THE WEIGHT DISTRIBUTION OF SOME MINIMAL 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 Let F_q be the finite field with q elements, p be an odd prime co-prime to q and $m \geq 1$ be an integer. In this paper, we explicitly determine the weight distribution of all the minimal cyclic codes of length p^m over F_q from their generating polynomials in a special case, when the multiplicative order of q modulo p^m is a power of p.

Keywords: Minimal cyclic codes, Cyclotomic cosets, Weight distribution.

INTRODUCTION

Let F_q be the finite field with q elements and n be a positive integer co-prime to q. A cyclic code C of length n over F_q is a linear subspace of F_q^n with the property that if $(a_0, a_1, \ldots, a_{n-1}) \in C$, then the cyclic shift $(a_{n-1}, a_0, \ldots, a_{n-2})$ is also in C. A cyclic code C of length n over F_q is also called a q-ary cyclic code of length n. We can also regard C as an ideal in the principal ideal ring $R_n := F_q[x]/\langle x^n - 1\rangle$ under the vector space isomorphism from F_q^n to R_n given by $(a_0, a_1, \ldots, a_{n-1}) \alpha\ a_0+a_1x+\ldots+a_{n-1}x^{n-1}$.

It is known that any ideal C in R_n is generated by a unique monic polynomial g(x), which is a divisor of (x^n-1), called the generating polynomial of C. A minimal ideal in R_n is called a minimal cyclic code of length n over F_q.

If C is a cyclic code of length n over F_q and $v \in C$, then the weight of v, wt(v), is defined to be the number of non-zero coordinates in v.

If $A_w^{(n)}$ denotes the number of codewords in C of weight w, $w \geq 0$, then the list $A_0^{(n)}, A_1^{(n)}, \ldots, A_n^{(n)}$ is called the weight distribution of C. The weight distribution of minimal cyclic codes has been an interesting object of study for a long time and is known in some cases. Ding [2] determined the weight distribution of q-ary minimal cyclic codes of length n provided $2 \le \frac{q^{O_n(q)}-1}{n} \le 4$, where $O_n(q)$ denotes the multiplicative order of q modulo n. He also pointed out that the weight formulas become quite messy if $\frac{q^{O_n(q)}-1}{n} \ge 5$ and therefore finding the weight distribution of q-ary minimal cyclic code is a notoriously difficult problem.

In this paper, we determine the weight distribution of all the minimal cyclic codes of length p^m over F_q, where p is an odd prime co-prime to q and m≥1 is an integer, for the case where multiplicative order of q modulo p^m is a power of p. In Section 2, we list all the minimal cyclic codes of length p^m over F_q and show that in order to determine the weight distribution of any of these codes, it is sufficient to find the weight distribution of the q-ary minimal cyclic code of length p^r, 1≤r≤m, which corresponds to the q-cyclotomic coset containing 1. In Section 3, we find the weight distribution of the minimal cyclic code of length p^r, 1≤r≤m, which corresponds to the q- cyclotomic coset containing 1 in the case defined above. Finally, in last, we also give an example.

2. Minimal cyclic codes and their weight distribution

Let F be the finite field with q elements and let n be a positive integer co-prime to q. Let α denote a primitive nth root of unity of some extension field of F_q. For any integer s, 0≤ s≤ n-1, the q -cyclotomic coset of s modulo n is the set

$$C_s := \{s, sq, sq^2, \ldots, sq^n\},$$

Where n is the least positive integer such that sq ≡s(mod n). Corresponding to the q-cyclotomic coset C_s, define

$$M_s^{(n)}(x) := \prod_{j \in C_s} (x - \alpha^j)$$

and

$M_s^{(n)}$:=the ideal in R_n generated by $\frac{x^n - 1}{M_s^{(n)}(x)}$

It is known that $M_s^{(n)}(x)$ is the minimal polynomial of α^s over F_q and $M_s^{(n)}$ is a minimal cyclic code of length n over F_q, called the q-ary minimal cyclic code of length n corresponding to the q-cyclotomic coset C_s. Furthermore, if C_{s1}, C_{s2},…, C_{sk} are all the distinct q-cyclotomic cosets modulo n, then $M_{s1}^{(n)}, M_{s2}^{(n)},..., M_{sk}^{(n)}$ are precisely all the distinct minimal cyclic codes of length n over F_q. We have the following:

Theorem 1. Let F_q be the finite field with q elements, p be an odd prime co-prime to q and m≥ 1 be an integer. Let g be a primitive root modulo p^m.

(i) The codes $\mathrm{M}_0^{(p^m)}, M_{g^k p^j}^{(p^m)}, 0 \le j \le m-1, 0 \le k \le \dfrac{\phi(p^{m-j})}{o_{p^{m-j}}(q)} - 1$, are precisely all the distinct minimal cyclic codes of length p^m over F_q, where denotes ϕ Euler's Phi function.

(ii) All the non-zero codewords in $M_0^{(p^m)}$ have weight p^m.

(iii) The code $M_{g^k p^j}^{(p^m)}$ is equivalent to the code $M_{p^j}^{(p^m)}$ and therefore they have the same weight distribution.

(iv) $M_{p^j}^{(p^m)}$ Is the repetition code of the minimal cyclic code $M_1^{(p^{m-j})}$ of length corresponding to the q-cyclotomic coset containing 1, repeated p^j times. Furthermore, for any w≥ 0,

$$A_w^{(p^m)} = \begin{cases} 0 if p^j \\ A_{w'}^{(p^{m-j})} \end{cases} \text{if p does not divide w;}$$

If $w=p^j w'$, $0 \le w' \le p^{m-j}$.

Where $A_w^{(p^m)} (resp. A_w^{p^{m-j}}), w \ge 0$, denote the weight distribution of $M_{p^j}^{(p^m)} (resp. M_1^{(p^{m-j})})$.

Proof. By [3, Lemma 1], all the distinct q-cyclotomic coset modulo p^m are given by $C_{0,} C_{g^k p^j}, 0 \le j \le m-1, 0 \le k \le \dfrac{\phi(p^{m-j})}{o_{p^{m-j}}(q)} - 1$. Therefore, (i) follows, (ii) and (iii) are obvious. The proof of (iv) is similar to that of Lemma 2 of [4].

It thus follows from the above theorem that the weight distribution of all the q-ary minimal cyclic code of length p^m can be determined from the weight distribution of q-ary minimal cyclic code $M_1^{(p^r)}$ of length p^r ($1 \le r \le m$), which corresponds to the q-cyclotomic coset containing 1.

3. The weight distribution of $M_1^{(p^R)}$, $1 \le r \le m$

We use some notations like $P_t(v)$, $L(v_1, v_2, \ldots, v_t)$, $N(v)$ which are described in [1].Throughout this section, F_q denotes the finite field with q elements , p be an odd prime co-prime to q and $m \ge 1$, an integer. Let $1 \le r \le m$ be fixed throughout. In this section, we determine the weight distribution of q-ary minimal cyclic code $M_1^{(p^r)}$ of length p^r corresponding to the q-cyclotomic coset containing 1, for the case defined above.

Theorem 3. Let F_q be the finite field with q elements, p be an odd prime co-prime to q and $m \ge 1$ be an integer. Suppose that the multiplicative order of q modulo p^m is p^d for some integer d (note that $0 \le d < m$). Then, if

(i) $r \le m-d$,the only possible non-zero weight in $M_1^{(p)^r}$ is p^r ,which is attained by all its q-1 non zero codewords.

(ii) $r > m-d$, the weight distribution $A_w^{(p^r)}, w \ge 0$, of $M_1^{(p^r)}$ is given by

$$A_w^{(p^r)} = \begin{cases} 0 & \text{if p does not divide w;} \\ \binom{p^{r-(m-d)}}{w'}(q-1)^{w'} & \end{cases}$$

If $w = p^{m-d} w', 0 \le w' \le p^{r-(m-d)}$.

In order to prove Theorem 3, we first prove the following

 ISSN: 2321-774X

Lemma 4. Let p,q,m,d be as defind in theorem 3.Then $O_{p^r}(q)$,the multiplicative order of q modulo p^r ,is given by

$$O_{p^r}(q) = \begin{cases} 1 if r \le m-d \\ p^{r-(m-d)} if r > m-d \end{cases}$$

Proof. First we assert that

$$O_{p^{(m-d)}}(q) = 1 \qquad (*)$$

To prove this, let $O_{p^{m-d}}(q) = t$ =t. Working, as in [3, Lemma 1], we get $O_{p^m}(q) = tp^d$ .As it is given that $O_{p^m}(q) = p^d$,we get t=1,which proves (*).

If r ≤ m-d, then by (*),we have $O_{p^r}(q)$ =1.for the case r >m-d, working again as in [3,Lemma 1],we obtain that $O_{p^r}(q) = p^{r-(m-d)}$ .This proves the lemma.

Lemma 5. . Let p,q,m,d be as in theorem 3.If r>m-d ,then there exists a primitive p^{m-d} th root of unity $\beta \in F_q$,such that the vectors

$$\sum_{j=0}^{p^{m-d}-1} \beta^{j+1} e_{i+jp^{r-(m-d)}} . 1 \le i \le p^{r-(m-d)},$$

Constitute a basis of $M_1^{(p^r)}$ over F_q.

Proof: It is trivial.

Proof of Theorem 3. (i) Let α be a primitive p^rth root of unity in some extension of F_q. If r ≤m-d, by lemma 4, the multiplicative order of q modulo p^r is 1. Therefore $\alpha^{q-1} = 1$, i.e., $\alpha \in F_q$ and the minimal polynomial of α over F_q is x-α. Hence $M_1^{(p^r)}$ is a 1-dimensional subspace of $F_q^{p^r}$ generated by

$\frac{x^{p^r}-1}{x-\alpha}=\alpha^{p^r-1}+\alpha^{p^r-2}x+\alpha^{p^r-3}x^2+...+\alpha x^{p^r-2}+x^{p^r-1}$ and therefore every codeword of $M_1^{(p^r)}$ is a scalar multiple of $\alpha^{p^r-1}+\alpha^{p^r-2}x+\alpha^{p^r-3}x^2+...+\alpha x^{p^r-2}+x^{p^r-1}$ .This implies that the only possible non-zero weight in $M_1^{(p^r)}$ is p^r, which is attained by all its (q-1) non-zero codewords.

(ii) If r> m-d, by lemma 5, any codeword $c\in M_1^{(p^r)}$ can be written as c= $\sum_{i=1}^{p^{r-(m-d)}}\sum_{j=0}^{p^{m-d}-1}\alpha_i\beta^{j+1}e_{i+jp^{r-(m-d)}},\alpha_i\in F_q$. Clearly, wt(c) is $p^{m-d}w'$, where w' is number of non-zero α_i's. Thus $A_w^{(p^r)}=0$ if p^{m-d} does not divide w. Moreover a code word in $M_1^{(p^r)}$ has weight $w=p^{m-d}w'$ if and only if it is a linear combination of any w' basis vectors over F_q out of a total $p^{r-(m-d)}$ basis vectors of $M_1^{(p^r)}$. This implies that there are $\binom{p^{r-(m-d)}}{w'}(q-1)^{w'}$ codewords in $M_1^{(p^r)}$ having weight $p^{m-d}w'$, which proves the theorem.

Example

Let p=3, r be a positive integer and q=7. As the multiplicative order of 7 modulo 3^m is 3^{m-1}, which is a power of 3, we apply Theorem 3 to compute the weight distribution of 7-ary minimal cyclic code $M_1^{(3^r)}$. Note that d=m-1 in this case. By Theorem 3, we see that the only possible non-zero weight in $M_1^{(3)}$ is 3, which is attained by all its 6 non-zero codewords. If r ≥ 2, the weight distribution of $M_1^{(3^r)}$ is given by

$$A_i^{(3^r)}=\begin{cases}0 \text{ if } 3 \text{ does not divide } i, \\ \binom{3^{r-1}}{j} \quad \text{if } i=3j, 0\le j\le 3^{r-1}.\end{cases}$$

REFERENCES

[1]A.Sharma, G.K.Bakshi, The weight distribution of some irreducible cyclic codes, Finite Fields Appl. (2011).

[2]C. Ding, The weight distribution of some irreducible cyclic codes, IEEE Trans. Inform, Theory 55 (3) (2009) 955-960.

[3]A.Sharma, G.K.Bakshi, V.C.Dumir, M.Raka, Cyclotomic numbers and primitive idempotents in the ringGF(q)[x]/($x^{p^n} - 1$). Finite Fields Appl. 10 (4)(2004) 653-673.

[4]A.Sharma, G.K.Bakshi, M.Raka, The weight distribution of irreducible cyclic codes of length 2^m, Finite Fields Appl. 13 (4) (2007) 1086-1095.

[5] R.Sehgal,R.L.Ward, Weight distribution of some irreducible cyclic codes, Math. Comp. 46 (173) (1986) 341-354.

[6]F.J.Macwilliams, N.J.A. Sloane,Theory of Error Correcting Codes, North-Holland, Amsterdam, 1977.