A CLASS OF CYCLIC CODES

Monika Sangwan(Research scholar)Department of Mathematics,
Guru Jambheshwar University of Science and Technology,
Hisar 125001(India)
Email. monika.gjust@gmail.com

ABSTRACT Cyclic codes have been widely used in digital communication system and consume electronics as they have efficient encoding and decoding algorithms. In coding theory cyclic codes has been an important topic of study for many years. In this paper a class of cyclic codes with some conditions is described.

Keywords: Cyclic codes, Linear codes, Gaussian periods.

INTRODUCTION

Throughout this paper, let p be a prime, $q= p^s$, $r= q^m$ for some integers s, m ≥ 1. Let F_r be a finite field of order r and γ be a generator of the multiplicative group $F_r^*=F_r\backslash \{0\}$. An [n, k, d]-linear code C over F_q is a K-dimensional subspace of F_q^n with minimum (Hamming) distance d. It is called cyclic if any $(c_0,c_1,\ldots,c_{n-1})\in C$ implies $(c_{n-1},c_0,\ldots,c_{n-2}) \in C$.

Consider the one-one linear map defined by

$$\sigma: \quad C \quad \rightarrow \quad R = F_q[x]/(x^n-1)$$

$$(c_0, c_1, \ldots , c_{n-1}) \alpha \; c_0+c_1x+\ldots+c_{n-1}x^{n-1}.$$

Then C is a cyclic code if and only if σ(C) is an ideal of the ring R. Since R is a principal ideal ring, there exists a unique monic polynomial g(x) with least degree satisfying σ(C) = g(x)R and $g(x)I(x^n-1)$. Then g(x) is called the generator polynomial of C and $h(x) = (x^n-1)/g(x)$ is called the parity- check polynomial of C. If h(x) has t irreducible factors over F_q, we say for simplicity such a cyclic code C to have t zeros.

The objectives of this paper are to describe a new class of cyclic codes with arbitrary number of zeros.

THE CLASS OF CYCLIC CODES

First of all, we make the following assumptions for the rest of this paper.

The Main Assumptions:

Let $r = q^m = p^{sm}$ be a prime power for some positive integers s, m and let $e \geq t \geq 2$. Assume that

(i) a is not congruent to zero modulo (r-1) and e/(r-1);

(ii) $a_i \equiv a + \frac{r-1}{e}\Delta_i \pmod{r-1}$, $1 \leq i \leq t$ where $\Delta_i \neq \Delta_j \pmod{e}$ for any $i \neq j$ and

$\gcd(\Delta_2 - \Delta_1, \ldots, \Delta_t - \Delta_1, e) = 1$;

(iii) $\deg h_{a1}(x) = \ldots = \deg h_{at}(x) = m$, and $h_{ai}(x) \neq h_{aj}(x)$ for any $1 \leq I \neq j \leq t$, where $h_a(x)$ is the minimal polynomial of γ^{-a} over F_q.

From what follows, define

$$\delta = \gcd(r-1, a_1, a_2, \ldots, a_t), \qquad n = \frac{r-1}{\delta}$$

and

$$N = \gcd\left(\frac{r-1}{q-1}, ae\right).$$

It is to verify that

$$e\delta \setminus N(q-1).$$

The class of cyclic codes considered in this paper is defined by

$$C = \left\{ c(x_1, x_2, \ldots, x_t) = \left(Tr_{r/q}\left(\sum_{j=1}^{t} x_j \gamma^{a_j i} \right) \right)_{i=0}^{n-1} : x_1, \ldots, x_t \in F_r \right\}$$

(1)

where $Tr_{r/q}$ denotes the trace map from F_r to F_q. It follows from Delsarte's theorem that the code C is an [n, tm] cyclic code over F_q with parity check polynomial $h(x) = h_{a1}(x) \ldots h_{at}(x)$. This code C may contain many cyclic codes studied in the literature as special cases. In particular, when t=2, $a_0 = \frac{q-1}{h}$, $a_1 = \frac{q-1}{h} + \frac{r-1}{e}$ for positive integers e, h such that e\h and h\(q-1), the code C has been studied in [7],[4],[9],[10],[11] and [6].

In the definition of C we choose integers a_1, a_2, … , a_t from a set of arithmetic sequence with common difference $\frac{r-1}{e}$ modulo r-1. This choice of these a_i's allow us to compute the weight distribution of the code C. If the integers a_i are not chosen in this way, it might be difficult to find the weight distribution. The conditions in the main assumptions are to guarantee that the dimension of C is equal to mt.

Group characters, Cyclotomy and Gaussian periods

Let $Tr_{r/p}$ denote the trace function from F_r to F_p . An additive character of F_r is a non zero function ψ from to be the set of complex number such that $\psi(x+y)=\psi(x)\psi(y)$ for any pair (x,y)$\in F_r^2$. For each b$\in F_r$, the function

$$\psi_b(c)=e^{2\Pi\sqrt{-1}Tr_{r/p}(bc)/p} \text{ for all } c\in F_r \qquad (2)$$

Defines an additive character of F_r. When b=0, $\psi_0(c)=1$ for all c$\in F_r$, and it is called the trivial additive character of F_r. When b=1, the character ψ_1 in (2) is called the canonical additive character of F_r . For any x $\in F_r$, one can easily check the following orthogonal property of additive characters, which we need in the sequel,

$$\frac{1}{r}\sum_{x\in F_r}\psi(ax)=\begin{cases}1, if a=0;\\ 0, if a\in F_{r.}\end{cases} \qquad (3)$$

Let r-1= lL for two positive integers l ≥ 1 and L ≥ 1, and let γ be a fixed primitive element of F_r. Define $C_i^{(L,r)}$ = $\gamma^i\langle\gamma^L\rangle$ for i=0, 1,…, L-1, where $\langle\gamma^L\rangle$ denotes the subgroup of F_r^* generated by γ^L . The cosets $C_i^{(L,r)}$ are called the cyclotomic classes of order L in F_r. The cyclotomic numbers of order L are defined by

$$(I, j)^{(L, r)} = \left|(C_i^{(L,r)}+1)\,I\,\, C_j^{(L,r)}\right|$$

for all 0≤ I, j ≤ L-1.

Cyclotomic numbers of order 2 are given in the following lemma [3] and will be needed in the sequel.

Lemma 1. The cyclotomic numbers of the order 2 are given by

$(0, 0)^{(2, r)} = \frac{(r-5)}{4}$; $(0, 1)^{(2, r)} = (1, 0)^{(2, r)} = (1, 1)^{(2, r)} = \frac{r-1}{4} if$ $r \equiv 1$ (mod 4); and

$(0, 0)^{(2, r)} = (1, 0)^{(2, r)} = (1, 1)^{(2, r)} = \frac{r-3}{4}$; $(0, 1)^{(2, r)} = \frac{r+1}{4}$; if $r \equiv 3$(mod 4).

The Gaussian period of order L are defined by

$$\eta_i^{(L,r)} = \sum_{x \in C_i^{(L,r)}} \varphi(x), \text{ i = 0, 1,\dots , L-1.}$$

Where φ is the canonical additive character of F_r.

The values of the Gaussian periods are in general way very hard to compute. However, they can be computed in a few cases. We will need the following lemmas whose proofs can be found in [3] and [8].

Lemma 2. When L=2, the Gaussian periods are given by

$$\eta_0^{(L,r)} = \begin{cases} \dfrac{-1+(-1)^{s.m-1} r^{1/2}}{2}, if p \equiv 1 (\text{mod } 4) \\ \dfrac{-1+(-1)^{s.m-1}(\sqrt{-1})^{s.m} r^{1/2}}{2}, if p \equiv 3 (\text{mod } 4) \end{cases}$$

and $$\eta_1^{(2,r)} = -1 - \eta_0^{(2,r)}.$$

Lemma 3. Let L=3, if p $\equiv 1$ (mod 3), and sm $\equiv 0$ (mod 3), then

$$\begin{cases} \eta_0^{(3,r)} = \dfrac{-1-c_1 r^{1/3}}{3} \\ \eta_1^{(3,r)} = \dfrac{-1+\frac{1}{2}(c_1+9d_1)r^{1/3}}{3} \\ \eta_2^{(3,r)} = \dfrac{-1+\frac{1}{2}(c_1-9d_1)r^{1/3}}{3} \end{cases}$$

where c_1 and d_1 are given by $4p^{s.m/3} = c_1^2 + 27 d_1^2$, $c_1 \equiv 1$ (mod 3) and gcd(c_1, p) =1.

In a special case, the so called semi-primitive case, the Gaussian periods are known and are described in the following lemma [1], [8].

Lemma 4. Assume that L>2 and there exists a positive integers j such that p^j -1 ≡ (mod L), and j is the least such. Let r = p^{2jv} for some integer v.

(a) If v, p and $(p^j+1)/L$ are all odd, then

$$\eta_{L/2}^{(L,r)} = \frac{(L-1)\sqrt{-r}-1}{L}, \ \eta_k^{(L,r)} = -\frac{\sqrt{r}+1}{L} \ fork \neq L/2.$$

(b) In all other cases,

$$\eta_0^{(L,r)} = \frac{(-1)^{v+1}(L-1)\sqrt{r}-1}{L}, \qquad \eta_k^{(L,r)} = \frac{(-1)^{v}\sqrt{r}-1}{L} \ fork \neq 0.$$

In other special case, the so called quadratic residue case, the Gaussian period can also be computed. The results below are from [2] or [5].

Lemma 5. Let 3≠ L ≡3 (mod 4) be a prime , p be a quadratic residue modulo L and $\frac{L-1}{2}.k$ = sm for some positive integer k .Let h_L be the ideal class no. of Q($\sqrt{-L}$) and a,b be integers satisfying

$$\begin{cases} a^2 + Lb^2 = 4p^{h_L} \\ a \equiv -2p\dfrac{L-1+2h_L}{4} \text{ (mod L)} \\ b > 0, p/b \end{cases} \qquad (4)$$

Then , the Gaussian period of L are given by

$$\begin{cases} \eta_0^{(l,r)} = \frac{1}{L}(P^{(K)}A^{(K)}(L-1)-1) \\ \eta_u^{(L,r)} = \eta_1 = \frac{-1}{L}(P^{(K)}A^{(K)} + P^{(K)}B^{(K)}L+1), if\,(\frac{u}{L}) = 1 \\ \eta_u^{(L,r)} = \eta_{-1} = \frac{-1}{L}(P^{(K)}A^{(K)} - P^{(K)}B^{(K)}L+1), if\,(\frac{u}{L}) = -1, \end{cases} \quad (5)$$

Where

$$\begin{cases} P^{(k)} = (-1)^{k-1} p^{\frac{k}{4}(L-1-2h_L)} \\ A^{(k)} = \mathrm{Re}(\frac{a+b\sqrt{-L}}{2})^k \\ B^{(k)} = \mathrm{Im}(\frac{a+b\sqrt{-L}}{2})^k / \sqrt{L}. \end{cases} \quad (6)$$

Remark: By using above facts about a class of cyclic codes, Cyclotomic number, Gaussians Period and the main assumptions we can compute the weight distribution of this class of cyclic codes.

REFERENCES

[1] L. D. Baumert and R.J. MacEliece, "Weights of irreducible cyclic codes", Information and control , vol. 20, no. 2, pp. 158-175, 1972.

[2] L. D. Baumert and J. Mykkeltveit, "Weight distribution of some irreducible cyclic codes", DSN Progress Report, no. 16, pp. 128-131, 1973.

[3] B. C. Berndt, R. J. Evans and K.S. Williams,Gauss and Jacobi Sums, J. Wiley and Sons Company, New York, 1997.

[4] C. Ding, Y. Liu, C. Ma and L. Zeng,“ The weight distribution of the duals of cyclic codes with two zeros", IEEE Trans. Inform. Theory, vol. 57, no. 12, pp. 8000-8006, 2011.

[5] C. Ding and J. Yang,"Hamming weights in irreducible cyclic codes", Discr. Math., vol. 14, no. 2, pp. 390-409,2008.

[6]T. Feng and K. Momihara,"Evaluation of the weight distribution of a class of cyclic codes based on index 2 Gauss sums", 2012, arXiv preprint.

[7] C. Ma, L. Zeng, Y. Liu, D. Feng and C. Ding, " The weight enumerator of a class of cyclic codes", IEEE Trans. Inform. Theory, vol. 57, no. 1, pp. 397-402, Jan. 2011.

[8] G. Myerson,"Period polynomials and Gauss sums for finite field", Acta Arith., vol. 39, pp. 251-264, 1981.

[9] B. Wang, C. Tang, Y. Qi, Y. Yang and M.Xu,"The weight distribution of cyclic codes and elliptic curve",IEEE Trans. InformTheory, vol. 58, no. 12, pp. 7253-7259, Dec. 2012.

[10]M. Xiong, "The weight distribution of a class of cyclic codes", Finite Fields Appl., vol. 18, no. 5, pp. 933-945, 2012.

[11] M. Xiong," The weight distribution of a class of cyclic codes II", to appear in Des. Codes Cryptogr.