On the weight distributions of some q-ary cyclic codes

Anuradha Sharma[*]
Department of Mathematics
Indian Institute of Technology Delhi
New Delhi-110016, India

Suman Bala
Department of Mathematics
Panjab University
Chandigarh-160014, India

Abstract

Let p be an odd prime, q be a prime power coprime to p, and n be a positive integer. For any positive integer $d \leq n$, let $g_1(x) = x^{p^{n-d}} - 1$, $g_2(x) = 1 + x^{p^{n-d+1}} + x^{2p^{n-d+1}} + \cdots + x^{(p^{d-1}-1)p^{n-d+1}}$ and $g_3(x) = 1 + x^{p^{n-d}} + x^{2p^{n-d}} + \cdots + x^{(p-1)p^{n-d}}$. In this paper, we determine the weight distributions of q-ary cyclic codes of length p^n generated by the polynomials $g_1(x)$, $g_2(x)$, $g_1(x)g_2(x)$ and $g_1(x)g_3(x)$, by employing the techniques developed in Sharma & Bakshi [11].

Keywords : cyclic codes, Hamming weight, weight spectrum.

2000 Mathematics Subject Classification : 94B15.

1 Introduction

Let $\mathbb{F}_q$ be the finite field with q elements and n be a positive integer coprime to q. A cyclic code C of length n over $\mathbb{F}_q$ is a linear subspace of $\mathbb{F}_q^n$ such

[*] Corresponding Author, Email: anuradha@maths.iitd.ac.in

that that if $(a_0, a_1, \cdots, a_{n-1}) \in C$, then the word $(a_{n-1}, a_0, a_1, \cdots, a_{n-2})$ is also in C. The cyclic code C can also be viewed as an ideal in the principal ideal ring $\mathbb{R}_n = \mathbb{F}_q[x]/ < x^n - 1 >$ under the vector space isomorphism from $\mathbb{F}_q^n \mapsto \mathbb{R}_n$, given by $(a_0, a_1, \cdots, a_{n-1}) \mapsto a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$. As an ideal in $\mathbb{R}_n$, the code C is generated by a unique monic polynomial $g(x)$, which is a divisor of $x^n - 1$, called the generator polynomial of C. If the quotient polynomial $\frac{x^n-1}{g(x)}$ is an irreducible polynomial over $\mathbb{F}_q$, then the code C is called irreducible; otherwise the code C is called reducible. An important parameter associated with a code is its Hamming weight distribution, which measures error-correcting properties of the code.

The Hamming weight of a vector $v \in \mathbb{F}_q^n$, denoted by $w(v)$, is the number of non-zero coordinates in v. For a code C of length n over $\mathbb{F}_q$, if $A_i^{(n)}$ denotes the number of codewords of Hamming weight i in C, then the list $A_0^{(n)}, A_1^{(n)}, \cdots, A_n^{(n)}$ is called the Hamming weight distribution (or weight spectrum) of C. The problem of determination of the weight distribution of a code is of great practical significance due to the following reasons:

(i) One can calculate the probability of undetected errors when the code is used purely for error detection, knowing its weight distribution.

(ii) If i is the least positive integer for which $A_i^{(n)}$ is non-zero, then the code can correct up to $\frac{i-1}{2}$ errors or detect up to $i - 1$ errors.

As the ring $\mathbb{R}_n$ is semi-simple, every q-ary reducible cyclic code of length n is a direct sum of certain irreducible cyclic codes of length n over $\mathbb{F}_q$. However, no relation is known between the weight distributions of reducible and those of irreducible cyclic codes.

The problem of computing the weight distributions of cyclic codes is generally very hard and very few results are known, and that too, in some special cases.

To obtain the weight distributions of certain binary irreducible cyclic codes, MacWilliams & Seery [8] gave a procedure which involves generation of a pseudo-random sequence. They also remarked that this method can be implemented only on a powerful computer. Vlugt [14] related the problem of computing weight distributions to the evaluation of certain sums involving Gauss sums, which are generally hard to determine explicitly. To evaluate these sums in some special cases, some algorithms were given by Baumert & McEliece [3], Moisio & Väänänen [9], Fitzgerald & Yucas [6], etc., using various techniques. Using the theory developed by Baumert & McEliece [3], Segal & Ward [10] also computed the weight distributions of some binary irreducible cyclic codes.

The MacWilliams identity relates the weight distribution of a code with that of its dual code. Wang, Tang, Qi, Yang & Xu [15] obtained the weight distributions of dual codes of cyclic codes with two zeros and for a few more cases, using the theory of elliptic curves, from which one can compute the weight distribution of cyclic codes using the MacWilliams identity. They also mentioned that the weight distributions of cyclic codes are difficult to determine in general.

By computing the values and multiplicities of certain special exponential sums involving Dembowski-Ostrom polynomial, Feng & Luo [5] determined the weight distributions of a special class of linear codes. Extending this result, Luo & Feng [7] determined the weight distributions of two special classes of cyclic codes by determining the values distribution of a certain exponential sum using the theory of quadratic forms.

Aubry & Langevin [1] studied the weight divisibility of binary irreducible cyclic codes. Zanotti [16] also studied the weight behavior of irreducible cyclic balanced weight codes, (i.e., the codes in which there are the same number of codewords for each non-zero weight). Augot [2] used the theory of Grobner basis for a certain system of algebraic equations to give information about the minimum weight codewords.

The weight distribution of a p-ary cyclic code over $\mathbb{F}_p$ with non-zeros

α^{-1}, $\alpha^{-(p^k+1)}$ and $\alpha^{-(p^{3k}+1)}$, are obtained by Zeng, Hu, Jiang, Yue & Cao [17], where α is a primitive element of $\mathbb{F}_{p^n}$, p being an odd prime, and $n \geq 3$, $k \geq 1$ are integers such that $\frac{n}{\gcd(n,k)}$ is odd. Zeng, Shan & Hu [18] determined the minimum distance of a binary cyclic code with three zeros α, α^3 and α^{13} of length $2^m - 1$ and studied the weight divisibility of its dual code, where $m \geq 5$ is odd and α is a primitive element of the finite field $\mathbb{F}_{2^m}$.

Sharma, Bakshi & Raka [13] obtained the weight distribution of all the q-ary irreducible cyclic codes of length 2^m. Recently, Ding [4] determined the weight distributions of q-ary irreducible cyclic codes of length n provided $2 \leq \frac{q^{O_n(q)}-1}{n} \leq 4$, where $O_n(q)$ denotes the multiplicative order of q modulo n. He also remarked that the weight formulas become quite messy if $\frac{q^{O_n(q)}-1}{n} \geq 5$ and therefore finding the weight distribution of q-ary irreducible cyclic codes is a notoriously difficult problem. In a recent work, Sharma & Bakshi [11] obtained the weight distributions of some other classes of q-ary irreducible cyclic codes of odd prime power lengths directly from their generator polynomials.

This paper is another step towards solving the problem of determination of weight distributions of cyclic codes. In this paper, we will employ the techniques developed in [11] to determine the weight distributions of some q-ary cyclic codes of odd prime power lengths.

Throughout this paper, we let p be an odd prime and $n \geq 1$ be an integer. For $1 \leq d \leq n$, we consider the following factorization of $x^{p^n} - 1$ over $\mathbb{F}_q$:

$$x^{p^n} - 1 = g_1(x)g_2(x)g_3(x),$$

where $g_1(x) = x^{p^{n-d}} - 1$, $g_2(x) = 1 + x^{p^{n-d+1}} + x^{2p^{n-d+1}} + \cdots + x^{(p^{d-1}-1)p^{n-d+1}}$ and $g_3(x) = 1 + x^{p^{n-d}} + x^{2p^{n-d}} + \cdots + x^{(p-1)p^{n-d}}$.

Sharma & Bala [12] determined the weight distributions of the binary (reducible) cyclic codes generated by the polynomials $g_3(x)$ and $g_2(x)g_3(x)$.

The organization of this paper is as follows: In Section 2, we determine the weight distribution of the q-ary cyclic code C_1 of length p^n generated by $g_1(x)$. In Section 3, we determine the weight distribution of the q-ary cyclic code C_2 of length p^n generated by $g_2(x)$. In Section 4, we determine the weight distributions of the q-ary cyclic codes C_3 of length p^n generated by $g_1(x)g_2(x)$. In Section 5, we determine the weight distribution of the q-ary cyclic code C_4 of length p^n generated by $g_1(x)g_3(x)$, (Proofs of the results, being similar to that of Theorems 2 & 3 of [11], are omitted in this paper).

Using the results derived in this paper, one can compute the weight distributions of the dual codes of C_1, C_2, C_3 and C_4, by applying the MacWilliams identity.

2 The weight distribution of C_1

To obtain the weight distribution of the code C_1, first we need to fix some notations.

Given integers $t \geq 1$ and $\nu \geq 2$, let $P_d(\nu; t)$ denote the set of all tuples $(\nu_1, \nu_2, \cdots, \nu_t)$ of integers ν_i's satisfying $2 \leq \nu_i \leq p^d$ $(1 \leq i \leq t)$ and $\sum\limits_{i=1}^{t} \nu_i = \nu$. And for any $(\nu_1, \nu_2, \cdots, \nu_t) \in P_d(\nu; t)$, let $L_d(\nu_1, \nu_2, \cdots, \nu_t)$ denote the set of all tuples $(\ell_1, \ell_2, \cdots, \ell_t)$ of integers ℓ_j's satisfying $\ell_j \geq \nu_j - 2$ $(1 \leq j \leq t)$ and $\sum\limits_{j=1}^{t} \ell_j \leq p^d - 2t$. Further for any $(\ell_1, \ell_2, \cdots, \ell_t) \in L_d(\nu_1, \nu_2, \cdots, \nu_t)$, let $a_d(\ell_1, \ell_2, \cdots, \ell_t)$ be given by

$$\sum_{k_1=0}^{p^d-\sum_{i=1}^{t}\ell_i-2t} \; \sum_{k_2=k_1+\ell_1+2}^{p^d-\sum_{i=2}^{t}\ell_i-2(t-1)} \cdots \sum_{k_{t-1}=k_{t-2}+\ell_{t-2}+2}^{p^d-\sum_{i=t-1}^{t}\ell_i-4} \; \sum_{k_t=k_{t-1}+\ell_{t-1}+2}^{p^d-\ell_t-2} 1. \quad (1)$$

In the following theorem, we determine the weight distribution of the q-ary cyclic code C_1 generated by the polynomial $g_1(x)$.

Theorem 1 *Let p be an odd prime, $n \geq 1$ be an integer and q be a prime* *power with* $gcd(q,p) = 1$. *Let* $g_1(x) = x^{p^{n-d}} - 1$, *where* $1 \leq d \leq n$. *Then the weight distribution* $A_0^{(p^n)}, A_1^{(p^n)}, A_2^{(p^n)}, \cdots$ *of the cyclic code* C_1, *generated by* $g_1(x)$, *over* $\mathbb{F}_q$ *is given by*

$$A_w^{(p^n)} = \sum N(w_1)N(w_2)\cdots N(w_{p^{n-d}}).$$

Here the summation runs over all tuples $(w_1, w_2, \cdots, w_{p^{n-d}})$ *of non-negative integers* w_i*'s satisfying* $\sum\limits_{i=1}^{p^{n-d}} w_i = w$, *and for any* $\nu \geq 0$, $N(\nu)$ *equals*

(i) 1 if $\nu = 0$;

(ii) 0 if $\nu = 1$ *or* $\nu \geq p^d + 1$;

(iii) $\sum\limits_{t \geq 1} \sum\limits_{(\nu_1,\nu_2,\cdots,\nu_t) \in P_d(\nu;t)} \sum\limits_{(\ell_1,\ell_2,\cdots,\ell_t) \in L_d(\nu_1,\nu_2,\cdots,\nu_t)} A_d(\nu_1, \nu_2, \cdots, \nu_t; \ell_1, \ell_2, \cdots, \ell_t)$

if $2 \leq \nu \leq p^d$, *with* $A_d(\nu_1, \nu_2, \cdots, \nu_t; \ell_1, \ell_2, \cdots, \ell_t)$ *given by*

$$a_d(\ell_1, \ell_2, \cdots, \ell_t) \binom{\ell_1}{\nu_1 - 2} \binom{\ell_2}{\nu_2 - 2} \cdots \binom{\ell_t}{\nu_t - 2} (q-1)^t (q-2)^{\nu - 2t},$$

where $a_d(\ell_1, \ell_2, \cdots, \ell_t)$ *is as defined by (1).*

Proof. Proof is similar to that of Theorem 2 of [12].

3 The weight distribution of C_2

In the following theorem, we determine the weight distribution of the q-ary cyclic code C_2 of length p^n generated by the polynomial $g_2(x)$.

Theorem 2 *Let* p *be an odd prime,* n *be a positive integer and* q *be a prime power with* $gcd(q,p) = 1$. *Let* $g_2(x) = 1 + x^{p^{n-d+1}} + x^{2p^{n-d+1}} + \cdots + x^{(p^{d-1}-1)p^{n-d+1}}$, *where* d *is an integer satisfying* $1 \leq d \leq n$. *Then the weight distribution* $A_0^{(p^n)}, A_1^{(p^n)}, A_2^{(p^n)}, \cdots$ *of* C_2 *is given by*

$$A_w^{(p^n)} = \begin{cases} 0 & \text{if } p^{d-1} \text{ does not divide } w; \\ \binom{p^{n-d+1}}{j} (q-1)^j & \text{if } w = p^{d-1}j,\ 0 \leq j \leq p^{n-d+1}. \end{cases}$$

Proof. Proof is similar to that of Theorem 3 of [12].

4 The weight distribution of C_3

To compute the weight distribution of C_3, we make the following observations:

Lemma 1 *Let C and $\mathcal{D}$ be cyclic codes of length m and ℓ generated by the polynomials $g(x)$ and $h(x)$ respectively. If $g(x) = h(x)(1 + x^{\ell} + x^{2\ell} + \cdots + x^{\ell(k-1)})$, then*

(a) $m = \ell k$.

(b) C is a repetition code of $\mathcal{D}$, repeated k times.

(c) the weight distribution $A_0^{(m)}, A_1^{(m)}, \cdots, A_m^{(m)}$ of C and the weight distribution $B_0^{(\ell)}, B_1^{(\ell)}, \cdots, B_\ell^{(\ell)}$ of $\mathcal{D}$ are related by

$$A_w^{(m)} = \begin{cases} 0 & if k \nmid w; \\ B_{w'}^{(\ell)} & if w = kw',\ 0 \leq w' \leq \ell \end{cases}$$

for $0 \leq w \leq m$.

Proof. Proof is trivial.

Theorem 3 *Let p be an odd prime and $n \geq 1$ be an integer. Let $g_1(x) = x^{p^{n-d}} - 1$ and $g_2(x) = 1 + x^{p^{n-d+1}} + x^{2p^{n-d+1}} + \cdots + x^{(p^{d-1}-1)p^{n-d+1}}$, where d is an integer satisfying $1 \leq d \leq n$. Then the code C_3, generated by $g_1(x)g_2(x)$, of length p^n is a repetition code of the code $\widehat{C_1} =< g_1(x) >$ of length p^{n-d+1}, repeated p^{d-1} times. Hence the weight distribution $B_0^{(p^n)}, B_1^{(p^n)}, \cdots, B_{p^n}^{(p^n)}$ of C_3 is given by*

$$B_w^{(p^n)} = \begin{cases} 0 & if p^{d-1} \nmid w; \\ A_j^{(p^{n-d+1})} & if w = p^{d-1}j,\ 0 \leq j \leq p^{n-d+1} \end{cases}$$

for $0 \leq w \leq p^n$, where $A_0^{(p^{n-d+1})}, A_1^{(p^{n-d+1})}, A_2^{(p^{n-d+1})}, \cdots$ is the weight distribution of the code $\widehat{C_1}$, which can be computed using Theorem 1.

Proof. Proof follows from Lemma 1.

5 The weight distribution of $\mathcal{C}_4$

In the following theorem, we determine the weight distribution of the q-ary cyclic code $\mathcal{C}_4$ of length p^n.

Theorem 4 *Let p be an odd prime, $n \geq 1$ be an integer and q be a prime power with $gcd(q,p) = 1$. Let $g_1(x) = x^{p^{n-d}} - 1$ and $g_3(x) = 1 + x^{p^{n-d}} + x^{2p^{n-d}} + \cdots + x^{(p-1)p^{n-d}}$, where $1 \leq d \leq n$. Then the weight distribution $A_0^{(p^n)}, A_1^{(p^n)}, A_2^{(p^n)}, \cdots$ of the cyclic code $\mathcal{C}_4$, generated by $g_1(x)g_3(x)$, over $\mathbb{F}_q$ is given by*

$$A_w^{(p^n)} = \sum N(w_1)N(w_2)\cdots N(w_{p^{n-d+1}}).$$

Here the summation runs over all tuples $(w_1, w_2, \cdots, w_{p^{n-d+1}})$ of non-negative integers w_i's satisfying $\sum\limits_{i=1}^{p^{n-d+1}} w_i = w$, and for any $\nu \geq 0$, $N(\nu)$ equals

(i) 1 if $\nu = 0$;

(ii) 0 if $\nu = 1$ or $\nu \geq p^{d-1} + 1$;

(iii) $\sum\limits_{t\geq 1} \sum\limits_{(\nu_1,\nu_2,\cdots,\nu_t)\in P_{d-1}(\nu;t)} \sum\limits_{(\ell_1,\ell_2,\cdots,\ell_t)\in L_{d-1}(\nu_1,\nu_2,\cdots,\nu_t)} A_{d-1}(\nu_1,\nu_2,\cdots,\nu_t;\ell_1,\ell_2,\cdots,\ell_t)$

if $2 \leq \nu \leq p^{d-1}$, with $A_{d-1}(\nu_1,\nu_2,\cdots,\nu_t;\ell_1,\ell_2,\cdots,\ell_t)$ given by

$$a_{d-1}(\ell_1,\ell_2,\cdots,\ell_t)\begin{pmatrix} \ell_1 \\ \nu_1 - 2 \end{pmatrix}\begin{pmatrix} \ell_2 \\ \nu_2 - 2 \end{pmatrix}\cdots\begin{pmatrix} \ell_t \\ \nu_t - 2 \end{pmatrix}(q-1)^t(q-2)^{\nu-2t},$$

$a_{d-1}(\ell_1,\ell_2,\cdots,\ell_t)$ being equal to the sum

$$\sum_{k_1=0}^{p^{d-1}-\sum_{i=1}^t \ell_i - 2t} \quad \sum_{k_2=k_1+\ell_1+2}^{p^{d-1}-\sum_{i=2}^t \ell_i - 2(t-1)} \cdots \sum_{k_{t-1}=k_{t-2}+\ell_{t-2}+2}^{p^{d-1}-\sum_{i=t-1}^t \ell_i - 4} \quad \sum_{k_t=k_{t-1}+\ell_{t-1}+2}^{p^{d-1}-\ell_t-2} 1.$$

Proof. Since $g_1(x)g_3(x) = x^{p^{n-d+1}} - 1$, working as in Theorem 1 with d replaced by $d-1$, we get the desired result.

References

[1] Y. Aubry & P. Langevin, "On the weights of binary irreducible cyclic codes", Proc. Workshop on Coding and Cryptography, Bergen, Norway, pp. 161–169, 2005.

[2] D. Augot, "Description of minimum weight codewords of cyclic codes by algebraic systems", *Finite Fields Appl.* 2, no. 2, 138-152, 1996.

[3] L. D. Baumert & R. J. McEliece, "Weights of irreducible cyclic codes", *Information and Control* 20, pp. 158-175, 1972.

[4] C. Ding, "The weight distributions of some irreducible cyclic codes", *IEEE Trans. Inform. Theory* 55, no. 3, pp. 955-960, 2009.

[5] K. Feng & J. Luo, "Weight distributions of some reducible cyclic codes", *Finite Fields Appl.* 14, no. 2, pp. 390-409, April 2008.

[6] R. W. Fitzgerald & J. L. Yucas, "Sums of Gauss sums and weights of irreducible codes", *Finite Fields Appl.* 11, no. 1, 89–110, 2005.

[7] J. Luo & K. Feng, "On the weight distributions of two classes of cyclic codes", *IEEE Trans. Inform. Theory* 54, no. 12, pp. 5332-5344, Dec. 2008.

[8] F. J. MacWilliams & J. Seery, "The weight distributions of some minimal cyclic codes", *IEEE Trans. Inform. Theory* 27, no. 6, pp. 796-806, 1981.

[9] M. J. Moisio & K. O. Väänänen, "Two recursive algorithms for computing the weight distribution of certain irreducible cyclic codes", *IEEE Trans. Inform. Theory* 45, no. 4, pp. 1244-1249, 1999.

[10] R. Segal & R. L. Ward, "Weight distributions of some irreducible cyclic codes", *Math. Comp.* 46, no. 173, pp. 341-354, 1986.

[11] A. Sharma & G. K. Bakshi, "The weight distributions of some irreducible cyclic codes", *Finite Fields Appl.* 18, no. 1, pp. 144-159, 2012.

[12] A. Sharma & S. Bala, "The weight distributions of some binary cyclic codes," Ars Combinatoria (in press).

[13] A. Sharma, G. K. Bakshi & M. Raka, "The weight distributions of irreducible cyclic codes of length 2^m", *Finite Fields Appl.* 13, no. 4, pp. 1086-1095, 2007.

[14] M. van der Vlugt, "Hasse-Davenport curves, Gauss sums, and weight distributions of irreducible cyclic codes", *J. Number Theory* 55, no. 2, pp. 145-159, 1995.

[15] B. Wang, C. Tang, Y. Qi, Y. Yang & M. Xu, "The Weight Distributions of Cyclic Codes and Elliptic Curves", arXiv:1109.0628v1.

[16] J. P. Zanotti, "Weight behavior of irreducible cyclic BWD-codes", *Finite Fields Appl.* 2, no. 2, pp. 192-203, 1996.

[17] X. Zeng, L. Hu, W. Jiang, Q. Yue & X. Cao, "The weight distributions of a class of p-ary cyclic codes", *Finite Fields Appl.* 16, no. 1, pp. 56-73, January 2010.

[18] X. Zeng, J. Shan & L. Hu, "A triple-error-correcting cyclic code from the Gold and Kasami-Welch APN power functions", *Finite Fields Appl.*, doi:10.1016/j.ffa.2011.06.005, 2011.