IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Construction Of Class Of Cyclic Codes Of Composite Length By Using Concatenation Of Linear Code

Anju Sharma[1], Vinod Kumar[1], Amit Tuteja[1] and Rupa Rani Sharma[2]

[1]Department of Mathematics, Guru Kashi University, Bathinda, Punjab.
[2]Department of Applied Sciences, G.L. Bajaj Institute of Technology and Management, Greater Noida, India.

Abstract

A cyclic code is a block code, where the circular shifts of each codeword give another word that belongs to the code. They are error-correcting codes that have algebraic properties that are convenient for efficient error detection and correction. This means that the construction of cyclic code is important. In this paper, we propose a new construction of a class of cyclic codes with good parameters by using a concatenation of linear codes over a finite field. After construction, the generator polynomial for the constructed cyclic code is given and proves some related results.

Keywords: Cyclic code, Construction of cyclic code, Concatenation of linear codes.

1 Introduction

CYCLIC codes are an interesting class of linear codes. The error-correcting capability of cyclic codes may not be as good as linear codes in general. However, cyclic codes have wide applications in storage and communication systems because they have efficient encoding and decoding algorithms (Prange et al. 1985). Famous families of cyclic codes include BCH codes, the Golay codes, the binary hamming codes, and quadratic residue codes, just to name a few. While cyclic codes have been studied for a long time, it remains an interesting question to construct cyclic codes with good parameters and good properties as they have found many new applications, for example, in the construction of locally recoverable codes (Chen, Bin, et al. 2017) and of convolutional codes (Smarandache et al. 2001).

Let F_q be a finite field of order q. Let n, r be two distinct odd primes such that $gcd(nr, q) = 1$ and q is a quadratic residue for both n and r. In an interesting paper (Ding, Cunsheng 2011), Ding provided three constructions of cyclic codes of length nr and dimension $\frac{nr+1}{2}$ over F_q by using quadratic residue codes of length n and r respectively. In papers (Maosheng et al. 2018,2021), Maosheng et al. provided general theory about cyclic codes of composite length nr and partially explained why the cyclic codes from Ding's construction all have relatively large minimum distance. They also provided a general construction of cyclic code of length nr and dimension $\frac{(n+1)r}{2}$ based on quadratic residue codes of length n.

In this paper, firstly we introduce repetition code of linear code C with index l by using concatenation of linear code. Using repetition code of cyclic code C with index l, the construction of class of cyclic code having composite length nl whose minimum distance is greater than minimum distance of old cyclic code C is given. In section 3, a generator polynomial has given for constructed cyclic code by using generator polynomial of old cyclic code. At last in section 5, some results are proposed which are related to constructed cyclic code that will help to detect errors.

2 Preliminaries

In this short section, collection of several basic facts about cyclic code are revised which will be used throughout the paper. Interested readers may refer to (Ling and Xing 2004) for more details. Throughout the text , F_q denotes the finite field with q elements, where q is a prime power. F_q^n denotes the n-dimensional vector space over F_q. Subspace of F_q^n is called linear code of length n over F_q. $k = log_q(|C|)$ is called dimension of linear code C over F_q.

Definition 2.1:Let C be linear code with length n and $x, y \in C$ (i.e. $x = (x_1, x_2, \dots x_n)$ and $y = (y_1, y_2 \dots y_n)$). then d (x,y) is called hamming distance from x to y if

$d(x,y) = d(x_1,y_1) + d(x_2,y_2) + \dots + d(x_n,y_n)$.

where , $d(x_i,y_i) = 1$ if $x_i \neq y_i$

$d(x_i,y_i) = 0$ if $x_i = y_i$

Definition 2.2: Let C be code with cardinality greater than 2 then minimum distance of C is equal to $\min\{d(x,y): x, y \in C, x \neq y\}$.

It is denoted by $d(C)$ or as simply d.

i.e. $d(C) = \min\{d(x,y): x, y \in C, x \neq y\}$.

Definition 2.3: If Linear code C having length n, dimension k, minimum distance d then linear code C is called [n, k, d]-linear code.

Definition 2.4: If C is any linear code of length n over F_q then

$C^{\perp} = \{ (v_1, v_2, \dots v_n) \in F_q^n : \langle (v_1, v_2, \dots v_n), (x_1, x_2, \dots x_n) \rangle = 0$, for all $(x_1, x_2, \dots x_n) \in C \}$ is called dual code of C.

Definition 2.5: A subset S of F_q^n is cyclic if $(a_{n-1}, a_0, a_1, \dots, a_{n-2}) \in S$ whenever $(a_0, a_1, \dots, a_{n-1}) \in S$. A linear code C is called a cyclic code if C is a cyclic set.

The word $(u_{n-r}, \dots, u_{n-1}, u_0, \dots, u_{n-r-1})$ is said to be obtained from the word $(u_0, \dots, u_{n-1}) \in F_q^n$ by cyclically shifting r positions.

It is easy to verify that the dual code of a cyclic code is also a cyclic code.

In order to convert the combinatorial structure of cyclic codes into an algebraic one , consider the following correspondence :

$\pi : F_q^n \to \frac{F_q[x]}{\langle x^n - 1 \rangle}, \ (a_0, a_1, \dots, a_{n-1}) \mapsto a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$.

Then π is an F_q linear transformation of vector spaces over F_q. From now on , sometimes it is identied F_q^n with $\frac{F_q[x]}{\langle x^n - 1 \rangle}$, and a vector $u = (u_0, \dots, u_{n-1})$ with the polynomial $u(x) = \sum_{i=0}^{n-1} u_i x^i$, it is known that $\frac{F_q[x]}{\langle x^n - 1 \rangle}$ is a ring (but not a field unless $n = 1$). Thus, it has a multiplicative operation besides the addition in F_q^n.

Following theorem show relation between cyclic code of F_q^n and ideal of $\frac{F_q\,[x]}{<x^n-1>}$.

Theorem 2.6: a nonempty subset C of F_q^n is a cyclic code iff $\pi(C)$ is an ideal of $\frac{F_q\,[x]}{<x^n-1>}$.

Example 2.7: The code C = {(0,0,0), (1,1,1), (2,2,2)} is a ternary cyclic code . The corresponding ideal in $\frac{F_q\,[x]}{<x^n-1>}$ is $\pi(C)$ = { 0,1 + x + x^2, 2 + 2x + $2x^2$}.

Theorem 2.8: Let I be a nonzero ideal in $\frac{F_q\,[x]}{<x^n-1>}$ and let $g(x)$ be a nonzero monic polynomial of the least degree in I. Then $g(x)$ is a generator of I and divides $x^n - 1$.

Definition 2.9: The unique monic polynomial of the least degree of a nonzero ideal I of $\frac{F_q\,[x]}{<x^n-1>}$ is called the generator polynomial of I. For a cyclic code C, the generator polynomial of $\pi(C)$ is also called the generator polynomial of C.

Theorem 2.10: There is a one-to-one correspondence between the cyclic codes C in F_q^n and the monic divisors of $x^n - 1 \in F_q[x]$.

3 Construction Of Cyclic Code

Here, we introduce repetition code of linear code C with index l by concatenating linear code . In addition the construction of class of cyclic code having composite length nl and dimension k (dimension of old cyclic code C) is given by usage of repetition code of linear code C with index l.

Let C be any linear code with parameters $[n, k, d\ ]$ over F_q. Then set $\{\ (\mathrm{u}, \mathrm{u}, \ldots, \mathrm{u}) : \mathrm{u} \in \mathrm{C}\ \} \subseteq F_q^{nl}$ is called repetition code of C with index l and it is denoted by $RC[C, l]$.

Theorem 3.1: Let C be any $[n, k, d]$ – linear code over F_q. Then $RC\ [C, l]$ is $[\ ln\ , k\ , ld\ ] -$ linear code over F_q.

Proof :- Let C be any $[n, k, d] -$ linear code over F_q

And $RC[C, l] = \{\ (\mathrm{u}, \mathrm{u}, \ldots, \mathrm{u}) : \mathrm{u} \in \mathrm{C}\ \} \subseteq F_q^{nl}$

To show $RC[C, l]$ is linear code :-

Consider $x, y \in RC[C, l]$ and $\alpha, \beta \in F_q$

$\therefore \exists\ \mathrm{u}, \mathrm{v} \in \mathrm{C}$ such that $x = (u, u, \ldots, u)$ and $y = (v, v, \ldots\ldots, v)$

$\therefore\ \alpha x + \beta y = \alpha\ (u, u, \ldots, u) + \beta\ (v, v, \ldots., v)$

$\therefore = (\alpha u, \alpha u, \ldots\ldots, \alpha u) + (\ \beta v, \beta v, \ldots \beta v)$

$\therefore = (\ \alpha u + \beta v, \alpha u + \beta v\ , \ldots, \alpha u + \beta v\ )$

$\therefore\ \alpha x + \beta y \in RC[C, l]$ .... $(\because\ \alpha u + \beta v \in C\ )$.

$\therefore\ RC\ [C, l]$ is linear code.

To find parameters:-

Clearly, length of $RC[C, l] = ln$

Dimension of $RC[C, l] = log_q\ (|RC[C, l]|) = log_q(|C|) = k$

Minimum distance of $RC[C, l] = d\ (\ RC\ [C, l])$

$\therefore\ = \min \{\ d\ (x, y) : x, y \in RC[C, l]\ , x \neq y\ \}$

$\therefore\ = \min \{\ d\ (\ (u, u, \ldots . u), (v, v, \ldots v)\ ) : u, v \in C\ , u \neq v\ \}$

$\therefore\ = \min \{\ l \times d\ (u, v) : u, v \in C\ , u \neq v\}$

$\therefore\ = l \times \min \{d\ (u, v) : u, v \in C\ , u \neq v\}$

$$\therefore\quad d(\ RC\ [C, l]\ ) = ld$$

$\therefore\ RC[C, l]$ is $[\ ln\ , k\ , ld\ ] -$ linear code over F_q.

Corollary 3.2: If $C = F_q^n$ then $RC[C,l]$ is $[ln,n,l]$ – linear code over F_q.
Proof : Let $C = F_q^n$
$\therefore$ dim(C) = dim (F_q^n) = n and $d(C) = d(F_q^n) = 1$.
By using Theorem 3.1,
$RC[C,l]$ is $[ln,n,l]$– linear code over F_q.

Following result gives the construction of class of cyclic code.

Theorem 3.3: If C is $[n,k,d]$ – cyclic code over F_q then $RC[C,l]$ is $[nl,k,ld]$ – cyclic code over F_q.
Proof : Let C be any $[n,k,d]$ − cyclic code over F_q.
$\therefore RC[C,l]$ is $[ln,k,ld]$ − linear code over F_q.
To show $RC[C,l]$ is cyclic code :-
Consider $(c_1,c_2,\dots,c_n,c_{n+1},\dots,c_{2n},\dots\dots,c_{(l-1)n+1},\dots.c_{ln}) \in RC[C,l]$
$\therefore \exists u \in C$ such that

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

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

Now, given that C is cyclic code

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

$$\therefore (c_n,c_1,\dots,c_{n-1},c_n,c_1,\dots\dots,c_{n-1},\dots.,c_n,c_1,\dots.,c_{n-1}) \in RC[C,l]$$

$$\therefore (c_{ln},c_1,\dots,c_{n-1},c_n,c_{n+1},\dots.,c_{2n-1},\dots.,c_{(l-1)n},c_{(l-1)n+1},\dots,c_{ln-1}) \in RC[C,l]$$

$\therefore RC[C,l]$ is $[nl,k,ld]$ – cyclic code over F_q.

4 Generator Polynomial for Constructed Cyclic Code And Its Dual

In theorem 3.3, we have seen $RC[C,l]$ is cyclic code if linear code C is cyclic code. Every cyclic code has generator polynomial so the generator polynomial for constructed $RC[C,l]$ cyclic code can be found. In following theorem 4.1, generator polynomial for $RC[C,l]$ cyclic code is provided by the use of generator polynomial of cyclic code C.

Theorem 4.1 : If $g(x)$ is generator polynomial of cyclic code C then
$(1 + x^n + x^{2n} + \cdots.. + x^{ln})\, g(x)$ is generator polynomial of $RC[C,l]$.
Proof : Let C be any $[n,k,d]$ −cyclic code over F_q and $g(x)$ be generator polynomial of C. $\therefore$
$RC[C,l]$ is $[n,k,d]$ − cyclic code over F_q.
To find generator polynomial of $[C,l]$:
Consider $\pi : F_q^n \to \frac{F_q[x]}{<x^n-1>}$ and $\pi' : F_q^{ln} \to \frac{F_q[x]}{<x^{ln}-1>}$ defined
as $\pi((c_1, c_2, \dots., c_n)) = c_1 + c_2x + \dots. + c_nx^{n-1}$
and $\pi'((c_1, c_2, \dots., c_n, c_{n+1}, \dots, c_{2n}, \dots., c_{(l-1)n+1}, \dots, c_{ln})) = c_1 + c_2x + \dots. + c_nx^{n-1} + c_{n+1}x^n + \dots\dots + c_{2n}x^{2n-1} + \dots.. + c_{(l-1)n+1}x^{(l-1)n} + \dots. + c_{ln}x^{ln-1}$ respectively.

Consider $(c_1, c_2, \dots., c_n, c_{n+1}, \dots, c_{2n}, \dots., c_{(l-1)n+1}, \dots, c_{ln}) \in RC[C,l]$.

$\therefore \exists$ u $\in C$ such that u = $(c_1 , c_2 ,\ldots,c_n) = (c_{n+1},\ldots,c_{2n}) =\ldots= (c_{(l-1)n+1},\ldots,c_{ln})\therefore c_1 = c_{n+1} =\ldots= c_{(l-1)n+1}, c_2 = c_{n+2}=\ldots= c_{(l-1)n+2} ,\ldots, c_n = c_{2n} =\ldots= c_{ln}$

$\therefore \pi'((c_1 , c_2 , \ldots , c_n ,c_{n+1},\ldots,c_{2n},\ldots,c_{(l-1)n+1},\ldots,c_{ln})) = c_1 + c_2x +\ldots+c_nx^{n-1} + c_{n+1}x^n +\ldots+c_{2n}x^{2n-1}+\ldots+ c_{(l-1)n+1}x^{(l-1)n}+\ldots+c_{ln}x^{ln-1}$

$\therefore= c_1 + c_2x +\ldots+c_nx^{n-1} + c_1x^n +\ldots+c_nx^{2n-1}+\ldots+ c_1x^{(l-1)n}+\ldots+c_nx^{ln-1}$

$\therefore= (c_1 + c_2x +\ldots+c_nx^{n-1}) + (c_1 + c_2x +\ldots+c_nx^{n-1})\, x^n +\ldots + (c_1 + c_2x +\ldots+c_nx^{n-1})\, x^{ln}$

By using theorems (2.6) and (2.10),

$\pi'((c_1 , c_2 , \ldots , c_n ,c_{n+1},\ldots,c_{2n},\ldots,c_{(l-1)n+1},\ldots,c_{ln})) = f(x)g(x) + f(x)g(x)x^n + \cdots. + f(x)g(x)x^{ln}$

$$\therefore = (1 + x^n + \ldots + x^{ln})g(x)$$

Clearly, $(1 + x^n + \ldots+ x^{ln})$ g(x) is monic least degree polynomial such that

$\pi' (RC[C,l]) = <(1 + x^n + \ldots+ x^{ln})\, g(x) >$

$\therefore (1 + x^n + \ldots + x^{ln})\, g(x)$ is generator polynomial of cyclic code $RC[C,l]$.

5 Some Related Results

In this section, we give some related results for improvement of our knowledge about repetition code of linear code C with index l.

Theorem 5.1: If $x \in RC[C,l]$ then $l \mid wt(x)$

Proof : Let C be any $[n,k,d]$ – linear code over F_q and $RC[C,l]=\{(u,u,\ldots,u): u \in C \} \subseteq F_q^{ln}$.

$\therefore RC[C,l]$ is $[nl,k,ld]$ – linear code over F_q.

Now, consider $x \in RC[C,l]$

$\therefore u \in C$ such that $x = (u,u,.\ldots,u)$

$\therefore wt(x) = wt((u,u,\ldots u))$

$\therefore wt(x) = d((u,u,\ldots,u),0)$

$\therefore wt(x) = l \times d(u,0)$

$\therefore l \mid wt(x)$

Above theorem shows $RC[C,l]$ has more capacity to detect error than usual linear code.

A reversible code(Massey, James L 1964) is a code such that reversing the order of the components of a codeword gives always a codeword. Following result shows repetition code of C with index l is reversible code if C is reversible code.

Theorem 5.2: If C is $[n,k,d]$ reversible code then $RC[C,l]$ is $[nl,k,ld]$ – reversible code.

Proof : Let C be any $[n,k,d]$ –reversible code over F_q and

$RC[C,l]=\{(u,u,\ldots,u): u \in C \} \subseteq F_q^{ln}$.

$\therefore RC[C.l]$ is $[nl,k,ld]$-linear code over F_q.

To show $RC[C,l]$ is reversible code:

Consider $(c_1, c_2, \ldots, c_n, c_{n+1}, \ldots, c_{2n}, \ldots, c_{(l-1)n+1}, \ldots. c_{ln}) \in RC[C,l]$

$\therefore \exists u \in C$ such that

$$\therefore u = (c_1, c_2, \ldots, c_n) = (c_{n+1}, \ldots, c_{2n}) = \cdots = (c_{(l-1)n+1}, \ldots, c_{ln})$$

$$\therefore c_1 = c_{n+1} = \cdots = c_{(l-1)n+1}, \quad c_2 = c_{n+2} = \cdots = c_{(l-1)n+2}, \ldots, c_n = c_{2n} = \cdots = c_{ln}$$

Now, given that C is reversible code

$$\therefore (c_n , c_{n-1} , \ldots, c_1) \in C$$

$$\therefore (c_n, c_{n-1}, \ldots, c_1, c_n, c_{n-1}, \ldots\ldots, c_1, \ldots., c_n, c_{n-1}, \ldots., c_1) \in RC[C,l]$$
$$\therefore (c_{ln}, c_{ln-1}, \ldots, c_{(l-1)n+1}, \ldots\ldots, c_{2n}, \ldots., c_{n+1}, c_n, c_{n-1}, \ldots, c_1) \in RC[C,l]$$

$\therefore RC[C,l]$ is $[nl, k, ld]$ – reversible code over F_q.

6 Conclusion

In this paper, we introduced repetition code of linear code C with index l by using concatenation of linear code and constructed the class of cyclic code of composite length with improved parameters by usage of $[C,l]$. In section 4, a generator polynomial for constructed class of cyclic code was provided. At last, some related results are proved.

Open Question: In paper (Massey et al. 1994), Massey et al. gave result about relation between cyclic code, reversible code and linear code with complementary dual (an LCD code), so we can ask question “If C is LCD code then is $RC[C,l]$ LCD code?”

References

[1] Forney, George. "On decoding BCH codes." *IEEE Transactions on information theory* 11.4 (1965): 549-557.
[2] Prange, Eugene. "Some cyclic error-correcting codes with simple decoding algorithms." AFCRC-TN-58-156 (1985).
[3] Rong, Chunming, and Tor Helleseth. "Use characteristic sets to decode cyclic codes up to actual minimum distance." London Mathematical Society Lecture Note Series (1996): 297-312.
[4] Chen, Bin, et al. "Constructions of optimal cyclic (r, delta) locally repairable codes." IEEE Transactions on Information Theory 64.4 (2017): 2499-2511.
[5] Tamo, Itzhak, et al. "Cyclic LRC codes, binary LRC codes, and upper bounds on the distance of cyclic codes." arXiv preprint arXiv:1603.08878 (2016).
[6] Qian, Jianfa, and Lina Zhang. "New Optimal Cyclic Locally Recoverable Codes of Length n= 2 (q+1). " IEEE Transactions on Information Theory 66.1 (2019): 233-239.
[7] Smarandache, Roxana, Heide Gluesing-Luerssen, and Joachim Rosenthal. "Constructions of MDS-convolutional codes." IEEE Transactions on Information Theory 47.5 (2001): 2045-2049.
[8] Ding, Cunsheng. "Cyclotomic constructions of cyclic codes with length being the product of two primes." IEEE transactions on information theory 58.4 (2011): 2231-2236.
[9] Huffman, W. Cary, and Vera Pless. Fundamentals of error-correcting codes. Cambridge university press, 2010.
[10] Yang, Xiang, and James L. Massey. "The condition for a cyclic code to have a complementary dual." Discrete Mathematics 126.1-3 (1994): 391-393.
[11] Xiong, Maosheng. "On cyclic codes of composite length and the minimum distance." IEEE Transactions on Information Theory 64.9 (2018): 6305-6314.
[12] Xiong, Maosheng, and Aixian Zhang. "On cyclic codes of composite length and the minimum distance II." IEEE Transactions on Information Theory 67.8 (2021): 5097-5103.
[13] Ling, San, and Chaoping Xing. Coding theory: a first course. Cambridge University Press, 2004.
[14] Massey, James L. "Reversible codes." Information and Control 7.3 (1964): 369-380.
[15] Singla, A., Kumar, V., & Sharma, R. R. (2023). Numerical Study on the Impact of COVID–19 to Insurance Sector. Mathematical Statistician and Engineering Applications, 72(1), 252-264.