ISSN 2250-3153

CYCLIC CODES OF LENTH N OVER $GF(q)$ $q-$ CYCLOTOMIC COSETS MODULO N AND APPLICATION OF BURNSIDE'S LEMMA

M. Mary Jansi Rani*

*Department of Mathematics, Assistant Professor and Head, Sureya College of Eingeering, Trichy

Abstract : The idea of q - cyclotomic cosets modulo n due to carry Huffman and Vera pless is considered in the context of linear codes of length n over $GF(q)$ where $q = p^m$, p is a prime, $m \geq 1$. An explicit formula for the number of q - cyclostomes cosets modulo is obtained as an application of the classical Burnsides lemnra. The formula for the number of cyclic codes in $R_n = F_q[x]/(x^n - 1)$ is deduced. Illustration is shown for special value of q and n.

Index terms: Field extensions, splitting fields, cyclic codes, minimal polynomial, primitive roots, Orbit of group action, q-Cyclotomic cosets.

1. INTRODUCTION

Let $\mathbb{F}_q$ denotes a finite field having q- elements q = p^l where p is a prime and l ≥ 1. The set of nonzero elements of $\mathbb{F}_q$ is denoted $\mathbb{F}_q^*$ is a cyclic group of order q-1 under multiplication. It implies that $\mathbb{F}_q^*$ = { α^i / 0 ≤ i ≤ q-2 } Where α is a generator of the cyclic group F_q^*. Infact α may be taken as an imaginary (q-1) th root of unity α is a complex number such that |α | = 1.

Definition 1 A linear code C is called cyclic code if whenever a = $a_0, a_1, a_2, a_3 \ldots\ldots a_{n-1}$ is a code word, then a' obtained from a by a cyclic shift of the coordinates is such that
$a' = a_{n-1}, a_0, a_1, a_2 \ldots\ldots a_{n-2}$ is also a codeword. By a cyclic shift of the coordinates we mean a permutation π of the set $\{1,2,3 \ldots\ldots\ldots n\}$ defined by $\pi(i) = i + 1 (\text{mod } n)$ of $i \to i + 1 \pmod n$.

Definition 2 The q-cyclotomic cosets of s modulo n is the set $C_s = \left\{s, sq, sq^2 \ldots\ldots sq^{r-1}\right\}$ modulo n where r is the smallest positive integer such that $sq^r \equiv s \pmod n$. C_s is the orbite of the permutation $\tau : i \to i_q \pmod n$ that contains s. It is shown in [3] that the number of cyclic codes in R_n is 2^m where mis the number of q – cyclotomic cosets modulo n.

The purpose of this note is to give an evaluation of m using a counting principle called Burnsides Lemma [7] while highlighting a few related results we revisit cyclic codes of length 2^m considered by Manju Pruthi in [5].

2. PPRELIMINARIES

Let s be an integer satisfies $0 \leq s \leq n-1$. The q –cyclotomic cosets of s modulo n is given by $C_s = \left\{s, sq, sq^2 \ldots\ldots sq^{r-1}\right\}$ where

r = $\exp_n q$. That implies r is the least positive integer such that

$$sq^r \equiv s \pmod n \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Definition 3 Let $\sigma = \pi_{q^i}$ for I = ,1,2,3,…..r-1 be a permutation belonging to G_q .Let $s \in T$,$0 \leq s \leq n-1$. The orbit of s under σ written $O_{s,\sigma} = \sigma^t$ (s) $t \in N \cup \{0\}$.

Example 4 Let T ={ 0,1,2,3,4 } n = 5 q =3 G_3 = { $I_5, \pi_3, \pi_{3^2}, \pi_{3^3}$ }.We note that π_{3^4} (T) the orbit of $2 \in T$ under π_3 is O_{2,π_3} = $\{\pi_3{}^t (2) / t \in N\}$= { 2, $\pi_3(2)$,$\pi_{3^2}(2)$, $\pi_{3^2}(2)$, $\pi_{3^2}(2)$}

Next, when C is a cyclic code of length n, a codeword c(x) = $c_0 c_1 c_2 \ldots\ldots\ldots c_{n-1}$ where $c_i \in \mathbb{F}_q$ is identified with the polynomial c(x) =$c_0 + c_1 x + c_2 x^2 \ldots\ldots\ldots c_{n-1} x^{n-1}$ which is an element of $\mathbb{R}_n$ Since $\mathbb{R}_n$ is the ring the set $V_{n,q}$[x] = { $c_0 + c_1 x + c_2 x^2 \ldots\ldots\ldots c_{n-1} x^{n-1}$ / $c_i \in \mathbb{F}_q$ i = 0,1,2,3……..n-1} is a vector space of dimension n over $\mathbb{F}_q$.Therefore $V_{n,q}$[x] is isomorphic to $\mathbb{R}_n$ when multiplication of polynomial in $V_{n,q}$[x] is reduced modulo $x^n - 1$.while considering $\mathbb{R}_n$ since $\langle x^n - 1 \rangle$ is principle ideal of $\mathbb{F}_q[x]$, I[x] = $\langle x^n - 1 \rangle$ = {g(x) $(x^n - 1)$ / g(x) $\in \mathbb{F}_q[x]$ } an element of $\mathbb{R}_n$ is of the form $c_0 + c_1 x + c_2 x^2 \ldots\ldots\ldots c_{n-1} x^{n-1}$ + I [x] $c_i \in \mathbb{F}_q$. Since $\mathbb{R}_n$ is also a principle ideal domain, the principle ideal generated by h (x) $\in \mathbb{R}_n$ is denoted by $\langle h(x) \rangle$ .If α is a primitive n^{th} root of unity α^n =1 and $\alpha^m \neq 1$ occurring in some extension $\mathbb{F}_q{}^t$ of $\mathbb{F}_q$, t ≥ 1 ,then h(x) = $\Pi_s M_{\alpha^s}$ (x) where s runs through a subset of representatives of the q – cyclotomic cosets modulo n and M_{α^s} (x) = $\Pi_{i \in c_s} (x - \alpha^i)$ where c_s is the q cyclotomic cosets modulo n in [3] . If $\mathbb{F}_q{}^{t*}$=$\mathbb{F}_q{}^t$- {0} is a cyclic group of order q^t -1. If α is a primitive n^{th} root of unity occurring $\mathbb{F}_q{}^{t*}$, α^n =1 implies that $\mathbb{F}_q{}^{t*}$ contains a cyclic subgroup of order n and by Lagrange's theorem n divides O($\mathbb{F}_q{}^{t*}$) = q^t -1. Suppose that r is a primitive element in $\mathbb{F}_q{}^t$ where t = $exp_n q$. If $\alpha \in \mathbb{F}_q{}^t$ is such that $\alpha = r^d$ is a primitive n^{th} root of unity where d = $\frac{q^t-1}{n}$ the zeros of M_{α^s} (x)'s are α^{ds}, $\alpha^{dsq}, \alpha^{dsq^2} \ldots\ldots\ldots\ldots \alpha^{dsq^{r-1}}$.

There are actually $\alpha^s, \alpha^{sq}, \alpha^{sq^2} \ldots\ldots\ldots\ldots \alpha^{sq^{r-1}}$ where r is the least positive integer such that ds$q^r \equiv ds(q^t$-1) if and only if s$q^r \equiv$ s (mod n).This leads to the definition of the q-cyclotomic cosets given in (1).

3. q ARY CYCLIC CODES OF LENGTH 2^m (m - 3)

We consider cyclic codes of length 2^m (m $\geq$ 3) over GF(q) = $\mathbb{F}_q$ where q = p^l, p an odd prime and $l \geq 1$.Manju pruthi [5] obtains q cyclotomic cosets modulo 2^m using purely number theoretic ideas and the structure of a cyclic code given as a $[2^m, 2^{i-1}, 2^{m-i+1}]$ code over $\mathbb{F}_q$,

1 $\leq$ i $\leq$ m and m $\geq$ 3. The restriction m $\geq$ 3 arises from the fact that when q is odd $q^{\frac{\varphi(2^m)}{2}} \equiv 1 \ (mod\ 2^m)$. In other words, 2^m (m $\geq$ 3) has no primitive roots modulo 2^m It follows that exp q = 2^{m-2}, $\varphi(2^m)$ =2^{m-1} Manju pruthi articles [5] appeared before the publication of the book [3] authored by Huffman and Pless.

4. AN APPLICATION OF BURNSIDES LEMMA

Definition 5 In [7] For x, y ∈ X we define a congruence x ≡ y (mod G) to mean that there exists an element g ∈ G such that g(x) = y congruence mod G is an equivalence relation on x. The equivalence classes under ≡ are called the orbit of G in x.

Definition 6 In [7] For x∈ X we define G x as the set given by G_x = { g∈G/ g(x) = x} is called the stabilizer of x in G. If O_x denotes the orbit of G containing x, then $|G| = |G_x||O_x|$ where $|O_x|$is the number of cosets of G_x in G.

Theorem 1 Let T ={0,1,2,…… (n-1)} be the least non negative complete residue system (mod n).If G_q denotes the group of permutations π_q : i→ i_q for i∈ T. The number of q – cyclotomic cosets modulo n is given by $N_n(q) = \frac{1}{r}\sum_{g \in G} \psi(g)$ Where ψ (g) is the number of elements of T which are left fixed by g Є G_q

Proof : We suppose that S(G) denotes the set of orbits of G_q in X. let d denote the number of elements of the form g(x) where x∈ X , g∈ G_q and g(x) = x for fixed g∈ G_q . The number of such elements is ψ (g) .Then d = $\sum_{g \in G} \psi(g)$

Now, for fixed x∈ X the number of elements g(x) for which g(x) = X, g∈ G_q is by definition of G_q is $|G_q|$. If J denotes the union of orbits of G_q we obtain

$$d = \sum_{y \in J} |G_y|$$

$$= \sum_{O \in s(G)} \sum_{x \in Gq} |G_q| = \sum_{O \in s(G)} \sum_{x \in X} |G_q|$$

$$= \sum_{O \in s(G)} \sum_{x \in X} \frac{|G_q|}{|O_x|}$$

$$= \sum_{O \in s(G)} |O_x| \frac{|G_q|}{|O_x|}$$

$$= |G_q| \sum_{O \in s(G)} 1$$

$$= |G_q| N_n(q)$$

$$= rN_n(q) \quad \text{since } |G_q| = r,\ exp_n\ q = r.$$

$$rN_n(q) = \sum_{y \in J} |G_y|$$

$$N_n(q) = \frac{1}{r}\sum_{y \in J} |G_y|$$

$$= \frac{1}{r}\sum_{y \in Gq} \psi(g)$$

Example 8 We consider 2– cyclotomic sets modulo 9. Here as $exp_9(9) = 6 = \emptyset(9)$, 2 is a primitive root modulo 9.

We have $C_o = \{0\}$, $C_1 = \{1,2,4,8,7,5\}$, $C_3 = \{3,6\}$

The primitive 9th roots of unity lie in F_{26} , but in no smaller extension of GF (2). The irreducible factors of $x^9 - 1$ over GF (2) have degree 1, 6 & 2. The polynomials are $M_1(X) = x+1$, $M_\alpha(x) = x^6 + x^3 + 1$.Where α is a primitive 9th roof of unity in $\mathbb{F}_2{}^6$ α^3 is a primitive 3rd root of unity as $(\alpha^3)^3 = 1$. The extension $\mathbb{F}_2{}^6$ of $\mathbb{F}_2{}^3$ is of degree 2. So, irreducible polynomial α^3 over GF (2)is of degree 2.The only quadratic irreducible polynomial over G F(2) is X^2+X+1. Therefore $X^9 - 1 = (X+1)(X^6 + X^3 + 1)(X^2 + X + 1)$ Here $q = 2$, $|G_2| = 6$ The elements of G_2 are $\{I, \Pi_2, \Pi_4, \Pi_8, \Pi_{16}, \Pi_{32}\}$

$T=\{0,1,2,3,4,5,6,7,8\}$ ψ (I) = 8 elements of T which are kept fixed on multiplication by 2. The q – cyclotomic cosets modulo 9 are already shown So, by Burnside's lemma, number of 2 cyclotomic cosets (mod 9) $=18/6=3$

Example 9 We consider 3-cyclotomic cosets modulo 13 .α be a primitive 13^{th} root of unity. The 3 – cyclotomic cosets are

$C_o=\{0\}$ $C_1=\{1,3,9\}$ $C_2=\{2,6,5\}$ $C_4=\{4,12,10\}$ $C_7=\{7,8,11\}$ As $\exp_{13}(3)=3$ the primitive 13th roots of unity lie on $\mathbb{F}_{3^3}$ but in no smaller extension of GF(3). The irreducible factors of X^{13}-1 are

$$M_1(X)=X-1=X+2$$
$$M_\alpha(X)=X^3+2X+1$$

$M_{\alpha^2}(X), M_{\alpha^4}(X)$ and $M_{\alpha^7}(X)$ are also of degree 3. The number of 3 – cyclotomic cosets modulo 13 is 5. In the notation of burnsides lemma. $|G_q|$ = 3 $\psi(I)$= 13, $\psi(\pi_3)$ = 1, $\psi(\pi_9)$ = 1 So, the number of 3 – cyclotomic cosets modulo 13 is

$$\frac{1}{3}(13+1+1)=5$$

Theorem 10 The number of cyclic codes in $R_n=F_q[x]/(x^n-1)$ is equal to 2^N where N is the number of q – cyclotomic cosets modulon n.

Proof Let α be a primitive nth root of unity occurring in F_{qt} where $t=\exp_n(q)$. A cyclic code C in R_n is generated by a manic polynomial h(x) of minimum degree. From (2) we see that h(x) contains $M_{\alpha^S}(X)$ determined by q – cyclotomic cosets modulon n, as a factor $M_{\alpha^S}(X)$ is manic and in irreducible over F_q. Since $M_{\alpha^S}(X)$ splits only in an extension $\mathbb{F}_{q^t}$ of $\mathbb{F}_q$ .So, each non zero cyclic code C is associated with one or more q- cyclotomic cosets chosen one at a line , two at a line and so an out of the N – q – cyclotomic cosets modulo n we observe that (o) The zero cyclic code corresponds to x^n-1 the counting of a non zero cyclic code C happens with counting 1.

1) $\binom{N}{1}$ times, when each q – cyclotomic coset modulo n is chosen one at a time.

2) $\binom{N}{N}$ Times, when two q – cyclotomic cosets modulo n are chosen at a time.

……..

…….

3) $\binom{N}{i}$ times, when i q – cyclotomic coset modulo n are chosen at a time.

4) $\binom{N}{N}$ times, when all the N q – cyclotomic coset modulo n are chosen at a time.

Thus the total member of cyclic codes in R_n is given by $1+\binom{N}{1}+\binom{N}{2}+.....\binom{N}{i}+.....1=2^N$.

Example 12 We consider 2 – cyclotomic cosets modulo 15. If α is a primitive 15th root of unity α belongs to $F_2^4=F_{16}$. The 2 – cyclotomic cosets modulo 15 are

$C_o=\{0\}$, $C_1=\{1,2,4,8\}$, $C_3=\{3,6,9,12\}$,$C_5=\{5,10\}$, $C_7=\{7,11,13,14\}$.

$$(X-\alpha)(X-\alpha^2)(X-\alpha^4)(X-\alpha^8) = M_{\alpha}(X) = X^4 + X + 1$$
$$(X-\alpha^3)(X-\alpha^6)(X-\alpha^9)(X-\alpha^{12}) = M_{\alpha^3}(X) = X^4 + X^3 + X^2 + X + 1$$
$$(X-\alpha^5)(X-\alpha^{10}) = M_{\alpha^5}(X) = X^2 + X + 1$$
$$(X-\alpha^7)(X-\alpha^{11})(X-\alpha^{13})(X-\alpha^{14}) = M_{\alpha^7}(X) = X^4 + X^3 + 1$$

The factorization of $X^{15}-1$ into irreducible polynomials over $\mathbb{F}_2$ is the number of cyclic codes in is

$$X^{15} - 1 = (X+1)(X^4 + X + 1)(X^4 + X^3 + X + 1)(X^4 + X^3 + 1)$$

Example 13 We consider 3 – cyclotomic cosets modulo 13. $\exp_{13}(3) = 3$ Let α be primitive 13th root of unity. The splitting field of α is $F_{3^3} = F_{27}$ $(X^{13} - 1) = (X-1)(X^3 + 2X + 1)$. The 3– cyclotomic cosets modulo 13 are

$$C_o = \{0\} \quad C_1 = \{1,3,9\} \quad C_2 = \{2,6,5\} \quad C_4 = \{4,12,10\} \quad C_7 = \{7,8,11\}$$
$$M_{\alpha}(X) = (X-\alpha)(X-\alpha^3)(X-\alpha^9) = X^3 + 2X + 1 \quad M_{\alpha^2}(X) = (X-\alpha^2)(X-\alpha^6)(X-\alpha^5)$$
$$M_{\alpha^4}(X) = (X-\alpha^4)(X-\alpha^{12})(X-\alpha^{10})$$
$$M_{\alpha^7}(X) = (X-\alpha^7)(X-\alpha^8)(X-\alpha^{11})$$

The number of cyclic codes in $R_{13} = \dfrac{F_3[X]}{X^{13}-1}$ is $2^5 = 32$.

References

[1] Alexander Barg, Error Correcting codes, ENEE626 Lecture 12 (Oct 18, 2005).

[2] Tom. M. Apostal, Introduction to Analytic Number theory. Springer vulgar UTM (1976) Chapters 10 pp 204 - 212.

[3] Carry Huffman and VeraPless, Fundamentals of error- correcting codes, Cambridge university (2004) Chapter 3, section 3.7 pp 112 -118 Chapter 4, section 4.1, 4.2 pp 122 -127.

[4] J. B. Fraleish, First course in Abstract Algebra. Addition - Wesley publishing co. in. Reading Mas- sachusetts, osa 2nd Edn (1968) Sections 35, 42 pp 288-294, 348-351.

[5] Manju Pruthi, Cyclic codes of length 2^n, Proc. Ind. Acad. Sci (Mathsci), Vol. III, No. 4 Nov 2001, pp 371-379.

[6] Pruthi Manju and Arora S. K Minimal codes of prime power length finite fields and their application,Vol. 3 (1997) pp 99-113.

[7] R.Sivarama Krishnan, Certain Number theoretic Episodes in Algebra. Boca Raton, Florida Use(2006), Chapter 7, Sections 7.4 pp 188 – 193.

Authors

First Authors : M.Mary Jansi Rani ,M.Sc,M.Phil,Assistant Professor and Head,Sureya College of Engineering college,Trichy.
e-Mail id –anthuvanjansi@gmail.com.