Nn-1}}_{N}\right) \in A \in C \quad \ldots. (7)$$
$$\therefore A \in C \text{ is a parameterized cyclic code } [nN, k, d(A)N] \text{ over } \mathbb{F}_q.$$

Corollary 1: Let $A = \text{im}(\pi) = \pi(\mathbb{F}_{q^k})$be a cyclic code with the parameters $[k, k, d(A)]$ over $\mathbb{F}_q$ and $C = \{(\alpha, \alpha, \ldots, \alpha): \alpha \in \mathbb{F}_{q^k}\}$ be a linear code with the parameters $[N, 1, N]$ over $\mathbb{F}_{q^k}$. With the parameters $[kN, k, N]$ over $\mathbb{F}_q$, the A∈C is a cyclic code.

Proof: Let $A = \text{im}(\pi) = \pi(\mathbb{F}_{q^k})$be a cyclic code with the parameters $[k, k, d(A)]$ over $\mathbb{F}_q$and $C = \{(\alpha, \alpha, \ldots, \alpha): \alpha \in \mathbb{F}_{q^k}\}$ be a linear code with the parameters $[N, 1, N]$ over $\mathbb{F}_{q^k}$. We may construct A∈C is cyclic code with the parameters $[kN, k, d(A)N]$ over $\mathbb{F}_q$ by using the aforementioned Theorem 1. A is obviously a sub code of $\mathbb{F}_q^k$ and $\dim(A) = k$.

$$\therefore A = \mathbb{F}_q^k$$
$$\therefore d(A) = 1 \quad \ldots. (8)$$

The parameters of the cyclic code

$$\therefore \text{A∈C are } [kN, k, N] \text{ over } \mathbb{F}_q \quad \ldots. (9)$$

4.2 The Constructed Cyclic Code Generator Matrix

Using the generator polynomial of inner code A, we will provide the generator polynomials for created cyclic code and its dual in this section.

Theorem 2: Consider the linear code $C = \{(\alpha, \alpha, \ldots, \alpha): \alpha \in \mathbb{F}_{q^k}\}$ with parameters $[N, 1, N]$ over $\mathbb{F}_{q^k}$ and the cyclic code $A = \text{im}(\pi) = \pi(\mathbb{F}_{q^k})$ with parameters $[n, k, d(A)]$ over $\mathbb{F}_q$. If g(x) is a generator polynomial of $A \in C$, then $G(x) = (1 + x^n + x^{2n} + \cdots + +x^{(N-1)n})g(x)$is a generator polynomial of $A \in C$.

Proof: Let $A = \text{im}(\pi) = \pi(\mathbb{F}_{q^k})$, and $C = \{(\alpha, \alpha, \ldots, \alpha): \alpha \in \mathbb{F}_{q^k}\}$be linear codes with parameters $[N, 1, N]$ over $\mathbb{F}_{q^k}$ have the parameters $[n, k, d(A)]$ over $\mathbb{F}_q$, and be a cyclic code.

$\therefore$ The parameters of the cyclic code $A \in C$are $[kN, k, N]$ over $\mathbb{F}_q$. To determine $A \in C$ generating polynomial: Reflect on

$\pi: F_q^n \to \frac{F_q[x]}{\langle x^n - 1\rangle}$ moreover $\pi': F_q^{Nn} \to \frac{F_q[x]}{\langle x^{Nn} - 1\rangle}$ amorphous as $\pi((c_1, c_2, \ldots, c_n)) = c_1 + c_2 x + \cdots + c_n x^{n-1}$ as well as $\pi'\left((c_1, c_2, \ldots, c_n, c_{n+1}, \ldots, c_{2n}, \ldots, c_{(N-1)n+1}, \ldots, c_{Nn})\right) = c_1 + c_2 x + \cdots \ldots + c_n x^{n-1} + c_{n+1} x^n + \cdots + c_{2n} x^{2n-1} + \cdots + c_{((N-1)n+1)} x^{(N-1)n} + \cdots \cdot c_{Nn} x^{Nn-1}$ correspondingly.

reflect on $(c_1, c_2, \dots, c_n, c_{n+1}, \dots, c_{2n}, \dots, c_{(N-1)n+1}, \dots, c_{Nn}) \in A \in C$

$\therefore \exists \alpha \in \mathbb{F}_{q^k}$ such that $\pi(\alpha) = (c_1, c_2, \dots, c_n) = (c_{n+1}, \dots, c_{2n}) = \cdots =$

$(c_{(N-1)n+1}, \dots, c_{Nn}) \in A$

$\therefore c_1 = c_{n+1} = \cdots = c_{(N-1)n+1}, c_2 = c_{n+2} = \cdots = c_{(N-1)n+2}, \dots, c_n = c_{2n} =$

$\dots = c_{Nn} \dots \dots . (10)$

$\therefore \pi' \left((c_1, c_2, \dots, c_n, c_{n+1}, \dots, c_{2n,}, \dots, c_{(N-1)n+1}, \dots, c_{Nn}) \right) = c_1 + c_2 x + \cdots \dots +$

$c_n x^{n-1} + c_{n+1} x^n + \cdots + c_{2n} x^{2n-1} + \cdots + c_{((N-1)n+1)} x^{(N-1)n} + \cdots . c_{Nn} x^{Nn-1}$

$\therefore = c_1 + c_2 x + \cdots + c_n x^{n-1} + c_1 x^n + c_2 x^{(n+1)} + \cdots + c_n x^{2n-1} + \cdots + c_1 x^{((N-1)n} +$

$c_2 x^{(N-1)n+1} + \cdots + c_n x^{Nn-1}$

$\therefore = (c_1 + c_2 x + \cdots + c_n x^{n-1}) + (c_1 + c_2 x + \cdots + c_n x^{n-1}) x^n + \cdots + (c_1 + c_2 x +$

$\dots + c_n x^{n-1}) x^{((N-1)n}$

$\therefore = \left(1 + x^n + x^{2n} + \cdots + x^{(Nn-1)}\right)(c_1 + c_2 x + \cdots + c_n x^{n-1})$

$\therefore = \left(1 + x^n + x^{2n} + \cdots + x^{(Nn-1)}\right) f(x) g(x)$

$\therefore \left(1 + x^n + x^{2n} + \cdots + x^{(Nn-1)}\right) g(x)$ is monic least degree polynomial s.t.

$\pi'(A \in C) =< \left(1 + x^n + x^{2n} + \cdots + x^{(Nn-1)}\right) g(x) >$

$\therefore \left(1 + x^n + x^{2n} + \cdots + x^{(Nn-1)}\right) g(x)$ is originator polynomial of $A \in C$ ... (11)

Theorem 3: Consider the linear codes $C = \{(\alpha, \alpha, \dots, \alpha): \alpha \in \mathbb{F}_{q^k}\}$ and $A = \text{im}(\pi) = \pi(\mathbb{F}_{q^k})$ with parameters $[N, 1, N]$ over $\mathbb{F}_{q^k}$ and $[n, k, d(A)]$ over $\mathbb{F}_q$, respectively. If $c \in A \in C$, then $N \mid \text{wt}(c)$.

Proof: Consider the linear codes $C = \{(\alpha, \alpha, \dots, \alpha): \alpha \in \mathbb{F}_{q^k}\}$ and $A = \text{im}(\pi) = \pi(\mathbb{F}_{q^k})$ with parameters$[N, 1, N]$ over $\mathbb{F}_{q^k}$ and $[n, k, d(A)]$ over $\mathbb{F}_q$, respectively. Regard as $c \in A \in C$

$\therefore \exists \alpha \in \mathbb{F}_{q^k}$ s.t. $c = (\pi(\alpha), \dots, \pi(\alpha))$ …. (12)

Using the definition,

$wt(c) = wt((\pi(\alpha), \dots, \pi(\alpha)))$

$\therefore wt(c) = N \times wt(\pi(\alpha))$ …. (13)

$\therefore N \mid wt(c)$

It is evident from the aforementioned theorem 6.1 that the weight distribution of A yields the weight distribution of the created cyclic code.

5. Conclusion

Using concatenated codes, we have demonstrated the design of a class of cyclic codes with better parameters in the entire section of our research study. We have supplied the generator matrix for the built cyclic code in the final part. Lastly, we have shown some findings regarding created cyclic code in the final section.

6. Limitations

- The research is specific to cyclic codes, which might limit its broader impact if other types of error-correcting codes offer better performance or different advantages for specific applications.
- The methods developed for composite lengths may not easily extend to other types of codes or to lengths with specific characteristics, potentially restricting the scope of the findings.
- Although the goal is to develop efficient coding, the practical performance and complexity of encoding and decoding algorithms for these new codes might not be fully analyzed or might be higher than standard, widely-used codes for specific applications.

7. Further Scope of the study

- Investigate how these codes can be adapted to construct quantum codes for error detection and correction in quantum systems, a key challenge in quantum information theory, as suggested by research on quantum codes with long lengths.
- Beyond the current use of generator matrices for efficient encoding, research can focus on developing specialized decoding algorithms tailored to the unique properties of these composite-length cyclic codes to further improve their efficiency.

References

1. Verma GK, Sharma RK. Construction of additive complementary dual codes over finite fields. Applicable Algebra in Engineering, Communication and Computing. 2024; [Epub ahead of print]:1-8. doi:10.1007/s00200-025-00693-7.
2. Zhang Z, Liao Q. A new construction for involutions over finite fields. Front Math China. 2022;17:553-65. doi:10.1007/s11464-022-1023-0.

3. Assmus E, Goethals JM, Mattson H. Generalized t-designs and majority decoding of linear codes. Information and Control. 1976;32:43-60. doi:10.1016/S0019-9958(76)90101-7.
4. Rabet ZM, Ayoub F, Belkasmi M, Bouanani FE. Construction of new finite geometry non-binary LDPC codes with reduced alphabets. Proc 6th Int Conf Adv Commun Technol Netw. 2023;1-8. doi:10.1109/CommNet60167.2023.10365279.
5. Ling S, Sole P. On the algebraic structure of quasi-cyclic codes I: Finite fields. IEEE Trans Inf Theory. 2001;47(1):2751-60. doi:10.1109/18.959257.
6. Niu T, Li K, Qu L, Wang Q. New constructions of involutions over finite fields. Cryptogr Commun. 2020;12(2):165-85. doi:10.1007/s12095-019-00386-2.
7. Hamada M. Concatenated quantum codes achieving high rates with polynomial-time error estimation or construction. Quantum Inf Process. 2008;7:1-15. doi:10.1007/s11128-007-0071-y.
8. Xiao X, Nasseri M, Vasic B, Lin S. Serial concatenation of Reed Muller and LDPC codes with low error floor. Proc 55th Annu Allerton Conf Commun Control Comput. 2017;688-93. doi:10.1109/ALLERTON.2017.8262810.
9. Eslami A, Pishro-Nik H. On finite-length performance of polar codes: stopping sets, error floor, and concatenated design. IEEE Trans Commun. 2013;61:919-29. doi:10.1109/TCOMM.2013.011413.110727.
10. Guo J, Qin M, Fabregas AG, Siegel PH. Enhanced belief propagation decoding of polar codes through concatenation. Proc IEEE Int Symp Inf Theory (ISIT). 2014;2987-91. doi:10.1109/ISIT.2014.6875393.