Finite Fields and Their Applications 29 (2014) 202–224

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

# The weight distributions of two classes of $p$-ary cyclic codes

Dabin Zheng[a,*], Xiaoqiang Wang[a], Lei Hu[b,c], Xiangyong Zeng[a,b]

[a] Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China
[b] State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing 100093, China
[c] Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing 100048, China

ARTICLE INFO

*Article history:*
Received 6 October 2013
Received in revised form 15 April 2014
Accepted 1 May 2014
Available online 24 May 2014
Communicated by Xiang-dong Hou

*MSC:*
94B15
11T71

*Keywords:*
Cyclic code
Weight distribution
Exponential sum
Quadratic form

ABSTRACT

Let $p$ be an odd prime, and $m$, $k$ be positive integers with $m \geq 3k$. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be cyclic codes over $\mathbb{F}_p$ with parity-check polynomials $h_2(x)h_3(x)$ and $h_1(x)h_2(x)h_3(x)$, respectively, where $h_1(x)$, $h_2(x)$ and $h_3(x)$ are the minimal polynomials of $\gamma^{-1}$, $\gamma^{-(p^k+1)}$ and $\gamma^{-(p^{3k}+1)}$ over $\mathbb{F}_p$, respectively, for a primitive element $\gamma$ of $\mathbb{F}_{p^m}$. Recently, Zeng et al. (2010) obtained the weight distribution of $\mathcal{C}_2$ for $\frac{m}{\gcd(m,k)}$ being odd. In this paper, we determine the weight distribution of $\mathcal{C}_1$, and the weight distribution of $\mathcal{C}_2$ for the case that $\frac{m}{\gcd(m,k)}$ is even.



* Corresponding author.
*E-mail addresses:* dzheng@hubu.edu.cn (D. Zheng), waxiqq@163.com (X. Wang), hu@is.ac.cn (L. Hu), xzeng@hubu.edu.cn (X. Zeng).

http://dx.doi.org/10.1016/j.ffa.2014.05.001

## 1. Introduction

Let $p$ be a prime. An $[n,k]$-linear code $\mathcal{C}$ over the finite field $\mathbb{F}_p$ is a $k$-dimensional linear subspace of $\mathbb{F}_p^n$. Moreover, if $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathcal{C}$ then $\mathcal{C}$ is called a cyclic code. It is well known that any cyclic code $\mathcal{C}$ of length $n$ over $\mathbb{F}_p$ corresponds to an ideal of $\mathbb{F}_p[x]/(x^n - 1)$ and can be expressed as $\mathcal{C} = \langle g(x) \rangle$, where $g(x)$ is monic and has the least degree. The $g(x)$ is called the generator polynomial and $h(x) = (x^n - 1)/g(x)$ is referred to as the parity-check polynomial of $\mathcal{C}$ [13].

The Hamming weight of a code word $(c_0, c_1, \cdots, c_{n-1})$ in $\mathcal{C}$ is the number of nonzero $c_i$ for $0 \le i \le n-1$. Let $A_i$ denote the number of nonzero codewords with Hamming weight $i$ in $\mathcal{C}$. The sequence $(1, A_1, \cdots, A_n)$ is called the weight distribution of $\mathcal{C}$. The weight distribution of a code not only gives the error correcting ability of the code, but also allows the computation of the error probability of error detection and correction [8]. So the study of the weight distribution of a cyclic code is important in both theory and applications. In general, the weight distributions of cyclic codes are difficult to be determined and they are known only for a few special classes of cyclic codes in literature (see, for example, [1–3,6,7,11,10,12,14–16,18–24] and references therein).

Throughout this paper, let $p$ be an odd prime and $k$ and $m$ be positive integers with $m \ge 3k$. Let $h_1(x)$, $h_2(x)$ and $h_3(x)$ be the minimal polynomials of $\gamma^{-1}$, $\gamma^{-(p^k+1)}$, $\gamma^{-(p^{3k}+1)}$ over $\mathbb{F}_p$, respectively, where $\gamma$ is a primitive element of the field $\mathbb{F}_{p^m}$. To find the degree of $h_i(x)$, $i = 1, 2, 3$, we need to investigate the length of cyclotomic coset of $1, p^k + 1, p^{3k} + 1$ modulo $p^m - 1$, respectively. It is easy to see that $\deg h_1(x) = m$. We can verify that $\deg h_3(x) = \frac{m}{2}$ if $m = 6k$ otherwise $\deg h_3(x) = m$ (see Appendix A). In a similar way, $\deg h_2(x) = \frac{m}{2}$ if $m = 2k$ otherwise $\deg h_2(x) = m$. Thus, $\deg h_2(x) = m$ since $m \ge 3k$. Moreover, $h_2(x) = h_3(x)$ if and only if $m = 4k$ (see Appendix A).

In this paper we always assume that $m \ge 3k$ and $m \ne 4k$. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the cyclic codes over $\mathbb{F}_p$ of length $n = p^m - 1$ with parity-check polynomials $h_2(x)h_3(x)$ and $h_1(x)h_2(x)h_3(x)$, respectively. To determine the weight distribution of $\mathcal{C}_1$ and $\mathcal{C}_2$, it is crucial to investigate the value distribution of the following exponential sum

$$S(a,b) = \sum_{x \in \mathbb{F}_{p^m}} \chi\left(ax^{p^k+1} + bx^{p^{3k}+1}\right),$$

where $\chi$ is a canonical additive character of $\mathbb{F}_{p^m}$, which is defined by $\chi(x) = \zeta_p^{\mathrm{Tr}(x)}$, and $\mathrm{Tr}(\cdot)$ is a trace function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ and $\zeta_p = e^{\frac{2\pi i}{p}}$ is a primitive $p$-th root of unity. It is known that possible distinct values of $S(a,b)$ for $(a,b)$ running through $\mathbb{F}_{p^m}^2$ are dependent on the rank and type of the quadratic form

$$Q_{a,b}(x) = \mathrm{Tr}\left(ax^{p^k+1} + bx^{p^{3k}+1}\right).$$

For the case of $\frac{m}{\gcd(m,k)}$ being odd, Zeng et al. [21] recently proved that the rank of the quadratic form $Q_{a,b}(x)$ has only 3 possible values by nonlinear polynomial method, and then obtain the weight distribution of the cyclic code $\mathcal{C}_2$.