Express, an International Journal of Multi Disciplinary Research
ISSN: 2348 – 2052, Vol. 1, Issue 6, June 2014
Available at: www.express-journal.com

ENUMERATION OF CYCLIC CODES OVER GF (5)

By

Flora Mati Runji
Department Of Mathematics, Statistics and Actuarial Sciences
Karatina University
Kenya
Email:florunji2010@gmail.com

Abstract

In this paper we establish how many cyclic codes of length n are there over GF (5) and make generalized deductions in case $n = 5^n$ and $n = 5m,\ (m,5) = 1,$ where m is not necessarily prime.A code C is said to be cyclic if it is a linear code and any cyclic shift of a codeword is also a codeword. Cyclic codes of length n are subspaces of $R_n = \frac{F[x]}{x^n - 1}$. In a non – zero cyclic code C, the unique monic polynomial $g(x)$ of least degree, is called the generator polynomial. Thus in finding cyclic codes of length n, we factorize $x^n - 1$ into irreducible polynomials. We then get all monic polynomials $g(x)$ that divide $x^n - 1$. Each $g(x)$ is a generator polynomial and generates a cyclic code.

Keywords: Cyclic Codes, length of a code, Factorization of Polynomials.

1. Introduction

Hill (1968), Peterson (1961) and Pretzel (1992) presents the fundamental concepts in coding theory and error- correcting codes. If F is a field, then F^n is a vector space over a field F . A set C of vectors from F^n of length n is called a linear code if and only if C is a subspace of F .

If F is a field, then $F[x]$ forms a commutative ring with unity. For cyclic codes, we are interested in $R_n = \frac{F[x]}{x^n - 1}$ which consists of congruence classes of polynomials in $F[x]$ modulo $x^n - 1$. Thus a code C in R_n is cyclic if and only if:

i) $a(x), b(x) \in C$ implies $a(x) + b(x) \in C$

ii) If $a(x) \in C$ and $r(x) \in R_n$ implies $r(x)a(x) \in C$

This implies that cyclic codes are the ideals of the ring R_n . For any $f(x) \in R_n$, then the set $\langle f(x) \rangle$ is a cyclic code generated by $f(x)$. Also for any non- zero cyclic code C in R_n there

exists a unique monic polynomial $g(x)$ of smallest degree such that $g(x)$ is a factor of $x^n - 1$ and $C = \langle g(x) \rangle$. This polynomial is called the generator polynomial of the code.

If C be an (n, k)- cyclic code over GF(q), then the generator polynomial of degree n-k always exists , its unique , and is a divisor of $x^n - 1$.

Thus to find all cyclic codes of a given length n, all we need is to factorize $x^n - 1$ into irreducible monic polynomials, which will form the generator polynomials for all the codes.

If C is a cyclic (n, k) – code with generator polynomial $g(x)$,then $g(x)$ is a factor of $x^n - 1$ and so $x^n - 1 = g(x)\,h(x)$, for some polynomial $h(x)$ called the **check polynomial** of C. If C is a cyclic code in R_n with generator polynomial $g(x)$ and check polynomial $h(x)$ then an element $f(x)$ of R_n is a codeword of C if and only if $f(x)h(x) = 0$ in R_n.

From the above, one observes that the properties and capabilities of all cyclic codes depend on the factors of their generator polynomial over some finite field. Therefore, when designing cyclic codes, the set of irreducible polynomials must be known. Consequently, great effort has been directed towards the factorization of polynomials. In practice, the polynomials over the binary field $GF(2)$ are the ones that have been extensively studied and used. Marsh (1957) , tabulated the irreducible polynomials over $GF(2)$ through degree 19. Berlekamp (1967), presented an algorithm for factoring a given polynomial over any finite field into powers of irreducible polynomials. The method used involved reducing the factorization of a polynomial of degree n over $GF(q)$ to the solution of about $\frac{n(q-1)}{q}$ linear equations in as many unknowns over $GF(q)$. This algorithm treats the factorization of the binomial $x^n - 1,\ n = q^i,\ i = 1,2,3,\ldots$ as a special case. The algorithm involves some matrix manipulations and the computation of a number of greatest common divisors.

McEliece (1969), presented some work similar to the one introduced by Berlekamp. Both Berlekamp and McEliece made the observation that a special class of polynomials, namely the one satisfying the relation:

$[h(x)]^q - h(x) \equiv 0 \bmod f(x)$, has a very interesting property regarding the factorization of a given $f(x)$ over $GF(q)$. Both had a common Theorem, but took somehow different approaches for generating polynomials $h(x)$ satisfying the above relation. At the final step,

both algorithms make use of the Euclidean Algorithm for the computation of the greatest common divisors resulting in the complete factorization of $f(x)$.David (1981), presents a probabilistic algorithm for factoring polynomials over finite fields. His approach combined with Berlekamp's algorithm avoids the need for resultants and linear equations. Hence it is a simpler algorithm.

On cyclic codes of length n over Z_{p^m}, p a prime, $m \geq 1$,a lot of work has been done especially for $p = 2$.Calderbank and Sloane (1995), worked on cyclic codes over the ring Z_{p^m} of length n such that $(n, p) = 1$.Woo (2013), studied cyclic codes of length 2^n over Z_4 and showed that any ideal of $Z_4[x]/x^{2^n}-1$ is generated by at most two polynomials of the standard forms. He further gave a description of the cyclic codes of even length over Z_4 namely the ideals of $Z_4[x]/x^l-1$, where *l* is an even integer.

2. Irreducible Monic Polynomials Over Gf(5)

A polynomial f(x) in F$[x]$ is said to be reducible if f(x) = a(x)b(x) where a(x),b(x) $\in$F$[x]$ and deg a(x) and deg b(x) are both less than deg f(x).

If f(x) is not reducible, it is irreducible.

According to Berlekamp(1968) , the number of irreducible polynomials, $L_q(n)$, of degree n over a finite field GF(q) is given by

$$L_q(n) = \frac{1}{n} \sum_{d|n} \mu(n/d)\, q^d ,$$

where, $\mu(n)$ is the Mobius function defined by

$\mu(1) = 1$,

$\mu(n) = 0$ if n has a squared factor

$\mu(p_1, p_2 \ldots\ldots p_k) = (-1)^k$ where $p_1, p_2 \ldots\ldots\ldots p_n$ are distinct primes.

Thus we can compute with this formula the number of irreducible monic polynomials where GF(q) = GF(5) i.e. q = 5 and n = degree.

For example,

For n = 1, $L_5(1) = 1/1\{\mu(1)5^1\} = 5$ polynomials.

n = 2, $L_5(2) = 1/2\{\mu(2/1)5^1 + \mu(2/2)5^2\}$

$= {}^1/_2\{-5 + 25) = 10$ polynomials

n = 3, $L_5(3)$ $= {}^1/_3\{\mu({}^3/_1)5^1 + \mu({}^3/_3)5^3\}$

$= {}^1/_3\{-5 + 125\} = 40$ polynomials

n = 4, $L_5(4) = {}^1/_4\{\mu({}^4/_1)5^1 + \mu({}^4/_2)5^2 + \mu({}^4/_4)5^4\}$

$= {}^1/_4\{0 - 25 + 625\} = 150\ polynomials$

n = 5, $L_5(5) = {}^1/_5\{\mu({}^5/_1)5^1 + \mu({}^5/_5)5^5\}$

$= {}^1/_5\{-5 + 3125\} = 624$ polynomials

n = 6, $L_5(6) = {}^1/_6\{\mu({}^6/_1)5^1 + \mu({}^6/_2)5^2 + \mu({}^6/_3)5^3 + \mu({}^6/_6)5^6\}$

$= {}^1/_6\{5 - 25 - 125 + 15625\}$

= 2580 polynomials.

N = 7, $L_5(7) = {}^1/_7\{\mu({}^7/_1)5^1 + \mu({}^7/_7)5^7\}$

$= {}^1/_7\{-5 + 5^7\}$

= 11,160 polynomials

3. Factorization of $x^n - 1$ over GF (5)

Proposition

If $x^n - 1 = [g_1(x)]^{k_1}[g_2(x)]^{k_2} \ldots [g_m(x)]^{k_m}$ where $g_1(x), g_2(x), \ldots, g_m(x)$ are distinct irreducible monic polynomials, then the number of cyclic codes of length n is given by:

$$(k_1+1)(k_2+1)\ldots(k_m+1) = \prod_{i=1}^{m}(k_i+1).$$

Proof

If g(x) is a generator polynomial, then g(x)|$x^n - 1$. Let $g(x) = [g_1(x)]^{r_1}[g_2(x)]^{r_2} \ldots [g_m(x)]^{r_m}$, where $0 \le r_i \le k_i$, the number of ways to choose r_i is $k_i + 1$ for each *i*. Total number of possible polynomials is $(k_1+1)(k_2+1)\ldots(k_m+1) = \prod_{i=1}^{m}(k_i+1)$.

Example :

Consider $x^3 - 1 = (x - 1)(x^2 + x + 1)$ over GF(5).

The number of cyclic codes of length 3 is 2 x 2 = 4

The generator polynomials and generator matrices are shown below.

Generator polynomial $g(x)$	Generator matrix
1	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
$x-1$	$\begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}$
x^2+x+1	$(1 \quad 1 \quad 1)$
$x^3-1=0$	$(0 \quad 0 \quad 0)$

Table 1: Number of cyclic codes of length n over GF (5)

x^n-1	**Factors**	**Number of cyclic codes**
x^2-1	$(x-1)(x+1)$	4
x^3-1	$(x-1)(x^2+x+1)$	4
x^4-1	$(x-1)(x-2)(x-3)(x-4)$	16
x^5-1	$(x-1)^5$	6
x^6-1	$(x+1)(x+4)(x^2+x+1)(x^2+4x+1)$	16
x^7-1	$(x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$	4
x^8-1	$(x+1)(x+2)(x+3)(x+4)(x^2+2)(x^2+3)$	64
x^9-1	$(x-1)(x^2+x+1)(x^6+x^3+1)$	8
$x^{10}-1$	$(x-1)^5(x+1)^5$	36

Next we look at relationships that appear in the number of cyclic codes when x^n-1 is factorized then make deductions where possible or generalizations.

Table 2: Number of cyclic codes of length $n = 5^k$

K	$x^n - 1$	Factors	No. of cyclic codes
0	$x - 1$	$x - 1$	2
1	$x^5 - 1$	$(x - 1)^5$	6
2	$x^{25} - 1$	$(x - 1)^{25}$	26
3	$x^{125} - 1$	$(x - 1)^{625}$	126
4	$x^{625} - 1$	$(x - 1)^{625}$	626
.			
.			
.			
K	$x^{5^k} - 1$	$(x - 1)^{5^k}$	$5^k + 1$

Thus the number of cyclic codes when $n = 5^k$ is equal to $5^k + 1$ or simply n + 1.

Table 3: Number of cyclic codes of length n = 5m, (m, 5) = 1 where m is not necessarily prime.

M	**$x^n - 1$**	**Factors**	**No. of cyclic codes**
2	$x^{10} - 1$	$(x - 1)^5(x + 1)^5$	$6^2 = 36$
3	$x^{15} - 1$	$(x - 1)^5(x^2 + x + 1)^5$	$6^2 = 36$
4	$x^{20} - 1$	$(x - 1)^5(x - 2)^5(x - 3)^5(x - 4)^5$	$6^4 = 1296$
6	$x^{30} - 1$	$(x - 1)^5(x - 4)^5(x^2 + x + 1)^5(x^2 + 4x + 1)^5$	$6^4 = 1296$
7	$x^{35} - 1$	$(x - 1)^5(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^5$	$6^2 = 36$
8	$x^{40} - 1$	$(x + 1)^5(x + 2)^5(x + 3)^5(x + 4)^5(x^2 + 2)^5(x^2 + 3)^5$	$6^6 = 46656$
9	$x^{45} - 1$	$(x - 1)^5(x^2 + x + 1)^5(x^6 + x^3 + 1)^5$	$6^3 = 216$

Thus if $n = 5m$ where $(m,5) = 1$ and $x^m - 1 = p_1(x)p_2(x)\ldots\ldots\ldots\ldots\ldots\ldots p_k(x)$ where $p_1(x)$, $p_2(x)$, ……, $p_k(x)$ are irreducible in GF(5) , then the number of cyclic codes of order $n = 5m$ is 6^k.

Theorem 1

Suppose $n = 5^r m$ where (5, m) = 1 and $x^m - 1$ has k distinct irreducible factors, i.e. $x^m - 1 = p_1(x)\ p_2(x)\ \ldots\ldots\ldots\ p_k(x)$, then the number of cyclic codes of order $n = 5^r m$ is $(5^r + 1)^k$.

Proof:

$x^n - 1 = x^{5^r} - 1 = (x^m - 1)^{5^r}$

$= [(p_1(x)\, p_2(x) \ldots p_k(x)]^{5^r}$

$$= \prod_i^k [p_i(x)]^{5^r}$$

i = 1, 2 …k which implies number of cyclic codes is equal to $(5^r + 1)^{k.}$

In this work we have given a general formula for getting the number of cyclic codes of order $x^n - 1$ where $n = 5^r m$, $(m, 5) = 1$ over GF(5). If the number of distinct irreducible factors of $x^m - 1$ were known, the result would be more specific.

REFERENCE

1. Berlekamp, E. *Algebraic Coding The*ory. McGraw – Hill Book Company, 1968.
2. Berlekamp, E. *Factoring Polynomials over Finite Fields*. B.S.T.J, Oct. 1967.
3. Calderbank A.R.and Sloane N.J.A. *Modular and P-adic cyclic codes, Designs codes Cryptography*, Vol.6, 1995, pg 21-35.
4. Claude S. *A mathematical theory of communication*, Bell Syst.Tech Journal V27, 1948, 379-423, 623-656
5. David, G.C. *A new Algorithm for Factoring Polynomials over Finite Fields*. Mathematics oof Computation, Vol.36, No. 154, 1981, pg 587-592.
6. Hill, R. *A First Course in Coding Theory*. Claredon Press: Oxford, 1986.
7. Marsh R.W. Table of Irreducible Polynomials over $GF(2)$through Degree 19. National Security Agency, Washington D.C., 1957.
8. McEliece R. *Factorization of Polynomials over Finite Fields*. Mathematics of Computation, Vol 23, No. 108, Oct. 1969, pg. 861- 67.
9. Peterson W. *Error – Correcting Codes*. MII Press, Cabridge Mass, 1961.
10. Pretzel, O. *Error – Correcting Codes and Finite Field*. Claredon Press: Oxford, 1992.
11. Woo, S. *Cyclic Codes of length 2^n over $\mathbb{Z}_4$*.Commun. Korean Math. Soc. Vol. 28, No. 1, 2013, pg 39-54.