JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A CONCATENATED CONSTRUCTION OF CLASS OF CYCLIC CODES OF COMPOSITE LENGTH

Saheb Navghare,
Research Student ,
School of Mathematical Sciences,
SRTM University, Nanded-431606, Maharashtra, India

Abstract : This research paper presents the construction of a new subclass of cyclic codes with composite length. We provide the generator matrix for the constructed cyclic codes, which can be used to efficiently encode and decode data. Additionally, we prove some results related to their weight distribution. Our findings contribute to the theory of cyclic codes and have potential applications in various fields, such as communication systems, error-correcting codes, and cryptography.

Index Terms **- Concatenated code; Cyclic code; Construction of cyclic codes.**

I. INTRODUCTION

Cyclic codes are a fascinating category of linear codes. While their error correcting capability may not be as strong as that of general linear codes, they find extensive use in storage and communication systems due to their efficient encoding and decoding algorithms ([3][4][6]). Well-known families of cyclic codes include BCH codes, Golay codes, binary Hamming codes, and quadratic residue codes, among others. Despite being studied for a considerable period, the construction of cyclic codes with favorable parameters and properties remains an intriguing question, particularly considering their newfound applications in the construction of locally recoverable codes ([1][8][5]) and convolutional codes ([7]).

In this study, we focus on constructing cyclic codes with good properties and parameters for composite lengths. Let us consider a finite field F_q of order q, where n and r are distinct odd primes satisfying $\gcd(nr, q) = 1$, and q is a quadratic residue for both n and r. Ding ([2]) presented three constructions of cyclic codes of length nr and dimensions $\frac{(nr+1)}{2}$ over F_q by utilizing quadratic residue codes of lengths n and r separately. Building upon Ding's work, Maosheng et al. ([9][10]) provided a general theory for cyclic codes of composite length nr and partially explained the reason behind the relatively large minimum distance of cyclic codes obtained from Ding's constructions. They also introduced a general construction of cyclic codes with length nr and dimension $\frac{(n+1)r}{2}$ based on quadratic residue codes of length n.

The second section of this research paper provides an introduction to cyclic codes, which are linear error-correcting codes widely used in information and communication technology. We discuss their properties and algebraic structure, drawing upon the theory of finite fields. In the third section, concatenated codes (Forney, 1965) are briefly overviewed along with their properties. The fourth section presents a construction approach for a specific class of cyclic codes with composite length. Subsequently, in the fifth section, we provide the generator matrix for the constructed cyclic code, a crucial tool for both encoding and decoding processes. The sixth section focuses on proving results related to the weight distribution of the constructed cyclic code, a vital measure of its errorcorrecting capability.

Finally, the last section concludes the research paper by summarizing the main findings and contributions. We discuss potential applications of the constructed cyclic code and suggest future research directions in the field of coding theory.

II. PRELIMINARIES

Cyclic codes are a class of linear error-correcting codes widely employed in information and communication technology. They possess a distinct algebraic structure that enables efficient encoding and decoding procedures. In this section, we present an overview of the fundamental concepts related to cyclic codes. For a more comprehensive understanding, interested readers may refer to Huffman and Pless (2010) and Ling and Xing (2004).

Let $\mathbb{F}_q$ denote a finite field comprising q elements. A cyclic code of length n over $\mathbb{F}_q$ is a linear code, denoted as C, which exhibits the cyclic shift property. This property implies that if a codeword $c = (c_0, c_1, \dots, c_{n-1})$ belongs to C, then its cyclic shift $(c_{n-1}, c_0, c_1, \dots, c_{n-2})$ also belongs to C. Essentially, cyclic codes remain invariant under cyclic shifts of their codewords.

Cyclic codes can be defined by their generator polynomial $g(x)$, which is a divisor of the polynomial $x^n - 1$ in the polynomial ring $\mathbb{F}_q[x]$. Specifically, the code C comprises all polynomials divisible by $g(x)$, denoted as $C = \{f(x) \in \mathbb{F}_q[x] \mid g(x) \text{ divides } f(x)\}$. The generator polynomial $g(x)$ possesses a degree of k, where k represents the code's dimension.

The generator polynomial $g(x)$ facilitates the construction of the code's generator matrix, denoted as G. This matrix is of dimensions $k \times n$, where the i-th row corresponds to the coefficients of the polynomial $x^{i-1}g(x)$ for $1 \leqslant i \leqslant k$. Consequently, any codeword c from the code C can be obtained by the matrixvector multiplication $c = mG$, where m represents a message vector of length k.

Additionally, the parity check matrix H of the code C can be derived from the generator polynomial $g(x)$. This matrix has dimensions $(n-k) \times n$, with its rows being the coefficients of the polynomial $x^{i-1}(x^n - 1)/g(x)$ for $1 \leqslant i \leqslant n-k$. Notably, any codeword c from the code C satisfies the equation $cH^T = 0$, where H^T represents the transpose of H.

Cyclic codes possess several properties that render them valuable for error correction. For instance, the minimum distance of a cyclic code can be determined using the generator polynomial method. This involves computing the roots of $g(x)$ over an extension field of $\mathbb{F}_q$. Moreover, cyclic codes can be efficiently encoded and decoded using techniques like the Berlekamp-Massey algorithm and the Reed-Solomon algorithm. These properties establish cyclic codes as powerful tools within the field of coding theory.

III. CONCATENATED CODES

We recall the definition and basic properties of concatenated codes in this section. Throughout the text, $\mathbb{F}_q$ denotes the finite field with q elements, where q is a prime power.

For positive integers $k \leqslant n$, let $\mathbb{F}_{q^k}$ and $\mathbb{F}_q{}^n$ denote the degree k extension of $\mathbb{F}_q$ and an n-dimensional vector space over $\mathbb{F}_q$, respectively.

Definition 3.1. Let C be a linear code with the parameters $[N, K, d(C)]$ over $\mathbb{F}_{q^k}$. Let $\pi: \mathbb{F}_{q^k} \to \mathbb{F}_q^n$ be an $\mathbb{F}_q$--linear injection and set $A := im(\pi) = \pi(\mathbb{F}_{q^k})$, which is an $[n, k, d(A)]$ linear code over $\mathbb{F}_q$. Then the set

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

is called a concatenated code, which is also denoted by $A \square C$. Here, A and C are called inner code and outer code, respectively.

Note that π is injective when its domain is extended to $\mathbb{F}_{q^k}^N$. Hence, $\pi(C)$ is a linear code with parameters $[nN, kK]$ over $\mathbb{F}_q$. It is easy to see that the minimum distance $d(\pi(C))$ is lower bounded by $d(A)d(C)$.

IV. CONCATENATION FOR CYCLIC CODE

In this section, we will construct cyclic code whose parameters will be better than old codes by using concatenated code. specially, we will give exact minimum distance of constructed cyclic code which helps to identify exact error correcting and detecting capacity of constructed cyclic code. We continue with the notation and definition in section 3, in particular about the map π.

Theorem 4.1. Let $C = \{(\alpha, \alpha, \dots, \alpha) : \alpha \in \mathbb{F}_{q^k}\}$ be a linear code with the parameters $[N, 1, N]$ over $\mathbb{F}_{q^k}$ and $A = im(\pi) = \pi(\mathbb{F}_{q^k})$ be a cyclic code with the parameters $[n, k, d(A)]$ over $\mathbb{F}_q$. Then the $A \square C$ is cyclic code with the parameters $[nN, k, d(A)N]$ over $\mathbb{F}_q$.

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

$\therefore\ A \square C = \{(\pi(\alpha), \dots, \pi(\alpha)) : \alpha \in \mathbb{F}_{q^k}\}$ is linear code

with parameters $[nN, k, d(A \square C)]$, where $d(A \square C) \geqslant Nd(A)$.

To find exact minimum distance of $A \square C$:

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

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

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

$$\therefore\ d(A \square C) = d(A)d(C) = d(A)N$$

$\therefore\ A \square C$ is linear code with parameters $[nN, k, d(A)N]$ over $\mathbb{F}_q$

To show $A \square C$ is cyclic code:

Consider $(\underbrace{c_1, c_2, \dots, c_n}_{1}, \underbrace{c_{n+1}, \dots, c_{2n}}_{2}, \dots, \underbrace{c_{(N-1)n+1}, \dots, c_{Nn}}_{N}) \in A \square C$

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

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

We know A is cyclic code, so we get

$$(c_n, c_1, \dots, c_{n-1}) \in A$$

$$\therefore\ \exists \beta \in \mathbb{F}_{q^k} \text{ such that } \pi(\beta) = (c_n, c_1, \dots, c_{n-1})$$

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

$$\therefore\ (\underbrace{c_{Nn}, c_1, \dots, c_{n-1}}_{1}, \underbrace{c_n, c_{n+1}, \dots, c_{2n-1}}_{2}, \dots, \underbrace{c_{(N-1)n}, c_{(N-1)n+1}, \dots, c_{Nn-1}}_{N}) \in A \square C$$

$\therefore A \square C$ is cyclic code with parameters $[nN, k, d(A)N]$ over $\mathbb{F}_q$.

Corollary 4.2. Let $C = \{(\alpha, \alpha, \dots, \alpha) : \alpha \in \mathbb{F}_{q^k}\}$ be a linear code with the parameters $[N, 1, N]$ over $\mathbb{F}_{q^k}$ and $A = im(\pi) = \pi(\mathbb{F}_{q^k})$ be a cyclic code with the parameters $[k, k, d(A)]$ over $\mathbb{F}_q$. Then the $A \square C$ is cyclic code with the parameters $[kN, k, N]$ over $\mathbb{F}_q$.

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

By using above Theorem 4.1 , we can write

$A \square C$ is cyclic code with the parameters $[kN, k, d(A)N]$ over $\mathbb{F}_q$.

clearly, A is subcode of $\mathbb{F}_q^k$ and $\dim(A) = k$

$$\therefore\ A = \mathbb{F}_q^k$$

$$\therefore\ d(A) = 1$$

$\therefore\ A \square C$ is cyclic code with the parameters $[kN, k, N]$ over $\mathbb{F}_q$.

V. Generator Matrix For The Constructed Cyclic Code

In this section, we will give the generator polynomials for constructed cyclic code and it's dual by using generator polynomial of inner code A.

Theorem 5.1. Let $C = \{(\alpha, \alpha, \dots, \alpha) : \alpha \in \mathbb{F}_{q^k}\}$ be a linear code with the parameters $[N, 1, N]$ over $\mathbb{F}_{q^k}$ and $A = im(\pi) = \pi(\mathbb{F}_{q^k})$ be a cyclic code with the parameters $[n, k, d(A)]$ over $\mathbb{F}_q$. Then the $G(x) = (1 + x^n + x^{2n} + \cdots + +x^{(N-1)n})g(x)$ is generator polynomial of $A \square C$ if $g(x)$ is generator polynomial of A.

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

$\therefore\ A \square C$ is cyclic code with the parameters $[kN, k, N]$ over $\mathbb{F}_q$.

To find generator polynomial of $A \square C$:

Consider $\pi: F_q^n \to \frac{F_q[x]}{<x^n-1>}$ and $\pi': F_q^{Nn} \to \frac{F_q[x]}{<x^{Nn}-1>}$ defined as $\pi\big((c_1, c_2, \dots, c_n)\big) = c_1 + c_2x + \cdots + c_nx^{n-1}$ and $\pi'\Big(\big((c_1, c_2, \dots, c_n, c_{n+1}, \dots, c_{2n,}, \dots, c_{(N-1)n+1}, \dots, c_{Nn}\big)\Big) = c_1 + c_2x + \cdots \dots + c_nx^{n-1} + c_{n+1}x^n + \cdots . + c_{2n}x^{2n-1} + \cdots + c_{((N-1)n+1)}x^{(N-1)n} + \cdots . c_{Nn}x^{Nn-1}$ respectively.

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

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

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

$\therefore \pi'\Big(\big((c_1, c_2, \dots, c_n, c_{n+1}, \dots, c_{2n,}, \dots, c_{(N-1)n+1}, \dots, c_{Nn}\big)\Big) = c_1 + c_2x + \cdots \dots + c_nx^{n-1} + c_{n+1}x^n + \cdots . + c_{2n}x^{2n-1} + \cdots + c_{((N-1)n+1)}x^{(N-1)n} + \cdots . c_{Nn}x^{Nn-1}$

$\therefore = c_1 + c_2x + \cdots + c_nx^{n-1} + c_1x^n + c_2x^{(n+1)} + \cdots + c_nx^{2n-1} + \cdots + c_1x^{((N-1)n} + c_2x^{(N-1)n+1} + \cdots + c_nx^{Nn-1}$

$\therefore = (c_1 + c_2x + \cdots + c_nx^{n-1}) + (c_1 + c_2x + \cdots + c_nx^{n-1})x^n + \cdots + (c_1 + c_2x + \dots + c_nx^{n-1})x^{((N-1)n}$

$\therefore = \big(1 + x^n + x^{2n} + \cdots + x^{(Nn-1)}\big)(c_1 + c_2x + \cdots + c_nx^{n-1})$

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

$\therefore \big(1 + x^n + x^{2n} + \cdots + x^{(Nn-1)}\big)g(x)$ is monic least degree polynomial such that $\pi'(A \square C) =< \big(1 + x^n + x^{2n} + \cdots + x^{(Nn-1)}\big)g(x) >$

$\therefore \big(1 + x^n + x^{2n} + \cdots + x^{(Nn-1)}\big)g(x)$ is generator polynomial of $A \square C$.

VI. Some Results

Theorem 6.1. Let $C = \{(\alpha, \alpha, \dots, \alpha): \alpha \in \mathbb{F}_{q^k}\}$ be a linear code with the parameters $[N, 1, N]$ over $\mathbb{F}_{q^k}$ and $A = im(\pi) = \pi(\mathbb{F}_{q^k})$ be a linear code with the parameters $[n, k, d(A)]$ over $\mathbb{F}_q$. Then $N \mid wt(c)$ if $c \in A \square C$.

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

Consider $c \in A \square C$

$$\therefore \exists \alpha \in \mathbb{F}_{q^k} \text{ such that } c = (\pi(\alpha), \dots, \pi(\alpha))$$

By using definition,

$$wt(c) = wt((\pi(\alpha), \dots, \pi(\alpha)))$$
$$\therefore wt(c) = N \times wt(\pi(\alpha))$$
$$\therefore N \mid wt(c)$$

By using above theorem 6.1, clearly, we can conclude, weight distribution of A gives weight distribution of constructed cyclic code.

Theorem 6.2. Let $C = \{(\alpha, \alpha, \dots, \alpha): \alpha \in \mathbb{F}_{q^k}\}$ be a linear code with the parameters $[N, 1, N]$ over $\mathbb{F}_{q^k}$ and $A = im(\pi) = \pi(\mathbb{F}_{q^k})$ be a cyclic code with the parameters $[n, k, d(A)]$ over $\mathbb{F}_q$. Then $A \square C$ is LCD cyclic code if A is reversible code and $\gcd(Nn, q) = 1$. Proof. Let $C = \{(\alpha, \alpha, \dots, \alpha): \alpha \in \mathbb{F}_{q^k}\}$ be a linear code with the parameters $[N, 1, N]$ over $\mathbb{F}_{q^k}$ and $A = im(\pi) = \pi(\mathbb{F}_{q^k})$ be a cyclic code with the parameters $[n, k, d(A)]$ over $\mathbb{F}_q$.

$$\therefore A \square C \text{ is cyclic code with parameters } [Nn, k, d(A)N]$$

Now, Consider A is reversible code and $\gcd(Nn, q) = 1$.

To show $A \square C$ is reversible code :

Consider $(\underbrace{c_1, c_2, \dots, c_n}_{1}, \underbrace{c_{n+1}, \dots, c_{2n}}_{2}, \dots, \underbrace{c_{(N-1)n+1}, \dots, c_{Nn}}_{N}) \in A \square C$

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

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

We know A is reversible code,so we get

$$(c_n, c_{n-1}, \dots, c_1) \in A$$

$$\therefore \exists \beta \in \mathbb{F}_{q^k} \text{ such that } \pi(\beta) = (c_n, c_{n-1}, \dots, c_1)$$

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

$$\therefore (\underbrace{c_{Nn}, c_{Nn-1}, \dots, c_{(N-1)n+1}}_{1}, \underbrace{c_{(N-1)n}, c_{(N-1)n-1}, \dots, c_{(N-2)n+1}}_{2}, \dots, \underbrace{c_n, c_{n-1}, \dots, c_1}_{N}) \in A \square C$$

$$\therefore A \square C \text{ is reversible code with parameters } [nN, k, d(A)N] \text{ over } \mathbb{F}_q \quad \dots\dots\dots(2)$$

By using Theorem,

$\therefore A \square C$ is LCD cyclic code with parameters $[nN, k, d(A)N]$ over $\mathbb{F}_q$.

VII. Conclusion

In the fourth section of our research article, we have presented the construction of a class of cyclic codes with improved parameters, utilizing concatenated codes. Moving forward to the fifth section, we have provided the generator matrix for the constructed cyclic code. Finally, in the last section, we have presented some results about constructed cyclic code.

References

[1] B. Chen, S.-T. Xia, J. Hao, and F.-W. Fu. Constructions of optimal cyclic ({r},{\ delta }) locally repairable codes. IEEE Transactions on Information Theory, 64(4):2499-2511, 2017.

[2] C. Ding. Cyclotomic constructions of cyclic codes with length being the product of two primes. IEEE transactions on information theory, 58(4):2231-2236, 2011.

[3] G. D. Forney. Concatenated codes. 1965.

[4] E. Prange. Some cyclic error-correcting codes with simple decoding algorithms. AFCRC-TN-58-156, 1985.

[5] J. Qian and L. Zhang. New optimal cyclic locally recoverable codes of length $n = 2(q + 1)$. IEEE Transactions on Information Theory, 66(1):233-239, 2019.

[6] C. Rong and T. Helleseth. Use characteristic sets to decode cyclic codes up to actual minimum distance. London Mathematical Society Lecture Note Series, pages 297-312, 1996.

[7] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Constructions of mds-convolutional codes. IEEE Transactions on Information Theory, 47(5):2045-2049, 2001.

[8] I. Tamo, A. Barg, S. Goparaju, and R. Calderbank. Cyclic lrc codes, binary lrc codes, and upper bounds on the distance of cyclic codes. International Journal of Information and Coding Theory, 3(4):345-364, 2016.

[9] M. Xiong. On cyclic codes of composite length and the minimum distance. IEEE Transactions on Information Theory, 64(9):6305-6314, 2018.

[10] M. Xiong and A. Zhang. On cyclic codes of composite length and the minimum distance ii. IEEE Transactions on Information Theory, 67(8):50975103, 2021.

[11] X. Yang and J. L. Massey. The condition for a cyclic code to have a complementary dual. Discrete Mathematics, 126(1-3):391-393, 1994.