Optimal p-ary cyclic codes with two zeros

Yan Liu[1,2], Xiwang Cao[3]

Abstract

As a subclass of linear codes, cyclic codes have efficient encoding and decoding algorithms, so they are widely used in many areas such as consumer electronics, data storage systems and communication systems. In this paper, we give a general construction of optimal p-ary cyclic codes which leads to three explicit constructions. In addition, another class of p-ary optimal cyclic codes are presented.

Key words and phrases: cyclic code, optimal code, Sphere packing bound.

MSC: 94B15, 11T71.

1 Introduction

Let p be a prime. Denote by $\mathbb{F}_p$ the finite field with p elements. An $[n, l, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_p$ is a linear subspace of $\mathbb{F}_p^n$ with dimension l and minimum Hamming distance d. Moreover, $\mathcal{C}$ is called cyclic if any $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. It is well known that each codeword $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_p^n$ can be regarded as a polynomial $c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_p[x]/(x^n - 1)$. Then a linear code $\mathcal{C}$ in $\mathbb{F}_p^n$ is cyclic if and only if $\mathcal{C}$ is an ideal of the polynomial residue class ring $\mathbb{F}_p[x]/(x^n - 1)$. Since each ideal of the ring $\mathbb{F}_p[x]/(x^n - 1)$ is principal, every cyclic code corresponds to a principal ideal $(g(x))$ of the multiples of a polynomial $g(x)$ which is the monic polynomial of lowest degree in the ideal. $g(x)$ is called the generator polynomial, $h(x) = (x^n - 1)/g(x)$ is called the parity-check polynomial of the code $\mathcal{C}$. If $g(x)$ can be reduced to a product of r different irreducible polynomials in $\mathbb{F}_p[x]$, then $\mathcal{C}$ is described to have r zeros.

Cyclic codes have wide practical applications in many areas as they have efficient encoding and decoding algorithms. Moreover, they also have wide applications in cryptography and sequence design. So in the past few decades, much progress has been

made on cyclic codes. It is worth mentioning that in recent years, many scholars are interested in studying optimal cyclic codes over finite fields according to Sphere packing bound [11]. For example, C. Carlet et al. [3] constructed optimal ternary cyclic codes with minimum distance 4 by using perfect nonlinear monomials. In 2013, C. Ding and T. Helleseth [4] obtained some optimal ternary cyclic codes by employing almost perfect nonlinear monomials and some other monomials over $\mathbb{F}_{p^m}$. They also presented nine open problems. After that, two of the open problems were solved by N. Li et al. [13,14]. In [13], the authors also presented several classes of optimal cyclic codes with parametes $[3^m - 1, 3^m - 1 - 2m, 4]$ and $[3^m - 1, 3^m - 2 - 2m, 5]$. In 2014, Z. Zhou and C. Ding [25] gave a class of optimal ternary cyclic codes. C. Fan et al. [8] obtained a new class of optimal ternary cyclic codes with minimum distance four. Furthermore, they also discussed the weight of duals of them. What's more, L. Wang and G. Wu [19] listed four classes of optimal ternary cyclic codes. Afterwards, H. Yan et al. [22] also obtained a new class of optimal ternary cyclic codes and discussed the weight of their duals. Different from these work, G. Xu et al. [21] constructed optimal p-ary cyclic codes by making use of monomilas. More generally, C. Ding and S. Ling [5] proposed a q-polynomial method for the construction of cyclic codes. Recently, W. Fang et al. [9] used q-polynomials to construct a class of $[2(q^m - 1)/(q - 1), 2(q^m - 1)/(q - 1), 4]$ constacyclic codes which are optimal. In addition, Y. Zhou et al. [24] constructed several classes of optimal negacyclic codes $[(5^m - 1)/2, (5^m - 1)/2, 4]$ over $\mathbb{F}_5$. For information on the related topics, the reader is referred to $[1, 2, 6, 7, 10, 12, 16–18, 20, 23]$ and the references therein.

The rest of this paper is organized as follows. Some preliminaries will be introduced in Section 2. Optimal p-ary cyclic codes are discussed in Section 3. Section 4 concludes this paper.

2　Preliminaries

In this section, we will fix some basic notation for this paper and introduce p-cyclotomic cosets that will be used in subsequent sections. Throughout this paper, we will use the following notation unless otherwise stated.

- p is an odd prime.

- $n = 2(p^m - 1)/(p - 1)$, where m is a positive integer.

- π is a primitive element of $\mathbb{F}_{p^m}$.

- $\sigma \in \mathbb{F}_{p^m}$ is a primitive n-th root of unity.

- $m_i(x)$ is the minimal polynomial of σ^i over $\mathbb{F}_p$.

- $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ associated with the integer addition modulo n and integer multiplication modulo n operations.

- $\Pi = \{\sigma, \sigma^2, \cdots, \sigma^{n-1}\}$.

For any integer j, $0 \le j \le n-1$, the p-cyclotomic coset modulo n containing j is defined by

$$C_j = \{j, pj, p^2 j, \cdots, p^{l_j - 1} j\} \subset \mathbb{Z}_n$$

where l_j is the minimal positive integer such that $p^{l_j} j \equiv j \pmod{n}$, and is called the *length* of C_j which is denoted by $|C_j|$. The smallest integer in C_j is called the *coset leader* of C_j. Let Γ be the set of all coset leaders. By definition, we have $\bigcup_{j \in \Gamma} C_j = \mathbb{Z}_n$. In the following, we give a lemma about the length of cyclotomic cosets.

Lemma 2.1 ([15]) *For any integer j, $0 \le j \le n-1$ with $\gcd(j, n) = d$, the length of C_j is equal to m if $1 \le d \le 2(p+1)$.*

Let $\mathcal{C}_p(u, v)$ be the cyclic code of length n over $\mathbb{F}_p$ with generator polynomial $m_u(x) m_v(x)$ where u, v are in $\mathbb{Z}_n$ and they are not in the same cyclotomic coset. The following two lemmas are important to prove the main results of this paper.

Lemma 2.2 ([15]) *The minimum distance of $\mathcal{C}_p(u, v)$ is no less than 3 if $\gcd(v - u, n) = 1$.*

Lemma 2.3 ([15]) *Let $v \notin C_1$ and $|C_v| = m$. Then $\mathcal{C}_p(1, v)$ is optimal with parameters $[n, n - 2m, 4]$ if the following conditions are satisfied:*

1) $\gcd(v - 1, n) = 1$;

2) $v \equiv 1 \pmod{\frac{p-1}{2}}$; *and*

3) *the equations $(x + \alpha)^v \pm (x^v + \alpha) = 0$ have no solutions in Π for any α in $\mathbb{F}_p^*$.*

Remark. The conditions 1) and 2) implies that v is even and $p \equiv 3 \pmod 4$ since $n = 2(p^m - 1)/(p - 1)$ is even.

In fact, the lemma above can be reduced to the following lemma.

Lemma 2.4 *Let $v \notin C_1$ and $|C_v| = m$. Then $\mathcal{C}_p(1, v)$ is optimal with parameters $[n, n - 2m, 4]$ if the following conditions are satisfied:*

1) $\gcd(v - 1, n) = 1$;

2) $v \equiv 1 \pmod{\frac{p-1}{2}}$; *and*

3) *the equations $(x + \alpha)^v \pm (x^v + \alpha) = 0$ have no solutions in $\Pi \setminus \{\sigma^{\frac{n}{2}}\}$, i.e., $\Pi \setminus \{-1\}$ for any α in $\mathbb{F}_p^*$.*

Proof. By Lemma 2.3, we only need to prove that -1 is not a solution of $(x + \alpha)^v \pm (x^v + \alpha) = 0$ for any α in $\mathbb{F}_p^*$. Otherwise, there is an element $\alpha_0 \in \mathbb{F}_p^* \setminus \{1\}$ such that

$$(-1 + \alpha_0)^v \pm ((-1)^v + \alpha_0) = 0. \tag{1}$$

By the conditions 1) and 2), suppose $v = \frac{p-1}{2} k + 1$, then k is an odd integer. Note that $\alpha_0 - 1 \in \mathbb{F}_p^*$, then (1) becomes $(-1 + \alpha_0) \mp (1 + \alpha_0) = 0$ which is impossible. ∎

3 New optimal p-ary codes with parameters $[n, n - 2m, 4]$

In this section, we will give two new classes of p-ary cyclic codes $\mathcal{C}_p(1, v)$ with parameters $[n, n - 2m, 4]$ which are optimal according to Sphere packing bound [11].

3.1 The first class of optimal p-ary codes

First, we consider the codes $\mathcal{C}_p(1, v)$ with $v = p^k + 1$, where k is an integer such that $0 \leq k \leq m - 1$.

Theorem 3.1 *Let $m > 2$ be an odd integer. Let $v = p^k + 1$ where k is an integer such that $0 \leq k \leq m - 1$. Then $\mathcal{C}_p(1, v)$ is optimal with parameters $[n, n - 2m, 4]$ if $\gcd(m, k) = \gcd(m, p - 1) = 1$ and $\frac{p-1}{2} \mid k$.*

Proof. It is easy to check that $\gcd(v - 1, n) = 1$ and $v \notin C_1$. Note that $\frac{p-1}{2} \mid k$, $v \equiv k + 1 \equiv 1 \pmod{\frac{p-1}{2}}$. In addition, $\gcd(v, \frac{n}{2}) = \gcd(p^k + 1, \frac{p^m - 1}{p - 1}) = 1$ since $\gcd(p^k + 1, p^m - 1) = 2$ when m is odd. Hence, $\gcd(v, n) = 2$. Then $|C_v| = m$ by Lemma 2.1.

In the following, we will prove the equations $(x + \alpha)^v \pm (x^v + \alpha) = 0$ have no solutions in $\Pi \setminus \{-1\}$ for any α in $\mathbb{F}_p^*$ when $\gcd(m, p - 1) = 1$. Suppose that there is a solution x_0 in $\Pi \setminus \{-1\}$. Then

$$(x_0 + \alpha)^v = \pm(x_0^v + \alpha). \tag{2}$$

Taking $(p^k - 1)$-th power on both sides of (2), we have

$$(x_0 + \alpha)^{p^{2k} - 1} = (x_0^{p^k + 1} + \alpha)^{p^k - 1}$$

which can be reduced to

$$x_0(x_0^{p^{2k} - 1} - 1)(x_0^{p^k} - 1) = 0.$$

Hence, $x_0^{p^{2k} - 1} = 1$ or $x_0^{p^k} = 1$ which is impossible, since $\gcd(p^k, n) = 1$, $\gcd(p^{2k} - 1, n) = 2 \gcd(p - 1, m) = 2$ when $\gcd(m, k) = 1$ and $\gcd(m, p - 1) = 1$. By Lemma 2.4, the result follows. ∎

Example 3.2 *Let $p = 5$, $m = 3$, $k = 2$. Then $v = 10$ and the code $\mathcal{C}_{1,10}$ is an optimal cyclic code with parameters $[62, 50, 4]$ and generator polynomial*

$$x^6 + 3x^5 + 2x^3 + 2x^2 + 4.$$

3.2 The second class of optimal p-ary codes

In the following, we consider the codes $\mathcal{C}_p(1, v)$ with

$$(p^t - 1)v \equiv p^s - p^h \pmod{p^m - 1} \tag{3}$$

where t, s, h, m are integers such that $0 \leq t, s, h \leq m - 1$.

Lemma 3.3 *Let t, s, h, m be integers such that $0 \leq t, s, h \leq m - 1$. Then the congruence equation (3) has solutions for v such that $C_v = m$ if $\gcd(m, t) = \gcd(m, s - h) = 1$.*

Proof. Let $\tau = \gcd(p^m - 1, p^t - 1)$ and $r = \gcd(p^m - 1, p^s - p^h)$. Then $\tau = r = p - 1$ since $\gcd(m, t) = \gcd(m, s - h) = 1$. So $\tau \mid (p^s - p^h)$ which implies (3) has solutions. Since $r = \gcd(p^m - 1, (p^t - 1)v) = p - 1$, it follows that $\gcd(v, n) = 1$ or 2. Then by Lemma 2.1, $C_v = m$. ∎

By Lemma 2.4 and 3.3, we have the following result.

Theorem 3.4 *Let t, s, h be integers such that $0 \leq t, s, h \leq m - 1$ and $\gcd(m, t) = \gcd(m, s - h) = 1$ where $m > 2$ is an integer with $\gcd(m, p - 1) \mid 2$. Let v be a solution of (3). Then $\mathcal{C}_p(1, v)$ is optimal with parameters $[n, n - 2m, 4]$ if $\gcd(p^h - v, n) = \gcd(v - 1, n) = 1$ and $v \equiv 1 \pmod{\frac{p-1}{2}}$.*

Proof. First, we prove $v \notin C_1$. Suppose that $v \in C_1$, then $p^\lambda \equiv v \pmod{n}$ for some integer λ. Hence $n \mid (p^\lambda - v)$. Then v is odd since p is odd and n is even which contradicts the condition $\gcd(v - 1, n) = 1$.

Next, we prove the equations $(x + \alpha)^v \pm (x^v + \alpha) = 0$ have no solutions in $\Pi \setminus \{\sigma^{\frac{n}{2}}\}$ for any α in $\mathbb{F}_p^*$. Suppose that there is a solution $x_0 \in \Pi \setminus \{-1\}$. Then

$$(x_0 + \alpha)^v = \pm(x_0^v + \alpha). \tag{4}$$

Taking $p^t - 1$-th power on both sides of (4), we have

$$(x_0 + \alpha)^{v(p^t - 1)} = (x_0^v + \alpha)^{p^t - 1}.$$

By (3), the equation above can be reduced to

$$x_0^{p^s} + x_0^v = x_0^{vp^t} + x_0^{p^h}$$

by easy calculation. Note that $p^t v \equiv v + p^s - p^h \pmod{p^m - 1}$, then the equation above becomes

$$x_0^v(x_0^{p^s - p^h} - 1)(x_0^{p^h - v} - 1) = 0.$$

Hence, $x_0^{p^s - p^h} = 1$ or $x_0^{p^h - v} = 1$ which is impossible, since $\gcd(p^h - v, n) = 1$, $\gcd(p^s - p^h, n) = 2$ when $\gcd(m, s - h) = 1$ and $\gcd(m, p - 1) \mid 2$. ∎

By Theorem 3.4, we can have three concrete constructions as follows.

Corollary 3.5 *Let $m > 2$ be an odd integer such that $\gcd(m, p - 1) = 1$. Let $t = 1, s = 0, h = 1$ and $v = \frac{n}{2} - 1$ be a solution of (3). Then $\mathcal{C}_p(1, v)$ is optimal with parameters $[n, n - 2m, 4]$ if $\frac{p-1}{2} \mid (m - 2)$.*

Proof. It is clear that $\gcd(m, t) = \gcd(m, s - h) = 1$. $\gcd(p^h - v, n) = \gcd(p + 1 - \frac{n}{2}, n) = \gcd(p + 1, \frac{n}{2}) = 1$ since m is odd. Note that $\gcd(v - 1, n) = \gcd(\frac{n}{2} - 2, n) = 1$. Furthermore, $v - 1 \equiv m - 2 \pmod{\frac{p-1}{2}}$. Then $v \equiv 1 \pmod{\frac{p-1}{2}}$ since $\frac{p-1}{2} \mid (m - 2)$. By Theorem 3.4, the result follows. ∎

Remark. If $p = 3$ in Corollary 3.5, then the result reduced to $\mathcal{C}_3(1, \frac{3^m - 3}{2})$ is optimal if $m \geq 3$ is odd which generalizes a result in [4].

Example 3.6 *Let $p = 7$, $m = 5$. Then $v = 2800$ and the code $\mathcal{C}_{1,2800}$ is an optimal cyclic code with parameters $[5602, 5592, 4]$ and generator polynomial*

$$x^{10} + 6x^9 + 2x^8 + 2x^7 + 6x^6 + 3x^5 + x^4 + 2x^3 + 5x^2 + 6x + 6.$$

Corollary 3.7 *Let $m > 2$ be an odd integer such that $\gcd(m, p-1) = 1$. Let $t = 1, s \geq 2, h = 0$ and $v = \frac{p^s - 1}{p - 1}$ be a solution of (3). Then $\mathcal{C}_p(1, v)$ is optimal with parameters $[n, n - 2m, 4]$ if s is even, $\gcd(m, s) = \gcd(m, s - 1) = 1$ and $\frac{p-1}{2} \mid (s - 1)$.*

Proof. It is clear that $\gcd(m, t) = \gcd(m, s - h) = 1$ since $\gcd(m, s) = 1$. $\gcd(p^h - v, n) = \gcd(v - 1, n) = \gcd(\frac{p^s - p}{p - 1}, n) = \gcd(\frac{p^{s-1} - 1}{p - 1}, n) = 1$ due to s is even and $\gcd(m, s - 1) = 1$. Furthermore, $v - 1 \equiv s - 1 \pmod{\frac{p-1}{2}}$. Note that $\frac{p-1}{2} \mid (s - 1)$, then $v \equiv 1 \pmod{\frac{p-1}{2}}$. By Theorem 3.4, the result follows. ∎

Example 3.8 *Let $p = 7$, $m = 5$, $s = 4$. Then $v = 400$ and the code $\mathcal{C}_{1,400}$ is optimal with parameters $[5602, 5592, 4]$ and generator polynomial*

$$x^{10} + 6x^9 + 2x^8 + 2x^7 + 6x^6 + 3x^5 + x^4 + 2x^3 + 5x^2 + 6x + 6.$$

Corollary 3.9 *Let $m > 2$ be an odd integer such that $\gcd(m, p-1) = 1$. Let $t = 1, s \geq 2, h = 0$ and $v = \frac{n}{2} + \frac{p^s - 1}{p - 1}$ be a solution of (3). Then $\mathcal{C}_p(1, v)$ is optimal with parameters $[n, n - 2m, 4]$ if s is odd, $\gcd(m, s) = \gcd(m, s - 1) = 1$ and $\frac{p-1}{2} \mid (m + s - 1)$.*

Proof. It is clear that $\gcd(m, t) = \gcd(m, s - h) = 1$ since $\gcd(m, s) = 1$. Since m and s are both odd, $\gcd(p^h - v, n) = \gcd(v - 1, n) = \gcd(\frac{n}{2} + \frac{p^s - 1}{p - 1} - 1, n) = \gcd(\frac{n}{2} + \frac{p^s - 1}{p - 1} - 1, \frac{n}{2}) = \gcd(\frac{p^s - 1}{p - 1} - 1, \frac{n}{2})$. Note that $\gcd(m, s - 1) = 1$, then $\gcd(\frac{p^s - 1}{p - 1} - 1, \frac{n}{2}) = \gcd(\frac{p^{s-1} - 1}{p - 1} - 1, \frac{p^m - 1}{p - 1}) = 1$. Furthermore, $v - 1 \equiv m + s - 1 \pmod{\frac{p-1}{2}}$. Then $v \equiv 1 \pmod{\frac{p-1}{2}}$ due to $\frac{p-1}{2} \mid m + s - 1$. By Theorem 3.4, the result follows. ∎

Example 3.10 *Let $p = 3$, $m = 7$, $s = 3$. Then $e = 86$ and the code $\mathcal{C}_{1,86}$ is optimal with parameters $[728, 714, 4]$ and generator polynomial*

$$x^{14} + x^{13} + 2x^{10} + x^9 + 2x^8 + x^6 + x^5 + x^4 + 2x^3 + 2.$$

4   Conclusions

In this paper, we give a general construction of optimal p-ary cyclic codes which leads to three explicit constructions. In addition, another class of optimal cyclic codes $\mathcal{C}_p(1, v)$ with $v = p^k + 1$ are presented.

References

[1] P. Charpin, A. Tietäväinen, V. Zinoviev, On binary cyclic codes with distance three, *Probl. Inf. Transm.*, **33** (1997), 3-14.

[2] P. Charpin, A. Tietäväinen, V. Zinoviev, On the minimum distances of non-binary cyclic codes, *Des. Codes Crypogr.*, **17** (1999), 81-85.

[3] C. Carlet, C. Ding, J. Yuan, Linear codes from highly nonlinear functions and their secret sharing schemes, *IEEE Trans. Inf. Theory*, **51, no. 6** (2005), 2089-2102.

[4] C. Ding, T. Helleseth, Optimal ternary cyclic codes from monomials, *IEEE Trans. Inf. Theory*, **59, no. 9** (2013), 5898-5904.

[5] C. Ding, S. Ling, A q-polynomial approach to cyclic codes, *Finite Fields Appl.*, **20** (2013), 1-14.

[6] C. Ding, C. Li, N. Li, Z. Zhou, Three-weight cyclic codes and their weight distributions, *Discrete Math.*, **339, no. 2** (2016), 415-427.

[7] C. Ding, Y. Liu, C. Ma, L. Zeng, The weight distributions of the duals of cyclic codes with two zeros, *IEEE Trans. Inf. Theory*, **57, no. 12** (2011), 8000-8006.

[8] C. Fan, N. li, Z. Zhou, A class of optimal ternary cyclic codes and their duals, *Finite Fields Appl.*, **37** (2016), 193-202.

[9] W. Fang, J. Wen, F. Fu, A q-polynomial approach to constacyclic codes, *Finite Fields Appl.*, **47** (2017), 161-182.

[10] T. Feng, On cyclic codes of length $2^{2^r} - 1$ with two zeros whose dual codes have three weights, *Des. Codes Crypogr.*, **62** (2012), 253-258.

[11] W. Huffman, V. Pless, Foundamentals of error-correcting codes, *Cambridge University Press*, (2003).

[12] C. Li, Q. Yue, Weight distributions of two classes of cyclic codes with respect to two distinct order elements, *IEEE Trans. Inf. Theory*, **60, no. 1** (2014), 296-303.

[13] N. Li, C. Li, T. Helleseth, C. Ding, X. Tang, Optimal ternary cyclic codes with minimun distance four and five, *Finite Fields Appl.*, **30** (2014), 100-120.

[14] N. Li, Z. Zhou, T. Helleseth, On a conjecture about a class of optimal ternary cyclic codes, Signal Design and its Applications in Communications (IWSDA), 2015 seventh Intertional Workshop on Signal, DOI:10.1109/IWSDA.2015.7458415.

[15] D. Liao, X. Kai, S. Zhu, P. Li , A class of optimal cyclic codes with two zeros, *IEEE Commun.Lett.*, DOI: 10.1109/LCOMM.2019.2921330.

[16] J. Luo, K. Feng, Cyclic codes and sequences form generalized Coulter-Matthews function, *IEEE Trans. Inf. Theory*, **54, no. 12** (2008), 5345-5353.

[17] C. Ma, L. Zeng, Y. Liu, D. Feng, C. Ding, The weight enumerator of a class of cyclic codes, *IEEE Trans. Inf. Theory*, **57, no. 1** (2011), 397-402.

[18] M. Shi, P. Solé, Optimal p-ary codes from one-weight and two-weight codes over $\mathbb{F}_p + v\mathbb{F}_p^*$, *J Syst Sci Complex*, **28, no. 3** (2015), 679-690.

[19] L. Wang, G. Wu, Several classes of optimal ternary cyclic codes with minimal distance four, *Finite Fields Appl.*, **40** (2016), 126-137.

[20] M. Xiong, N. Li, Optimal cyclic codes with generalized Niho-type zeros and the weight distribution, *IEEE Trans. Inf. Theory*, **61, no. 9** (2015), 4914-4922.

[21] G. Xu, X. Cao, S. Xu, Optimal p-ary cyclic codes with minimum distance four from monomials, *Cryptography and Communications*, **8, no. 4** (2016), 541-554.

[22] H. Yan, Z. Zhou, X. Du, A family of optimal ternary cyclic codes from the Niho-type exponent, *Finite Fields Appl.*, **54** (2018), 101-112.

[23] X. Zeng, L. Hu, W. Jiang, The weight distribution of a class of p-ary cyclic codes, *Finite Fields Appl.*, **16, no. 1** (2010), 126-137.

[24] Y. Zhou, X. Kai, S. Zhu, J. Li, On the minimum distance of negacyclic codes with two zeros, *Finite Fields Appl.*, **55** (2019), 134-150.

[25] Z. Zhou, C. Ding, A class of three-weight cyclic codes, *Finite Fields Appl.*, **25** (2014), 79-93.