

Exponent of cyclic codes over $\mathbb{F}_q$

N. Annamalai *

Department of Computational Science and Humanities

Indian Institute of Information Technology Kottayam

Pala 686635

Kerala

India

C. Durairajan [†]

Department of Mathematics

School of Mathematical Sciences

Bharathidasan University

Tiruchirappalli 620024

Tamil Nadu

India

Abstract

In this paper, we introduce the exponent of a cyclic code over the finite field $\mathbb{F}_q$ with $q = p^m$ elements. Also, we prove that the exponent of the dual of cyclic code satisfies the condition $n = \text{lcm}(e, r)$ where n is the length of the cyclic code, $e = \exp(C)$ and $r = \exp(C^\perp)$.

Subject Classification: (2010) 94B05, 94B15, 94B25.

Keywords: Order of the polynomial, Cyclic codes, Exponent, Dual code.

1. Introduction

Cyclic codes are a class of important linear codes and have generated great interest in coding theory. In general, they have natural encoding and decoding algorithm. Since cyclic codes can be described as ideals in polynomials residue rings, they have a rich algebraic structure. There is a

*E-mail: algebra.annamalai@gmail.com (Corresponding Author)

†E-mail: cdurai66@rediffmail.com

lot of literature on cyclic codes over fields and more recently over rings. In [3], [4] and [2], authors are discussed cyclic codes from generalized cyclotomic classes of different orders and obtained lower bounds of the minimum distance of these cyclic codes.

Cyclic codes have a unique property that is the codewords of cyclic code can be divided into a numbers of mutually disjoint equivalence classes according to an equivalence relation.

In this paper, we introduce the concept exponent of a cyclic codes over a finite field $\mathbb{F}_q$ with q elements.

2. Preliminaries

The ring $R = \frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$ is a polynomial residue ring. The cyclic code over $\mathbb{F}_q$ of length n can be described as an ideal of $\frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$. A code of length n over $\mathbb{F}_q$ is a nonempty subset of $\mathbb{F}_q^n$, and a code is linear over $\mathbb{F}_q$ if it is a subspace. For an n -tuple $c = (c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_q^n$, the polynomial $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$ is called its codeword polynomial. A linear code C of length n over $\mathbb{F}_q$ is cyclic if it is invariant under the automorphism σ which is given by

$$\sigma(c_0, c_1, \dots, c_{n-1}) = (c_{n-1}, c_0, \dots, c_{n-2}).$$

We call σ a cyclic permutation.

Since R is a principal ideal ring, if C is not trivial there exists a unique monic polynomial $g(x)$ that generates C . We call $g(x)$ the generator polynomial of C . Note that $g(x)$ divides $x^n - 1$ in $\mathbb{F}_q[x]$. If the dimension of the code C is k , the generator polynomial has degree $n - k$.

Since the generator polynomial is a divisor of $x^n - 1$ and is unique, the parity-check polynomial of C is well defined as the polynomial $h(x)$ in R such that $h(x) = (x^n - 1) / g(x)$.

Theorem 2.1 : Let $h(x), g(x)$ be, respectively, the parity-check and the generator polynomial of the cyclic code C . The dual code $C^\perp$ is cyclic with generator polynomial $g^\perp(x) = x^{\deg(h(x))} h(x^{-1})$.

Definition 2.2 : Let $f(x) \in \mathbb{F}_q[x]$ be a nonzero polynomial. If $f(0) \neq 0$, then the least positive integer e for which $f(x)$ divides $x^e - 1$ is called the period of $f(x)$ or order of $f(x)$ and denoted by $\text{ord}(f) = \text{ord}(f(x))$. If $f(0) = 0$, then $f(x) = x^h g(x)$, where $h \in \mathbb{N}$ and $g(x) \in \mathbb{F}_q[x]$ with $g(0) \neq 0$ are uniquely determined, $\text{ord}(f)$ is then defined to be $\text{ord}(g)$.

Lemma 2.3 : Let r be a positive integer. Then the polynomial $f(x) \in \mathbb{F}_q[x]$ with $f(0) \neq 0$ divides $x^r - 1$ if and only if $\text{ord}(f)$ divides r .

Corollary 2.4 : If e_1 and e_2 are positive integers, then the greatest common divisor of $x^{e_1} - 1$ and $x^{e_2} - 1$ in $\mathbb{F}_q[x]$ is $x^d - 1$, where d is the greatest common divisor of e_1 and e_2 .

Definition 2.5 : Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x]$ with $a_n \neq 0$. Then the reciprocal polynomial f^* of f is defined by

$$f^*(x) = x^n f\left(\frac{1}{x}\right) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n.$$

Theorem 2.6 : Let f be a nonzero polynomial in $\mathbb{F}_q[x]$ and f^* its reciprocal polynomial. Then $\text{ord}(f) = \text{ord}(f^*)$.

Theorem 2.7 : Let $g_1, g_2, \dots, g_k$ be pairwise prime nonzero polynomials over $\mathbb{F}_q$ and let $f = g_1 g_2 \cdots g_k$. Then $\text{ord}(f) = \text{lcm}(g_1, g_2, \dots, g_k)$.

3. Exponent of a Cyclic Codes over $\mathbb{F}_q$

In this section, we define the exponent of a cyclic codes over $\mathbb{F}_q$ and discussed its properties.

Let C be a cyclic code of length n over $\mathbb{F}_q$. Then C can be viewed as an ideal in $\frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$. Since $\mathbb{F}_q[x]$ is a principle ideal domain, $C = \langle g(x) \rangle$, where $g(x) \mid x^n - 1$, $g(0) \neq 0$ and $g(x)$ is monic.

Definition 3.1 : Let C be a cyclic code of length n over $\mathbb{F}_q$ with generator polynomial $g(x)$. Then the least positive integer e for which $g(x)$ divides $x^e - 1$ is called the exponent of the cyclic code C and denoted by $e = \text{exp}(C)$.

Example 3.2 : Let $C = \{000, 101, 110, 011\}$ be a cyclic code of length 3 over $\mathbb{F}_2$. Then the generator polynomial of C is $1 + x$. Hence, $\text{exp}(C) = 1$.

Example 3.3 : Let $C = \{000, 111, 222\}$ be a cyclic code of length 3 over $\mathbb{F}_3$. Then the generator polynomial of C is $1 + x + x^2$. Since $1 + x + x^2$ divides $x^3 - 1$, then $\text{exp}(C) = 3$.

Theorem 3.4 : Let C be an $[n, k]_q$ cyclic code over $\mathbb{F}_q$. If $e = \text{exp}(C)$, then $e \mid n$. In particular, $e \leq n$.

Proof : Let C be an $[n, k]_q$ cyclic code over $\mathbb{F}_q$. Let $g(x)$ be its generator polynomial. Then $g(x) \mid x^n - 1$. If $e = \exp(C)$, then $g(x) \mid x^e - 1$. By theorem, $e \mid n$. This implies that, $e \leq n$. $\square$

Theorem 3.5 : Let C be an $[n, k]_q$ cyclic code over $\mathbb{F}_q$. If $e = \exp(C)$, then $n - k \leq e$.

Proof : Let C be an $[n, k]_q$ cyclic code over $\mathbb{F}_q$. Let $g(x)$ be its generator polynomial. Then $\deg(g(x)) = n - k$. If $e = \exp(C)$, then $g(x) \mid x^e - 1$. This implies that, $\deg(g(x)) \leq \deg(x^e - 1)$, i.e., $n - k \leq e$. $\square$

Corollary 3.6 : Let C be an $[n, k]_q$ cyclic code over $\mathbb{F}_q$. If $e = \exp(C)$, then $n - k \leq e \leq n$.

Let C be an $[n, k]_q$ cyclic code with generator polynomial $g(x)$ of degree $n - k$. Then the dual code $C^\perp$ is an $[n, n - k]$ cyclic code with generator polynomial $h^*(x) = x^{\deg(h(x))} h(x^{-1})$ of degree k where $h(x) = \frac{x^n - 1}{g(x)}$.

Theorem 3.7 : Let C be an $[n, k]$ cyclic code over $\mathbb{F}_q$ and $C^\perp$ be its dual cyclic code. If $\exp(C) = e$, then $n = \text{lcm}(e, r)$ where $r = \exp(C^\perp)$.

Proof : Let $g(x)$ be a generator polynomial and $h(x)$ be a parity check polynomial of C such that $x^n - 1 = g(x)h(x)$ and $\gcd(g(x), h(x)) = 1$. Since $\text{ord}(x^n - 1) = n$, then by theorem $n = \text{lcm}(e, r)$ where $r = \exp(C^\perp)$. $\square$

Example 3.8 : Let $C = \{000, 001, 100, 010, 101, 111, 110, 011\}$ be a cyclic code of length 4 over $\mathbb{F}_2$. Then the generator polynomial of C is $1 + x$. This implies that $\exp(C) = 1$. The dual code $C^\perp$ of C is $C^\perp = \{0000\}$. Hence $\exp(C^\perp) = 3$.

Theorem 3.9 : Let C_i be an $[n, k_i]_q$ cyclic code over $\mathbb{F}_q$ for $i = 1, 2$. If e_i is the exponent of C_i , then $\exp(C_1 \oplus C_2) = e = \gcd(e_1, e_2)$.

Proof : Let C_1, C_2 be a cyclic code of length n over $\mathbb{F}_q$. Then $C_1 \oplus C_2 = \{c_1 + c_2 \mid c_i \in C_i, i = 1, 2\}$ is also a cyclic code of length n over $\mathbb{F}_q$. Let $g_1(x), g_2(x), g(x)$ be the generator polynomial of C_1, C_2 and $C_1 \oplus C_2$, respectively. If $\exp(C_1 \oplus C_2) = e$, then $g(x) \mid x^e - 1$. Since $C_i = \langle g_i(x) \rangle$, then $C_1 \oplus C_2 = \langle \gcd(g_1(x), g_2(x)) \rangle$. This implies that, $g(x) \mid g_i(x)$ for $i = 1, 2$. Then e divides e_i for $i = 1, 2$. Hence e divides $\gcd(e_1, e_2) = d$.

Suppose $e = dq + r$ where $0 \leq r < d$. Suppose $r \neq 0$, then

$$\begin{aligned}
x^e - 1 &= x^{dq+r} - 1 \\
&= x^{dq}x^r - x^r + x^r - 1 \\
&= x^r(x^{dq} - 1) + x^r - 1 \\
(x^e - 1) - x^r(x^{dq} - 1) &= x^r - 1.
\end{aligned}$$

Since $g(x)$ divides both $x^e - 1$ and $x^d - 1$, then $g(x)$ divides $x^r - 1$, which is a contradiction to e is the exponent of $C_1 \oplus C_2$. Therefore, $d \mid e$. Hence $e = d = \gcd(e_1, e_2)$. $\square$

We extend the above theorem for general case as following:

Theorem 3.10 : Let C_i be an $[n, k_i]$ cyclic code over $\mathbb{F}_q$ with generator polynomial $g_i(x)$ for $i = 1, 2, \dots, t$. If $\exp(C_i) = e_i$, then $\exp(C_1 \oplus C_2 \oplus \dots \oplus C_t) = \gcd(e_1, e_2, \dots, e_t)$.

Theorem 3.11 : Let C_i be an $[n, k_i]_q$ cyclic code over $\mathbb{F}_q$ for $i = 1, 2$. If e_i is the exponent of C_i , then $\exp(C_1 \cap C_2) = e = \text{lcm}(e_1, e_2)$.

Conclusion

In this paper, we studied the exponent of a cyclic code over the finite field $\mathbb{F}_q$ with $q = p^m$ elements. Also, we proved that the exponent of the dual of cyclic code is satisfies the condition $n = \text{lcm}(e, r)$ where n is the length of the cyclic code, $e = \exp(C)$ and $r = \exp(C^\perp)$.

Acknowledgment

The authors wish to thank the referees for many valuable comments.

References

- [1] David S. Dummit and Richard M. Foote, Abstract Algebra, Wiley; 3rd Edition, July 14, 2003.
- [2] Manju Pruthi and Sunil Kumar, Cyclic codes with generalized cyclotomic cubic classes, *Journal of Discrete Mathematical Sciences and Cryptography*, 22:6, 923-933(2019), DOI: 10.1080/09720529.2019.1627706.
- [3] Pankaj and Manju Pruthi, Cyclic codes from Whiteman's generalized cyclotomic sequences of order $2r, r \geq 2$, *Journal of Information and Optimization Sciences*, 38:3-4, 621-646(2017), DOI: 10.1080/02522667.2017.1303948.

- [4] Pankaj and Manju Pruthi, Cyclic codes of prime power length from generalized cyclotomic classes of order $2r$, *Journal of Information and Optimization Sciences*, 39:4, 965-971(2018), DOI: 10.1080/02522667.2018.1460136.
- [5] Rudolf Lidl and Harald Niederreiter, Introduction to finite fields and their applications, Cambridge University press, Cambridge, 1986.
- [6] Vera Pless, Introduction to the Theory of Error-Correcting Codes, John Wiley & Sons, Inc, 1998.

Received September, 2020

Revised January, 2021