ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Role of Zero Divisors on Cyclic Codes

V. Gayathri*, V. K. Radhakrishnan
Dept. of Mathematics, SCSVMV University, Enathur, Kanchipuram, TN, India
***Corresponding author: E-Mail: gay3.kanna@gmail.com**

ABSTRACT

In this paper, we deal with cyclic codes and we see how the non-trivial cyclic codes are generated by the zero divisors of the commutative ring GF (2)[x]/(x^n-1), the set of all polynomial of degree less than n (where n ≥ 1) in the variable x with coefficients from the binary field GF(2) under the binary operation polynomial addition and multiplication modulo x^n-1.

KEY WORDS: coding theory, binary codes, cyclic codes, rings, zero divisors**.**

1. INTRODUCTION

Coding theory is the study of error-control codes. Error control codes are used to detect errors and if possible, correct errors when transmitted through noisy channel.

The process begins with a message '*m*' to be sent from the source. The message is encoded into a code word '***c***' using an encoding technique. The code word '***c***' is transmitted through a channel which is subjected to noise in the form of atmospheric disturbances or hardware malfunctions. So the transmitted code word may get distorted. Coding theory is the study of codes which deals with developing ways to combat errors that may occur during transmission.

It can be achieved through cyclic codes with its rich algebraic structure because they are easy to construct and facilitates quick encoding and decoding techniques. A cyclic code, in particular, is an error control code which is used for error detection and error correction.

2. PRELIMINARIES

In this paper, we concentrate more on binary codes. In binary codes, the message '*m*' is encoded into a code word '***c***' which is a string of binary symbols {0, 1}. The collection of code words is said to be a code '*C*'. *GF*(2) = {0,1} is a finite field under the operation addition modulo the operation addition modulo 2.

$$0+0=0;\ 1+1=0;\ 0+1=1;\ 0+1=0$$

Linear Codes: A binary linear code C of length n is a set of binary n-tuples such that the component wise modulo 2 sum of any two codewords is contained in C.

For example, {0000, 0101, 1010, 1111} is a binary linear code.

Ring: Let *R* be a nonempty set and two binary operations denoted (+) and (*) are defined on *R*. Then *R* is said to be a ring, if

i. *R* is closed under addition and multiplication. i.e., for any $a,b \in R,\ a+b \in R$ and $ab \in R$

ii. Both addition and multiplication is associative. i.e., for any $a,b,c \in R$

$(a + b) + c = a + (b + c)$, $(ab)c = a(bc)$

iii. There exist an additive identity 0 in *R* such that

$a + 0 = 0 + a = a$, for any element $a \in R$.

iv. There exist an additive inverse $-a$ for each element $a \in R$ such that, $a + (-a) = 0 = (-a) + a$.

v. The addition is commutative. ie., $a + b = b + a$, for all $a,b \in R$.

vi. The addition and multiplication operation distribute: For any $a,b,c \in R$

$$a*(b+c)=(a*b)+(a*c)$$
$$(b+c)*a=(b*a)+(c*a)$$

Ideal: A nonempty set *A* of a ring *R* is an ideal of *R* if

i. $a-b \in A$ whenever $a,b \in A$.

ii. $ar, ra \in A$ whenever $a \in A$ and $r \in R$.

Zero Divisors of a Ring: A non-zero element $a \in R$ is a zero divisor of a ring *R* if there exist a non-zero element $b \in R$ such that $ab = 0$.

Cyclic Codes: A linear code *C* is a cyclic code if, whenever $(c_0,c_1,c_2,\ldots,c_{n-1},c_n) \in C \Rightarrow (c_n,c_1,c_2,\ldots,c_{n-1})$ is also a code word in *C*. ***Ex***: *C* = **{**00, 01, 10, 11} is a Cyclic code.

Cyclic code word ***c*** = $(c_0,c_1,c_2,\ldots,c_{n-1},c_n)$ of length *n* can be easily converted into code polynomials $c(x)=c_0+c_1x+c_2x^2+\ldots+c_{n-1}x^{n-1}$ of degree less than *n*. So throughout this paper, cyclic code is represented by code polynomial. Similar to integer modulo a specific prime integer *p*, here we employ code polynomials modulo x^n-1. In this case, x^n-1 is equivalent to 0 and x^n is equivalent to 1. Also in code polynomials, $x^k+x^k=0$.

In a cyclic code C of length n, the product $xc(x)$ modulo $x^n - 1$ gives another polynomial in C which is the right cyclic shift of $c(x)$.

In the language of code polynomial, the following theorem gives the necessary and sufficient condition for a code to be a cyclic code.

Theorem 1: A linear code C of length n over $GF(2)$ is cyclic if and only if C satisfies the following two conditions:
a) If $a(x)$ and $b(x)$ are code polynomials in C, then $a(x) - b(x) \in C$.
b) If $a(x)$ is a code polynomial in C and $r(x)$ is any polynomial of degree less than n, then $r(x)a(x) \in C$.

For a cyclic code of length n, the set of all code polynomials of degree less than n in the variable x with coefficients from $GF(2)$ under the operation polynomial addition and multiplication modulo $x^n - 1$ is a commutative ring with identity element $e(x) = 1$. This set of polynomial is denoted by $GF(2)[x]/\langle x^n - 1\rangle$.

The following theorem gives a connection between cyclic codes and ideals of the ring $GF(2)[x]/\langle x^n - 1\rangle$.

Theorem 2: Cyclic codes of length n over $GF(2)$ correspond precisely to the ideals in the ring $GF(2)[x]/\langle x^n - 1\rangle$.

A trivial example of an ideal in the ring $GF(2)[x]/< x^n - 1 >$ is the entire ring itself.

For example, the set of all polynomials of degree less than 3: $\{0, 1, x, x^2, 1 + x, 1 + x^2, x + x^2, 1 + x + x^2\}$ is an ideal in the ring $GF(2)[x]/\langle x^3 - 1\rangle$ where the corresponding binary code {000, 100, 010, 001, 110, 101, 011, 111} is a trivial example of a binary cyclic code of length 3.

3. CYCLIC CODES FROM ZERO DIVISORS

Now our aim is to find Non-Trivial Cyclic Codes and generate them by the zero divisors. In order to find the non-trivial cyclic codes, first let us find the zero divisors of the commutative ring $GF(2)[x]/\langle x^n - 1\rangle$.

Let us consider some particular cases, (say) for $n = 2$, $GF(2)[x]/< x^2 - 1 >= \{0, 1, x, 1 + x\}$.
The only zero divisor is $(1 + x)$ since there exist a nonzero polynomial $(1 + x)$ such that $(1 + x)(1 + x) = 0$.
The code polynomial generated by $(1 + x)$ is $\{0, (1 + x)\}$ whose corresponding binary cyclic code is {00, 11}.
For length $n = 3$, $GF(2)[x]/\langle x^3 - 1\rangle$ is the set, $\{0, 1, x, x^2, 1 + x, 1 + x^2, x + x^2, 1 + x + x^2\}$. The zero divisors of $GF(2)[x]/\langle x^3 - 1\rangle$ are $(1 + x)$, $(x + x^2)$, $(1 + x^2)$, $(1 + x + x^2)$.

The code polynomial generated by the zero divisors $(1 + x)$, $(1 + x^2)$, $(x + x^2)$ is the set, $\{0, (1 + x), (x + x^2), (1 + x^2)\}$ whose corresponding binary cyclic code is {000, 110, 011, 101}.

The code polynomial generated by the zero divisor $(1 + x + x^2)$ is $\{0, (1 + x + x^2)\}$ whose corresponding binary cyclic code is {000, 111}.

For length $n = 4$, $GF(2)[x]/\langle x^4 - 1\rangle$ have 16 code polynomials corresponding to those 16 cyclic codes.

The zero divisor of $GF(2)[x]/\langle x^4 - 1\rangle$ are $(1 + x)$, $(1 + x^2)$, $(x + x^2)$, $(x^2 + x^3)$, $(x + x^3)$, $(1 + x + x^2 + x^3)$.

The code polynomial generated by the zero divisors $(1 + x)$, $(1 + x^3)$, $(x + x^2)$, $(x^2 + x^3)$, $(x + x^3)$ is the set, $\{0, (1 + x), (x + x^2), (x^2 + x^3), (1 + x^3), (1 + x^2), (x + x^3), (1 + x + x^2 + x^3)\}$ whose corresponding binary cyclic code is {0000, 1100, 0110, 0011, 1001, 0101, 1010, 1111}.

The code polynomial generated by the zero divisors $(1 + x^2)$, $(x + x^3)$ is $\{0, (1 + x^2), (x + x^3), (1 + x + x^2 + x^3)\}$ whose corresponding binary cyclic code is {0000, 0101, 1010, 1111}.

The code polynomial generated by $(1 + x + x^2 + x^3)$ is $\{0, 1 + x + x^2 + x^3\}$ whose corresponding binary cyclic code is {0000, 1111}.

Similarly, we can find the cyclic codes of length $n \geq 5$ generated by the zero divisors of their corresponding ring.

Here, in all the cases, the binary cyclic code generated by the zero divisors is nontrivial and the zero divisors accounts for all possible generators of the nontrivial cyclic code of length n.

4. CONCLUSION

In order to find all the nontrivial cyclic codes of length n, we find the zero divisors of the ring $GF(2)[x]/< x^n - 1 >$ and the zero divisors generate only the nontrivial cyclic codes of length n.

We can also find them by finding the divisors of the polynomial $x^n - 1$ but the zero divisors account for all the generators of the nontrivial cyclic code.

REFERENCES

Adams, Sarah Spence, Introduction to Algebraic Coding Theory, Franklin W. Olin College: NSF CCLI, 2008.

Dave K Kythe, Prem K Kythe, Algebraic and Stochastic Coding Theory, CRC Press, 2012.

Gallian J, Contemporary Abstract Algebra, Nelson Education, 2009.

Hoffman D G, Coding Theory, The Essentials, Marcel Dekkar, NY, 1991.

Van Lint J H, Introduction to Coding Theory, Springer- Verlang, Berlin, 3rd edition, 1999.