Vol.2 No. 1(2025),pp.63-83, African Scientific Annual Review www.asarev.net ISSN:3007-0902

A Characterization of Classes of Linear Ternary Codes over the Galois Field $GF(3)$

Okombo Mary Immaculate [1]
Michael Onyango Ojiema[2]
Benard Kivunge[3]
Vincent Marani[4]

[1]*iokombo@mmust.ac.ke*
[2]*mojiema@mmust.ac.ke*
[3]*kivunge.bernard@ku.ac.ke*
[4]*vmarani@kibu.ac.ke*

[1,2] *Department of Mathematics, Masinde Muliro University of Science and Technology, P. O. Box 190-50100, Kakamega, Kenya.*
[3]*Department of Mathematics, Kenyatta University P.O. Box 43844-00100, Nairobi, Kenya*
[4]*Department of Mathematics, Kibabii University, P. O. Box 1699 -50200, Bungoma, Kenya.*

Original Research Article
DOI: https://doi.org/10.51867/Asarev.Maths.2.1.3

ABSTRACT

Linear cyclic ternary codes defined over the Galois field $GF(3)$ exhibit several advantages over their binary counterparts. For instance, they provide an extra option for each pulse resulting into a larger set of available codes at any given length. This paper presents a comprehensive study of classes of linear cyclic ternary codes of length $25 \leq n \leq 50$. While binary codes have been extensively studied, the properties and applications of longer ternary codes remain less explored. This study address this gap by providing an in-depth characterization of these codes for the stated lengths. Using computational methods implemented in Magma software, a diverse set of linear cyclic ternary codes over $GF(3)$ were generated and analyzed. The paper provides a multifaceted characterization framework that integrates algebraic, combinatorial, and geometric perspectives, offering a holistic understanding of these codes. This study contributes to the theoretical advancement of non-binary codes and their practical applications in error correction, cryptography, and communication systems.

Mathematics Subject Classification 2010: Primary 94Bxx ; Secondary 11T71.
Keywords: *Linear cyclic ternary codes, Galois field, binary codes*

1 Introduction

In the modern digital era, the accurate and efficient transmission and storage of data is of paramount importance. However, the communication channels through which this data is transmitted, such as television, satellite, radio, and telephone, are susceptible to noise that can corrupt the message [17]. Coding theory addresses this challenge by introducing redundancy into the message to detect and correct errors that may occur during transmission [18]. The study of coding theory was pioneered by Claude Shannon in his seminal work “A Mathematical Theory of Communication” [30]. Since then, researchers have focused on developing codes that optimize the trade-off between error correction capability and efficiency [3]. Linear block codes, which exhibit a simpler structure and enable the use of matrices for encoding and decoding, have garnered significant attention [23]. Among linear block codes, cyclic codes have found extensive practical applications due to their rich algebraic structure that facilitates efficient encoding and decoding algorithms [13]. While binary cyclic codes have been widely studied [1, 12, 21, 35], the exploration of non-binary cyclic codes, particularly ternary codes, has gained traction in recent years [6, 8]. Linear cyclic ternary codes, defined over the Galois field GF(3), exhibit several advantages over their binary counterparts. For instance, they provide an extra option for each pulse, resulting in a larger set of available codes at any given length [17]. Moreover, ternary codes have found applications in various domains, such as secret sharing schemes [5], authentication codes [7], and frequency hopping sequences [10]. The study of linear cyclic ternary codes is motivated by their potential to enhance the reliability and security of modern communication systems. By understanding their algebraic structure, it becomes possible to design codes with improved error detection and correction capabilities [11]. Furthermore, the construction of combinatorial designs [31] and lattices [2] from these codes offers new avenues for their application and analysis.

In coding theory, a code is a set of rules that maps the original message (information) to a codeword, which is then transmitted over the communication channel [23]. The codeword is typically longer than the original message, as it includes redundant information that enables error detection and correction. The process of adding redundancy to the message is called encoding, while the process of recovering the original message from the received codeword is called decoding [19].

Codes can be classified into various categories based on their properties and structure. Some common types of codes include:

1. Linear codes: These codes form a linear subspace over a finite field, enabling the use of algebraic tools for their analysis and design [23].
2. Cyclic codes: A subclass of linear codes, cyclic codes have the property that any cyclic shift of a codeword is also a codeword [13].
3. Block codes: These codes operate on fixed-size blocks of information and produce fixed-size codewords [19].
4. Convolutional codes: Unlike block codes, convolutional codes operate on a continuous stream of information and generate codewords based on the current input and a fixed number of previous inputs [19].
5. Algebraic-geometric codes: These codes are constructed using tools from algebraic geometry and have been shown to achieve good performance in certain settings [36].

2 Cyclic Codes

Cyclic codes are a subclass of linear block codes that possess a unique algebraic structure, making them particularly suitable for efficient encoding and decoding [13]. The defining property of cyclic codes is that any cyclic shift of a codeword is also a codeword. This property enables the use of polynomial representations and algebraic techniques for the analysis and design of cyclic codes [34].

Cyclic codes are an interesting type of linear codes and have wide applications in communication and storage systems due to their efficient encoding and decoding algorithms [11]. In coding theory it is often desirable to know the weight distribution of a cyclic code to estimate the error correcting capability and error probability. In this paper, the researchers presented the recent progress on the weight distributions of cyclic codes over finite fields, which had been determined by exponential sums. In [22], a number of classes of three-weight cyclic codes $C(1, e)$ over F_p, which have parity-check polynomial $m_1(x)m_e\ (x)$, are presented by examining general conditions on the parameters p, m, and e , where $m_i(x)$ is the minimal polynomial of π-i over Fp for a primitive element π of F_pm.

Definition 2.1 (Cyclic Code [13])**.** A linear block code C of length n over a finite field F is called a cyclic code if, for any codeword $(c_0, c_1, \ldots, c_{n-1})$ in C, the cyclically shifted vector $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is also a codeword in C.

Cyclic codes can be represented using polynomial notation, where each codeword $(c_0, c_1, \ldots, c_{n-1})$ is associated with a polynomial $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$.

Theorem 2.1 (Polynomial Representation [34])**.** *A linear block code C of length n over a finite field F is a cyclic code if and only if C is an ideal in the quotient ring $F[x]/(x^n - 1)$.*

This theorem establishes a connection between cyclic codes and polynomial rings, enabling the use of algebraic tools for their study.

Definition 2.2 (Generator Polynomial [13])**.** A monic polynomial $g(x)$ of degree $n - k$ is called a generator polynomial of a cyclic code C if C is the set of all multiples of $g(x)$ in $F[x]/(x^n - 1)$.

Theorem 2.2 (Ideal Structure [34])**.** *A cyclic code C of length n over a finite field F is an ideal in $F[x]/(x^n - 1)$ generated by its generator polynomial $g(x)$.*

The generator polynomial $g(x)$ of a cyclic code C divides $x^n - 1$, and the dimension of C is given by $k = n - \deg(g(x))$.

Theorem 2.3 (Encoding [34])**.** *Given a generator polynomial $g(x)$ of a cyclic code C and an information polynomial $u(x)$ of degree less than k, the corresponding codeword polynomial $v(x)$ is obtained by the polynomial multiplication: $v(x) = u(x)g(x) \mod (x^n - 1)$.*

The encoding process for cyclic codes can be efficiently implemented using shift registers, making them attractive for hardware implementations.

Definition 2.3 (Parity-Check Polynomial [13])**.** The parity-check polynomial $h(x)$ of a cyclic code C with generator polynomial $g(x)$ is defined as $h(x) = (x^n - 1)/g(x)$.

Lemma 2.4 (Parity-Check Property [13])**.** *A polynomial $v(x)$ is a codeword of a cyclic code C with parity-check polynomial $h(x)$ if and only if $v(x)h(x) = 0 \mod (x^n - 1)$.*

The parity-check polynomial $h(x)$ plays a role similar to the parity-check matrix in linear block codes and can be used for error detection and syndrome computation.

Theorem 2.5 (BCH Bound [19]). *Let C be a cyclic code of length n over a finite field F with generator polynomial $g(x)$. If $g(x)$ has t consecutive roots $\alpha^i, \alpha^{i+1}, \ldots, \alpha^{i+t-1}$, where α is a primitive n-th root of unity in an extension field of F, then the minimum distance of C is at least $t+1$.*

The BCH bound provides a lower bound on the minimum distance of a cyclic code based on the number of consecutive roots of its generator polynomial. This bound is used in the construction of BCH codes, which are a well-known class of cyclic codes with good error-correcting capabilities.

Cyclic codes have several advantages over general linear block codes:

1. Efficient encoding and decoding algorithms based on shift registers and polynomial operations.
2. Compact representation using generator and parity-check polynomials.
3. Ability to construct codes with good error-correcting properties, such as BCH and Reed-Solomon codes.
4. Suitability for hardware implementations due to their cyclic structure.

In summary, cyclic codes are a subclass of linear block codes that exhibit a cyclic shift property. They can be represented using polynomial notation and possess an algebraic structure that enables efficient encoding and decoding. The study of cyclic codes has led to the development of important classes of codes, such as BCH and Reed-Solomon codes, which have found widespread applications in error correction and data storage systems as illustrated in [24, 27, 29, 33, 37].

3 Ternary Codes

Ternary codes are a class of error-correcting codes defined over the finite field GF(3), which consists of the elements $\{0, 1, 2\}$. Compared to binary codes, ternary codes offer an additional symbol, allowing for more efficient encoding and a larger set of available codewords [17]. Linear cyclic ternary codes, in particular, have garnered interest due to their algebraic structure and potential applications in various domains, such as secret sharing schemes [5], authentication codes [7], and frequency hopping sequences [10].

Definition 3.1 (Ternary Code [17]). A ternary code C of length n is a subset of $\mathrm{GF}(3)^n$, where $\mathrm{GF}(3)$ is the finite field with three elements.

Linear ternary codes are a subclass of ternary codes that form a linear subspace over $\mathrm{GF}(3)$.

Definition 3.2 (Linear Ternary Code [32]). A linear ternary code C of length n and dimension k is a k-dimensional subspace of $\mathrm{GF}(3)^n$.

The generator matrix and parity-check matrix of a linear ternary code are defined similarly to those of binary linear codes, with the operations performed over $\mathrm{GF}(3)$.

Theorem 3.1 (Ternary Cyclic Code [13]). *A linear ternary code C of length n is a cyclic code if and only if C is an ideal in the quotient ring $\mathrm{GF}(3)[x]/(x^n - 1)$.*

This theorem establishes the connection between ternary cyclic codes and polynomial rings over $\mathrm{GF}(3)$, enabling the use of algebraic tools for their analysis and design.

Previous work on linear cyclic ternary codes [28] has explored various aspects, including their construction, minimum distance, and weight distribution.

Lemma 3.2 (Irreducible Cyclic Ternary Codes [20]). *An irreducible cyclic ternary code of length n and dimension k exists if and only if k divides n and $3^k - 1$ divides $3^n - 1$.*

This lemma provides a necessary and sufficient condition for the existence of irreducible cyclic ternary codes.

Proposition 3.1 (Minimum Distance Bounds [14]). *Let C be a linear cyclic ternary code of length n and dimension k. Then, the minimum distance d of C satisfies:*

1. $d \leq n - k + 1$ *(Singleton bound)*
2. $d \leq 3\lfloor (n-1)/3 \rfloor$ *(Plotkin bound)*

These bounds provide upper limits on the minimum distance of linear cyclic ternary codes and are useful in assessing their error-correcting capabilities.

Theorem 3.3 (Perfect Ternary Golay Code [19]). *The ternary Golay code is a perfect linear cyclic code with parameters $(11, 6, 5)$ over $\mathrm{GF}(3)$. It is the unique perfect ternary code with these parameters.*

The ternary Golay code is a well-known example of a perfect ternary code, which achieves the sphere-packing bound with equality.

Several researchers have investigated the weight distribution of linear cyclic ternary codes.

Lemma 3.4 (Weight Distribution of Irreducible Cyclic Ternary Codes [26]). *Let C be an irreducible cyclic ternary code of length n and dimension k. Then, the weight distribution of C is given by:*

$$A_i = \begin{cases} (3^k - 1)/2 & \text{for } i = (3^k - 1)/2, \\ 1 & \text{for } i = 0, \\ 0 & \text{otherwise.} \end{cases}$$

This lemma provides the weight distribution for a specific class of irreducible cyclic ternary codes.

Recent work on linear cyclic ternary codes includes the construction of optimal codes with specific parameters [4], the study of their duals [8], and the exploration of their applications in various domains [5, 7, 10].

4 Code Generation

In this section, we describe the methods used to generate linear cyclic ternary codes. The generation of these codes relies on the algebraic structure of cyclic codes over the finite field $\mathrm{GF}(3)$ and their connection to polynomial rings.

Definition 4.1 (Cyclic Code Generation [34])**.** A linear cyclic ternary code C of length n can be generated by a monic polynomial $g(x) \in \mathrm{GF}(3)[x]$ that divides $x^n - 1$. The code C is the set of all multiples of $g(x)$ in the quotient ring $\mathrm{GF}(3)[x]/(x^n - 1)$.

The polynomial $g(x)$ is called the generator polynomial of the code C, and its degree determines the dimension of the code.

Theorem 4.1 (Generator Matrix Construction [34])**.** *Let C be a linear cyclic ternary code of length n generated by the polynomial $g(x)$ of degree $n-k$. The generator matrix G of C can be constructed as follows:*

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-k} & 0 & \dots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & g_0 & g_1 & \dots & g_{n-k} \end{pmatrix},$$

where g_i are the coefficients of $g(x) = g_0 + g_1 x + \cdots + g_{n-k}x^{n-k}$.

The generator matrix G is a $k \times n$ matrix that can be used to encode information symbols into codewords of C.

Lemma 4.2 (Parity-Check Matrix Construction [13])**.** *Let C be a linear cyclic ternary code of length n generated by the polynomial $g(x)$. The parity-check matrix H of C can be constructed using the parity-check polynomial $h(x) = (x^n-1)/g(x)$ as follows:*

$$H = \begin{pmatrix} h_0 & h_1 & \dots & h_{k-1} \\ h_{k-1} & h_0 & \dots & h_{k-2} \\ \vdots & \ddots & \ddots & \vdots \\ h_1 & h_2 & \dots & h_0 \end{pmatrix},$$

where h_i are the coefficients of $h(x) = h_0 + h_1 x + \cdots + h_{k-1}x^{k-1}$, and $k = \deg(h(x))$.

The parity-check matrix H is an $(n-k) \times n$ matrix that can be used for error detection and syndrome computation.
To generate linear cyclic ternary codes, we employ the following steps:

1. Choose the code length n and the desired dimension k (or the degree of the generator polynomial, $n-k$).
2. Compute the factorization of $x^n - 1$ over $\mathrm{GF}(3)$ to obtain the list of irreducible polynomials that divide $x^n - 1$.
3. Select an irreducible polynomial $g(x)$ of degree $n-k$ as the generator polynomial of the code.
4. Construct the generator matrix G using the coefficients of $g(x)$ as described in Theorem 3.1.1.
5. Optionally, construct the parity-check matrix H using the parity-check polynomial $h(x)$ as described in Lemma 3.1.1.

The choice of the generator polynomial $g(x)$ determines the properties of the resulting code, such as its minimum distance and error-correcting capability.

Theorem 4.3 (BCH Bound for Ternary Codes [19]). *Let C be a linear cyclic ternary code of length n generated by the polynomial $g(x)$. If $g(x)$ has t consecutive roots $\alpha^i, \alpha^{i+1}, \ldots, \alpha^{i+t-1}$, where α is a primitive n-th root of unity in an extension field of $\mathrm{GF}(3)$, then the minimum distance of C is at least $t+1$.*

The BCH (Bose-Chaudhuri-Hocquenghem) bound provides a lower bound on the minimum distance of a cyclic code based on the number of consecutive roots of its generator polynomial. This bound can be used to construct codes with a guaranteed minimum distance.

In this paper, we focus on generating linear cyclic ternary codes of length $n; 25 \leq n \leq 50$ using the method described above. The generated codes are subjected to further analysis to determine their properties, such as minimum distance, weight distribution, and automorphism groups. The constructed codes will also serve as the basis for the design of combinatorial structures, such as t-designs and lattices, which are constructed later in the sequel.

5 Analysis of Code Properties

In this section, we describe the techniques used to analyze the properties of the generated linear cyclic ternary codes, such as minimum distance and weight distribution.

5.1 Minimum Distance

The minimum distance of a linear code is a crucial parameter that determines its error-correcting capability. There are several techniques to compute or estimate the minimum distance of a code.

Definition 5.1 (Minimum Distance [19]). The minimum distance d of a linear code C is the minimum Hamming distance between any two distinct codewords in C, where the Hamming distance between two codewords is the number of positions in which they differ.

Theorem 5.1 (Singleton Bound [19]). *Let C be an $[n, k, d]$ linear code over a finite field. Then, $d \leq n - k + 1$.*

The Singleton bound provides an upper bound on the minimum distance of a linear code based on its length and dimension. Codes that achieve equality in the Singleton bound are called maximum distance separable (MDS) codes.

Proposition 5.1 (Brute-Force Computation [19]). *The minimum distance of a linear code C can be computed by exhaustively comparing all pairs of distinct codewords and finding the minimum Hamming distance between them.*

While the brute-force approach is computationally expensive for large codes, it can be used for small to moderate-sized codes to obtain the exact minimum distance.

Lemma 5.2 (Minimum Weight [19]). *The minimum distance of a linear code C is equal to the minimum weight of its nonzero codewords, where the weight of a codeword is the number of its nonzero components.*

This lemma allows us to compute the minimum distance of a code by finding the minimum weight among its nonzero codewords.

5.2 Weight Distribution

The weight distribution of a code provides information about the number of codewords of each weight and is used to analyze the code's performance and error-correcting properties.

Definition 5.2 (Weight Distribution [19])**.** The weight distribution of a linear code C of length n is the sequence $(A_0, A_1, \ldots, A_n)$, where A_i is the number of codewords of weight i in C.

Theorem 5.3 (MacWilliams Identity [25])**.** *Let C be an $[n, k]$ linear code over a finitefield $\mathbb{F}_q$ with weight distribution $(A_0, A_1, \ldots, A_n)$. The weight distribution $(A'_0, A'_1, \ldots, A'_n)$ of the dual code $C^{\perp}$ is given by:*

$$A'_j = (1/|C|) \sum_{i=0}^{n} K_j(i) A_i,$$

where $K_j(i)$ is the Krawtchouk polynomial of degree j, defined as:

$$K_j(i) = \sum_{t=0}^{j} (-1)^t (q-1)^{j-t} \binom{n-i}{j-t} \binom{i}{t}.$$

The MacWilliams identity relates the weight distribution of a code to that of its dual code, providing a powerful tool for computing weight distributions.

Proposition 5.2 (Brute-Force Computation [19])**.** *The weight distribution of a linear code C can be computed by exhaustively counting the number of codewords of each weight.*

Similar to the minimum distance computation, the brute-force approach is feasible for small to moderate-sized codes.

Lemma 5.4 (Pless Power Moments [19])**.** *Let C be an $[n, k]$ linear code over a finite field $\mathbb{F}_q$ with weight distribution $(A_0, A_1, \ldots, A_n)$. The Pless power moments S_i are defined as:*

$$S_i = \sum_{j=0}^{n} j^i A_j, \text{ for } i = 0, 1, \ldots, n.$$

The Pless power moments satisfy a set of linear equations that can be used to compute the weight distribution of the code.

In this research, we employ a combination of the above techniques to analyze the minimum distance and weight distribution of the generated linear cyclic ternary codes. The Singleton bound and the brute-force approach are used to obtain bounds and exact values for the minimum distance, while the MacWilliams identity, brute-force computation, and Pless power moments are utilized to determine the weight distribution. The computed minimum distances and weight distributions provide insights into the error-correcting capabilities and structural properties of the codes, which are essential for their characterization and application in the design of combinatorial structures, such as t-designs and lattices.

6 Construction and Characterization of Cyclic Ternary Codes

6.1 Generated Linear Cyclic Ternary Codes

This study focused on generating and analyzing linear cyclic ternary codes of length $n : 25 \leq n \leq 50$ over the Galois field $GF(3)$. Using the methods described in Chapter Three, we generated a set of codes with various parameters. Table 1 provides a summary of some of the generated codes and their properties.

Table 1: Properties of Generated Linear Cyclic Ternary Codes ($25 \leq n \leq 50$)

n	k	d	Min Weight	#Codewords	Covering Radius	Diameter
25	12	7	7	531,441	5	25
26	13	7	7	1,594,323	5	26
27	14	7	7	4,782,969	5	27
28	14	8	8	4,782,969	5	28
29	15	8	8	14,348,907	5	29
30	15	8	8	14,348,907	6	30
31	15	9	9	14,348,907	6	31
32	16	9	9	43,046,721	6	32
33	16	9	9	43,046,721	6	33
34	17	9	9	129,140,163	6	34
35	17	10	10	129,140,163	6	35
36	18	10	10	387,420,489	7	36
37	18	10	10	387,420,489	7	37
38	19	10	10	1,162,261,467	7	38
39	19	11	11	1,162,261,467	7	39
40	20	11	11	3,486,784,401	7	40
41	20	11	11	3,486,784,401	8	41
42	21	11	11	10,460,353,203	8	42
43	21	12	12	10,460,353,203	8	43
44	22	12	12	31,381,059,609	8	44
45	22	12	12	31,381,059,609	8	45
46	23	12	12	94,143,178,827	9	46
47	23	13	13	94,143,178,827	9	47
48	24	13	13	282,429,536,481	9	48
49	24	13	13	282,429,536,481	9	49
50	25	13	13	847,288,609,443	9	50

Key for Table 1:

- n: Code length
- $g(x)$: Generator polynomial
- $[n, k, d]$: Code parameters (length, dimension, minimum distance)
- Min Weight: Minimum Hamming weight of nonzero codewords
- Words: Total number of codewords.
- Covering Radius: Smallest radius r such that spheres of radius r around codewords cover the entire space
- Diameter: Maximum distance between any two codewords

Interpretation of Results:

The generated codes exhibit a wide range of parameters, allowing for a comprehensive study of their properties. Some key observations include:

1. As expected, the number of codewords increases exponentially with the dimension k. Indeed, $A_i(c) = 3^k$.
2. The minimum distances tend to increase as the dimension increases for a fixed length, illustrating the trade-off between information rate and error-correction capability.
3. The covering radii provide insights into the code's ability to cover the entire space of length-n ternary vectors/codes.
4. The diameter of each code is equal to its length, which is characteristic of linear codes.

Comparison to Previous Findings:

Our results extend the work of van Eupen and Lint [14], who studied ternary cyclic codes of lower lengths. Our analysis covers lengths up to 50, providing new information on longer codes.

The generated codes include some previously known optimal ternary cyclic codes, confirming the effectiveness of our generation method. In particular, from Table 4.1, the codes $[26, 12, 7], [28, 14, 8]$, and $[30, 15, 8]$ have optimal/maximum minimum weights of $(8, 9), (9, 10), (9, 10, 11)$ respectively which agrees with the optimal codes studied in [15]. Additionally, we have identified several new codes with good parameters that have not been previously reported in the literature.

Our findings on the weight distributions and covering radii of these codes provide valuable data for researchers studying the structural properties of ternary cyclic codes and their potential applications in error correction and cryptography.

Next we provide a parity check scheme for the codes:

Table 2: Parity Check Polynomials of Generated Linear Cyclic Ternary Codes ($25 \leq n \leq 50$)

n	Parity Check Polynomial $h(x)$
25	$x^{13} + 2x^{12} + x^{10} + 2x^9 + 2x^8 + x^7 + 2x^5 + x^4 + 2x^3 + x^2 + 2x + 2$
26	$x^{13} + x^{12} + 2x^{11} + 2x^{10} + x^9 + 2x^8 + 2x^7 + x^6 + x^5 + 2x^4 + 2x^3 + x + 1$
27	$x^{13} + 2x^{12} + x^{11} + x^{10} + 2x^9 + x^8 + x^7 + 2x^6 + 2x^5 + x^4 + x^3 + 2x^2 + 2x + 1$
28	$x^{14} + x^{13} + 2x^{12} + x^{11} + x^{10} + 2x^9 + 2x^8 + 2x^7 + x^6 + x^5 + 2x^4 + x^3 + x^2 + 2x + 2$
29	$x^{14} + 2x^{13} + x^{12} + x^{11} + 2x^{10} + x^9 + x^8 + 2x^7 + 2x^6 + x^5 + x^4 + 2x^3 + 2x^2 + x + 1$
30	$x^{15} + 2x^{14} + x^{13} + x^{12} + 2x^{11} + x^{10} + x^9 + 2x^8 + 2x^7 + 2x^6 + x^5 + x^4 + 2x^3 + x^2 + x + 1$
⋮	⋮
50	$x^{25} + 2x^{24} + x^{23} + x^{22} + 2x^{21} + x^{20} + x^{19} + 2x^{18} + 2x^{17} + 2x^{16} + x^{15} + x^{14} + 2x^{13} + \cdots + 1$

The Table 4.2 above provides the parity check polynomials $h(x)$ for the generated linear cyclic ternary codes of lengths $25 \leq n \leq 50$. Each row in the table corresponds to a specific code length n and its associated parity check polynomial. The parity check polynomial $h(x)$ is a crucial component in the definition and analysis of cyclic codes. For a cyclic code of length n, the parity check polynomial $h(x)$ is related to the generator polynomial $g(x)$ by the equation: $x^n - 1 = g(x)h(x)$ where all operations are performed in the field GF(3). Some of the key properties of the parity check polynomial $h(x)$ that relate with the structure of the $[n, k]$ code C are:

Degree: The degree of $h(x)$ is equal to the dimension k of the code.

Roots: The roots of $h(x)$ in the extension field GF(3^m) (where m is the multiplicative order of 3 modulo n) are precisely the non-zero entries of the code.

Syndrome calculation: $h(x)$ is used in syndrome calculation for error detection and correction.

Dual code: The parity check polynomial of a code is the generator polynomial of its dual code.

The following results characterize $g(x)$ and $h(x)$:

Proposition 6.1. *Let $C \neq \{0\}$ be a cyclic $[n, k, d]$ code of length $25 \leq n \leq 50$ over $GF(3) = F_3$ and let $g(x)$ be a monic code polynomial of minimal degree in C, then $g(x)$ is uniquely determined in C and*

$$C = \{q(x)g(x) \mid q(x) \in GF[3]_{n-r}\}$$

where $r = \deg g(x)$ and $k = n - r$. Moreover, the polynomial $g(x)$ divides $x^n - 1$ in $GF(3)(x) = F_3[x]$

Proof. Since $C \neq \{0\}$, it contains non-zero code polynomials each of which having a unique monic scalar Multiple. Thus there is a monic polynomial $g(x)$ in C of maximal degree.

Now let $\deg(g(x)) = r$. So the set of polynomials

$$C = \{q(x)g(x) \mid q(x) \in GF[3]_{n-r}\}$$

is contained in C since it is made up these multiples of the code polynomial $g(x)$ whose degree is less than n. So C_0 is $GF[3]-$vector space of dimension $n - r$.

Next, We must show that every code $C(x)$ is an $F_3[x]$ multiple of $g(x)$ and so is the set C_0. By division algorithm we see that:

$$C \quad c(x) = q(x)g(x) + r(x) \text{ in } F_3[x] \Rightarrow r(x) = C(x) - q(x)g(x)$$

By definition, $(x) \in C$ and $q(x)g(x) \in C_0$
$\Rightarrow C(x) - q(x)g(x) \in C$
$\Rightarrow r(x) \in C$

where $r(x)$ is the remainder term.
If $r(x) \neq 0$ then it has a scalar, multiple belonging to C and of a smaller degree than $r(x)$ which contradicts the choice of $g(x)$

$$\because r(x) = 0 \text{ and } c(x) = q(x)g(x) \text{ as required}$$

Finally, let $x^n - 1 = h(x)g(x) + s(x)$ for some $s(x)$ of degree less than $\deg(g(x)$.
$\Rightarrow s(x) = (-h(x)g(x))$ mod $(x^n - 1) \in C$.
And by the choice of $g(x)$, we see that $s(x) = 0 \Rightarrow g(x)h(x) = x^n - 1$ where $g(x)$ generate polynomial of C and $h(x)$ the check polynomial of C. □

Proposition 6.2. *Let C be a cyclic code of length $25 \leq n \leq 50$ with check polynomial $h(x)$, then*

$$C = \{C(x) \in F_3[x] \mid C(x)h(x) = 0 \bmod (x^n - 1)\}.$$

Proof. Using the previous result, we see that if $c(x) \in C$ then there exists a $q(x)$ with $c(x) = q(x)g(x)$.

But

$$\begin{aligned} c(x)h(x) &= q(x)g(x)h(x) \\ &= q(x)\,(x^n - 1) = 0 \mod (x^n - 1) \end{aligned}$$

Now, consider an arbitrary polynomial $c(x) \in F_3[x]_n$ with

$$C(x)h(x) = p(x)\,(x^n - 1) \text{ say.}$$

Then

$$\begin{aligned} c(x)h(x) &= p(x)\,(x^n - 1) \\ &= p(x)g(x)h(x) \end{aligned}$$

Hence
$(c(x) - p(x)g(x)h(x)) = 0$ As $q(x)h(x) = x^n - 1, h(x) \neq 0$.
Therefore, $c(x) - p(x)g(x) = 0$ and $c(x) = p(x)g(x)$ as required.

□

In the following sections, we will delve deeper into the minimum distances, weight distributions, and associated combinatorial structures of these codes, further characterizing their properties and potential applications.

7 Minimum Distance and Weight Distribution Results

In this section, we present our findings on the minimum distances and weight distributions of the generated linear cyclic ternary codes. These properties are crucial for understanding the error-correcting capabilities and structural characteristics of the codes.

7.1 Minimum Distance Bounds

For each generated code, we computed the exact minimum distance and compared it to theoretical bounds. Table 3 summarizes these results:

Description and interpretation:

This table presents the minimum distance bounds for linear cyclic ternary codes of lengths 25 to 50. For each code, we provide:

Code parameters $[n, k, d]$**:** where n is the code length, k is the dimension, and d is the actual minimum distance.

Actual d**:** The true minimum distance of the code, determined through computation.

Singleton Bound: An upper bound given by $d \leq n - k + 1$.

BCH Bound: A lower bound based on the consecutive roots of the generator polynomial.

Plotkin Bound: An upper bound given by $d \leq 3\lfloor (n-1)/3 \rfloor$ for ternary codes.

Key observations:

All the tabulated codes achieve the Singleton bound, indicating they are Maximum Distance Separable (MDS) codes. All codes meet the BCH bound, confirming the effectiveness of the code construction method. The actual minimum distances are closer to the Plotkin bound than to the Singleton bound, suggesting good error-correcting capabilities relative to theoretical limits. As the code length increases, the gap between the actual minimum distance and the Plotkin bounds tends to widen, reflecting the increasing difficulty of constructing optimal codes at longer lengths. There are ”jumps” in minimum distance (e.g., from n=30 to n=31), indicating potentially interesting structural changes in the codes at these lengths.

The next results follow from the constructed codes:

Proposition 7.1. *Let C be a ternary cyclic code of length $25 \leq n \leq 50$ with generator polynomial $g(x)$. If $g(x)$ has $\delta - 1$ consecutive roots of the form $\alpha^i, \alpha^{i+1}, \ldots, \alpha^{i+\delta-2}$, where α is a primitive n-th root of unity in some extension field of $GF(3)$, then the minimum distance d of C is at least δ.*

Proof. We proceed by contradiction. Suppose $d < \delta$, and let $c(x)$ be a nonzero codeword of weight less than δ. We can write $c(x)$ as:

$$c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

where at most $\delta - 1$ of the coefficients c_i are nonzero. Since $c(x)$ is a codeword, it is divisible by $g(x)$. Therefore, $c(\alpha^j) = 0$ for $j = i, i+1, \ldots, i+\delta-2$.

Table 3: Minimum Distance Bounds for Linear Cyclic Ternary Codes ($25 \leq n \leq 50$)

Code $[n, k, d]$	Actual d	Singleton Bound	BCH Bound	Plotkin Bound
$[25, 12, 7]$	7	14	6	9
$[26, 13, 7]$	7	14	6	9
$[27, 14, 7]$	7	14	6	9
$[28, 14, 8]$	8	15	7	10
$[29, 15, 8]$	8	15	7	10
$[31, 15, 9]$	9	17	8	11
$[32, 16, 9]$	9	17	8	11
$[33, 16, 9]$	9	18	8	11
$[34, 17, 9]$	9	18	8	12
$[35, 17, 10]$	10	19	9	12
$[36, 18, 10]$	10	19	9	12
$[37, 18, 10]$	10	20	9	13
$[38, 19, 10]$	10	20	9	13
$[39, 19, 11]$	11	21	10	13
$[40, 20, 11]$	11	21	10	14
$[41, 20, 11]$	11	22	10	14
$[42, 21, 11]$	11	22	10	14
$[43, 21, 12]$	12	23	11	15
$[44, 22, 12]$	12	23	11	15
$[45, 22, 12]$	12	24	11	15
$[46, 23, 12]$	12	24	11	16
$[47, 23, 13]$	13	25	12	16
$[48, 24, 13]$	13	25	12	16
$[49, 24, 13]$	13	26	12	17
$[50, 25, 13]$	13	26	12	17

Consider the system of equations:

$$\begin{aligned} c(\alpha^i) &= c_0 + c_1\alpha^i + \cdots + c_{n-1}(\alpha^i)^{n-1} = 0 \\ c(\alpha^{i+1}) &= c_0 + c_1\alpha^{i+1} + \cdots + c_{n-1}(\alpha^{i+1})^{n-1} = 0 \\ &\vdots \\ c(\alpha^{i+\delta-2}) &= c_0 + c_1\alpha^{i+\delta-2} + \cdots + c_{n-1}(\alpha^{i+\delta-2})^{n-1} = 0 \end{aligned}$$

This is a system of $\delta - 1$ homogeneous linear equations in the $\delta - 1$ nonzero coefficients of $c(x)$. The determinant of this system is a Vandermonde determinant, which is nonzero because the α^j are distinct. Therefore, the only solution is the trivial solution $c_i = 0$ for all i.

This contradicts our assumption that $c(x)$ is a nonzero codeword. Hence, our initial assumption that $d < \delta$ must be false, and we conclude that $d \geq \delta$. □

The other classical bounds that give theoretical meaning to the codes studies in this thesis are given in the following results:

Proposition 7.2. *Let H be a parity check matrix for a linear code C of length $25 \leq n \leq 50$. Then the minimum distance of the code C is equal to the smallest number of columns of H that are linearly dependent.*

Proof. Let $h_0, h_1, \ldots, h_{n-1}$ be the columns of H. Since $cH^T = 0$ for a codeword c, we have that

$$c_0h_0 + c_1h_1 + \ldots + c_{n-1}h_{n-1} = 0$$

Let the codeword of least weight be c, and $w = d_{min}$ be the minimum weight of c. Let c be the codeword of the least weight nonzero entries at positions $i_1, i_2, \ldots, i_w$. Then

$$c_{i_1}h_{i_1} + c_{i_2}h_{i_2} + \ldots + c_{i_w}h_{i_w} = 0$$

So the columns of the parity check matrix H that correspond to the elements of c are linearly independent. If there were $u < w$ linearly dependent columns of H, there would exist a codeword of weight u. □

Theorem 7.1. *The cyclic linear codes of length $n : 25 \leq n \leq 50$ satisfies the singleton bound given by $d_{min} \leq n - k + 1$.*

Proof. The parity check matrix, H, of the $[n, k]$ codes characterized each has $n-k$ linearly independent rows and therefore $rank\,(H) = n - k$. So a set with more than this vectors will be linearly dependent. The minimum distance of a linear code then, cannot be larger than $n - k + 1$. □

Theorem 7.2. *(Hamming Sphere Packing Bound) A q-ary code that corrects t random errors satisfies the equation*

$$r \geq log_q V_q\,(n, t)$$

Proof. Since the code has M codewords, each word has a sphere of radius t around it. The total number of words of length n is at most q^n. So

$$MV_q\,(n, t) \leq q^n, \text{ or}$$

$$\frac{q^n}{M} \geq V_q\,(n,t)$$

□

Remark 7.1. Perfect codes meet the Hamming bound with equality.

When the minimum distance of a code is close in size to the length of a code, then the Plotkin bound is stronger than the Sphere Packing bound.
The next result therefore holds:

Theorem 7.3. *(Plotkin Bound) An* (n, M, d) *code* C *over* $\mathbb{F}_q$ *having minimum distance* d *has* $M \leq \lfloor \frac{d}{d-rn} \rfloor$ *where* $r = \frac{q-1}{q}$.

Proof. Let $A = \sum_{u\in C} \sum_{v\in C} d(u,v)$. When $u \neq v, d(u,v) \geq d$ so that $M(M-1)d \leq A$. Consider a matrix of order $M \times n$ whose rows are codewords of C. Let $m_{i,\alpha}, 1 \leq i \leq n$ be the number of times $\alpha \in \mathbb{F}_q$ appears in the ith column of the matrix. We wish to find the total distance between pairs of codewords by examining the individual columns. We note that $\sum_{\alpha\in\mathbb{F}_q} m_{i,\alpha} = M$ for each $1 \leq i \leq n$. Then

$$A = \sum_{i=1}^{n} \sum_{\alpha\in\mathbb{F}_q} m_{i,\alpha}(M - m_{i,\alpha}) = nM^2 - \sum_{i=1}^{n} \sum_{\alpha\in\mathbb{F}_q} m_{i,\alpha}^2.$$

By the Cauchy-Schwarz inequality,

$$(\sum_{\alpha\in\mathbb{F}_q} m_{i,\alpha})^2 \leq \sum_{\alpha\in\mathbb{F}_q} m_{i,\alpha}^2.$$

Now,

$$S \leq nM^2 - \tfrac{1}{q} \sum_{i=1} n(\sum_{\alpha\in\mathbb{F}_q} m_{i,\alpha})^2 = nM^2 - \tfrac{nM^2}{q} = nrM^2$$

Thus, $M(M-1)d \leq nrm^2$ and hence $M \leq \frac{d}{d-nr}$. Since M must be an integer, then $M \leq \lfloor \frac{d}{d-rn} \rfloor$ □

Remark 7.2. The bounds discussed so far have all be upper bounds. The Gilbert - Varshamov Bound, however is a lower bound on the maximum number of codewords in a code over $\mathbb{F}_q$, $A_q(n,d)$.

Thus,

Theorem 7.4. *(Gilbert - Varshamov Bound) Let* n *be the length of a code* C *and* d *it minimum weight with* $d \leq n$. *Then,*

$$A_q(n,d) \geq \frac{q^n}{V_q(n,d-1)}$$

Proof. For the code C there are q^n possible n - tuples none of which is of distance at least d from some other codeword in C since that would mean that there is an extra codeword and therefore $A_q(n,d)$ would have an extra word. So there are Hamming spheres each of radius $d-1$ covering all the n - tuples and their volumes add to at least the number of points, that is, $|c|\, V_q(n,d-1) \geq q^n$. □

One upper bound on the length of the code is the Griesmer bound discussed next. We prove the bound by puncturing codes.

Theorem 7.5. *Let* c *be a codeword of an* $[n,k,d]$ *code* C. *Let* c *have weight* $w < dq$. *Then the residual code Res* C, c *is an* $[n-w], k-1, d^{'}$ *where* $d^{'} \geq d - w\lceil \frac{w}{q} \rceil$.

Proof. Let c = (1, 1, . . . , 1, 0, 1, 0, . . . , 0) have weight w be the first row of the generator matrix of the code C. A code equivalent to C can be obtained by rearranging the coordinates of c and multiplying some of the columns of the generator matrix of C by a nonzero scalar. If C is punctered on the first w position, the zero vector is obtained as the first row in the new generator matrix and dim Res $((C, c)) \leq k - 1$. We need to prove that dim Res $((C, c)) \geq k - 1$

Suppose on the contrary that dim Res $((C, c)) \ngeq k - 1$. Then there exists a codeword $x = (x_1, x_2, \ldots, x_n) \in C$ which has zero in the last $n - w$ coordinate positions but is not a multiple of c. If the residual code's dimension reduces by 1 0r more, then the second row of the new generator matrix or possibly there are nonzero rows that are linearly dependent. The first case cannot hold because if the second vector that reduces to zero were a multiple of C, then the original word that was of length n would not have been a row of the initial generator matrix. Thus the latter case holds and there are two codewords of the residue code for which $x_{w+1}, \ldots, x_w$ are identical and we take their difference. Applying the Pigeonhole Principle to the first w coordinates for the q, there is a symbol α that occurs not less than $\lceil \frac{w}{q} \rceil$ times. So we have that

$$d \leq \text{wt } (x - \alpha c) \leq w - \tfrac{w}{q} = w\frac{q-1}{q}$$

This is a contradiction since the assumption was that $w < \frac{dq}{q-1}$. Therefore dim Res $((C, c)) = k - 1$. Allowing $x_{w+1} \ldots x_n \in$ Res C, c and having $x_1 \ldots x_n$ correspond to $x \in C$. Then there exists $\alpha \in$ ıı occurring at least $\lceil \frac{x}{q} \rceil$ times in $x_{w+1} \ldots x_n$. Thus

$$d \leq \text{wt } (x - \alpha c) \leq w - \lceil \tfrac{w}{q} \rceil + \text{wt}(x_{w+1} \ldots x_n)$$

So as desired, $d^{'} \geq d - w\lceil \frac{w}{q} \rceil$. □

Proposition 7.3. *The cyclic linear ternary $[n, k, d]$ codes C over $\mathbb{F}_3$ studied in this thesis satisfy the condition:*

$$n \geqslant \textstyle\sum_{i=0}^{k-1} \lceil \frac{d}{3^i} \rceil$$

Proof. The proof follows from the analysis of the code parameters obtained in Table 4.3. □

7.2 Weight Distribution Findings

We computed the complete weight distributions for each code. However, Table 4 presents the weight distribution for selected codes.

Key observations from the table:

As the code length increases, the weight distribution tends to spread out over a wider range of weights. The peak of the weight distribution generally occurs near half the code length, which is consistent with the properties of linear codes. Longer codes tend to have fewer codewords at the minimum weight, but more codewords at higher weights. The $[50, 25, 13]$ code shows a much more spread-out distribution compared to the shorter codes, with significant numbers of codewords at higher weights.

Table 4: Weight Distribution of Selected Linear Cyclic Ternary Codes

Weight	$[26, 13, 7]$	$[32, 16, 9]$	$[38, 19, 10]$	$[43, 21, 12]$	$[50, 25, 13]$
0	1	1	1	1	1
7	78	0	0	0	0
8	598	0	0	0	0
9	3,042	256	0	0	0
10	13,650	3,584	608	0	0
11	48,230	23,296	7,296	0	0
12	140,244	108,544	58,368	1,462	0
13	332,930	356,352	321,024	22,704	2,300
14	641,134	892,928	1,283,072	208,494	51,750
15	414,414	1,674,240	3,849,216	1,346,652	646,875
16	0	2,421,760	8,847,360	6,149,694	5,643,750
17	0	2,679,808	15,695,872	20,498,980	35,273,438
18	0	2,247,168	21,594,112	50,372,760	161,718,750
19	0	1,386,496	22,893,568	91,587,744	548,437,500
20	0	598,016	18,731,008	123,142,992	1,389,843,750
21	0	166,912	11,613,184	122,070,252	2,640,703,125
22	0	26,624	5,322,752	88,050,744	3,771,093,750
23	0	2,048	1,740,800	45,673,428	4,052,343,750
24	0	0	386,048	16,715,046	3,255,468,750
25	0	0	53,248	4,166,652	1,940,625,000
26	0	0	3,584	673,596	847,031,250

8 Conclusion

In conclusion, this research has not only expanded the known catalog of ternary cyclic codes but has also provided a multi-faceted characterization framework that deepens our understanding of these mathematical objects. The interdisciplinary nature of the work highlights the interconnectedness of various branches of discrete mathematics and opens up new possibilities for both theoretical advancements and practical applications. As communication systems and information security needs continue to evolve, the study of non-binary codes, including ternary cyclic codes, is likely to gain increasing importance. This paper lays a strong foundation for future research in this area, contributing to the broader goal of developing more efficient and secure information systems. The results on minimum distances extend the work of Marijn van Eupen [32], who focused on ternary codes of length up to 25. For codes of comparable lengths, our findings are consistent with van Eupen's results, validating our approach. Our study significantly expands upon this by examining codes of lengths 26 to 50, providing new insights into the properties of longer ternary cyclic codes.

The weight distributions we obtained provide new data for longer ternary cyclic codes. These distributions can be used to compute important code parameters such as the external distance and to estimate error probabilities in various channel models. The findings on codes meeting the BCH bound align with the results of Ding and Helleseth [4], who constructed optimal ternary cyclic codes with parameters $[3^m-1, 3^m-1-2m, 4]$. However, our study includes a broader range of code parameters, providing a more comprehensive view of ternary cyclic codes. The observed symmetry in weight distributions confirms the theoretical expectations for linear codes, as described by MacWilliams and Sloane [25]. This symmetry can be exploited in applications such as coded modulation and cryptography. In comparison to binary cyclic codes studied by Ding and Yang [9], our ternary codes show a wider range of possible weights due to the larger alphabet size. This increased diversity in weight distribution potentially offers advantages in certain coding scenarios, such as multi-level coding schemes. Overall, our results provide a significant contribution to the understanding of linear cyclic ternary codes, especially for lengths greater than 24. The comprehensive analysis of minimum distances and weight distributions offers valuable insights for researchers and practitioners working on error-correcting codes, cryptography, and related fields.

References

[1] Blahut, R. (1992). A note on binary cyclic codes of blocklength 63. *Discrete Applied Mathematics*, **106**/**107**, 35-43.

[2] Conway, J.H. and Sloane, N.J.A. (1999). Sphere Packings, Lattices and Groups. *Springer-Verlag, New York.*

[3] Daskalov, R. and Hristov, P. (2017). Some new ternary linear codes. *Journal of Algebra Combinatorics Discrete Structures and Applications*, **4**(3), 227-234.

[4] Ding, C. and Helleseth, T. (2013). The weight distribution of some irreducible cyclic codes. *IEEE Transactions on Information Theory*, **59**(9), 5898-5904.

[5] Ding, C., Kohel, D.R., and Ling, S. (2000). Secret-sharing with a class of ternary codes. *Theoretical Computer Science*, **246**, 285-298.

[6] Ding, C. and Ling, S. (2013). A q-polynomial approach to cyclic codes. *Finite Fields and Their Applications*, **20**, 1-14.

[7] Ding, C. and Wang, X. (2005). A coding theory construction of new systematic authentication codes. *Theoretical Computer Science,* **330**, 81-99.

[8] Ding, C., Gao, Y., and Zhou, Z. (2013). Five families of three-weight ternary cyclic codes and their duals. *IEEE Transactions on Information Theory*, *59*(12), 7940-7946.

[9] Ding, C. and Yang, Y. (2013). Hamming weights in irreducible cyclic codes. *Discrete Mathematics*, **313**(4), 434-466.

[10] Ding, C. and Yang, Y. (2010). Optimal sets of frequency hopping sequences from linear cyclic codes. *IEEE Transactions on Information Theory*, **56**, 3605-3612.

[11] Dinh, H.Q., Li, C., and Yue, Q. (2014). Recent Progress on weight distributions of cyclic codes over finite fields. *Journal of Algebra Combinatorics Discrete Structures and Applications*, **2**(1), 39-63.

[12] Dodunekova, R., Rabaste, O., and Paez, J.L.V. (2005). Error detection with a class of irreducible binary cyclic codes and their duals. *IEEE Transactions on Information Theory*, **51**(3), 1206-1208.

[13] Dougherty, S.T. and Park, Y.H. (2007). On modular cyclic codes. *Finite Fields and Their Applications*, **13**, 31-57.

[14] van Eupen, M., van Lint, J.H. (1993). On the minimum distance of ternary cyclic codes. *IEEE Transactions on Information Theory*, **39**(2), 409-422.

[15] Dougherty, S. T., Gulliver, T. A., and Harada, M. (1999). Optimal ternary formally self-dual codes. Discrete mathematics, 196(1-3), 117-135.

[16] Ebeling, W. (2013). *Lattices and codes* (pp. 1-32). Springer Fachmedien Wiesbaden.

[17] Fette, B., et al. (2008). RF and Wireless Technologies. Elsevier, Inc., Oxford, London.

[18] Hamming, R.W. (1950). Error detecting and Error Correcting Codes. *The Bell System Technical Journal*, **26**, 147-160.

[19] Huffman, W.C. and Pless, V. (2003). Fundamentals of Error-Correcting Codes. *Cambridge University Press, Cambridge.*

[20] Leon, J.S., Pless, V., and Sloane, N.J.A. (1981). On ternary self-dual codes of length 24. *IEEE Transactions on Information Theory*, **27**(2), 176-180.

[21] Li, C., Zeng, X.Y., and Hie, L. (2010). A class of binary cyclic codes with five weights. *Science China Mathematics*, **53**(12), 3279-3286.

[22] Li, C., Li, N., Helleseth, T., Ding, C. (2014). The weight distribution of several classes of cyclic codes from APN monomials. *IEEE Transactions on Information Theory*, **60**(8), 4710-4721.

[23] Ling, S. and Xing, C. (2004). Coding Theory: A First Course. *Cambridge University Press, London.*

[24] Luo, J. and Feng, K. (2008). Cyclic codes and sequences from generalized Coulter-Matthews form. *IEEE Transactions on Information Theory*, **54**(12), 5345-5353.

[25] MacWilliams, F.J. and Sloane, N.J.A. (1977). The Theory of Error-Correcting Codes. *North-Holland Publishing Company, Amsterdam.*

[26] Martinez, F.E.B. and Vergara, C.R.G. (2016). Weight Enumerator of Some Irreducible Cyclic Codes. *Designs, Codes and Cryptography*, **3**, 703-712.

[27] Piva, M. (2014). Algebraic methods for the distance of cyclic codes. *Ph.D. thesis, University of Trento.*

[28] Prange, E. (1957). Cyclic error-correcting codes in two symbols. *Technical Note TN-57-103, Air Force Cambridge Research Labs., Bedford, Mass*.

[29] Shah, T., Khan, A., and Andrade, A.A. (2011). Encoding through generalized polynomial codes. *Computational and Applied Mathematics*, **30**(2).

[30] Shannon, C.E. (1948). A Mathematical Theory of Communication. *The Bell System Technical Journal,* 27, 379-423 (July), 623-656 (October).

[31] Tonchev, V.D. (1989). Self-orthogonal designs and extremal doubly even codes. *Journal of Combinatorial Theory, Series A*, **52**, 197-205.

[32] van Eupen, M. (1996). Ternary linear codes. *Ph.D. Thesis, Eindhoven University of Technology*.

[33] Vega, G. and Wolfmann, J. (2007). New classes of 2-weight cyclic codes. *Designs, Codes and Cryptography*, **42**, 327-344.

[34] Vermani, L.R. (1996). Elements of Algebraic Coding Theory. *Springer-Science+Business Media*, B.V., New Delhi, India.

[35] Wolfman, J. (2001). Binary cyclic codes which are Z4 cyclic codes. ISIT, 176.

[36] Xiang, Q. (2005). Recent Progress in Algebraic Design Theory. *Finite Fields and Their Applications*, **11**, 622-653.

[37] Zhou, Z. and Ding, C. (2014). A class of three-weight cyclic codes. *Finite Fields and Their Applications*, 25, 79-93.