Designs, Codes and Cryptography (2023) 91:1873–1888
https://doi.org/10.1007/s10623-023-01184-x

Cyclic codes of length 5*p* with MDS symbol-pair

Fengwei Li[1,2]

Received: 8 August 2022 / Revised: 31 December 2022 / Accepted: 5 January 2023 /
Published online: 17 January 2023

Abstract
Let p be a prime with $5|(p-1)$. Let S be a set of all repeated-root cyclic codes $\mathcal{C} = \langle g(x) \rangle$, $(x^5-1)|g(x)$, of length $5p$ over a field field $\mathbb{F}_p$, whose Hamming distances are at most 7. In this paper, we present a method to find all maximum distance separable (MDS) symbol-pair codes in S. By this method we can easily obtain the results in Ma and Luo (Des Codes Cryptogr 90:121–137, 2022) and new MDS symbol-pair codes, so we remain two possible MDS symbol-pair codes for readers.

Keywords Symbol-pair code · MDS symbol-pair code · Cyclic code

Mathematics Subject Classification 94B05 · 94B15

1 Introduction

Symbol-pair codes introduced by Cassuto and Blaum [1] are designed to protect against pair errors in symbol-pair read channels. Cassuto and Litsyn [3] constructed cyclic symbol-pair codes using algebraic methods and showed that there exist symbol-pair codes whose rates are strictly higher, compared to codes for the Hamming metric with the same relative distance. Yaakobi et al. [16] studied b-symbol read channels and generalized some of the known results for symbol-pair codes to those for b-symbol read channels. Dinh et al. [9–11] investigated the symbol-pair weight distributions of repeated-root constacyclic codes etc.

Communicated by G. Ge.

The paper was supported by National Natural Science Foundation of China under Grant 12171420, Natural Science Foundation of Shandong Province under Grant ZR2021MA046, and Plateau science of Zaozhuang University.

✉ Fengwei Li
lfwzzu@126.com

1 College of Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, People's Republic of China

2 School of Mathematics and Statistics, Zaozhuang University, Zaozhuang 277160, People's Republic of China

The minimum symbol-pair distance plays an important role in determining the error correcting capability of a symbol-pair code. In general, a code over $\mathbb{F}_q$ of length n with size M and minimum pair-distance d_p is called an (n, M, d_p) symbol-pair code. An (n, M, d_p) symbol-pair code can correct up to $\lfloor (d_p - 1)/2 \rfloor$ pair errors (see [1, Proposition 3]). Chee et al. [4] gave the Singleton-type bound for symbol-pair codes relates the parameters n, M and d_p.

Lemma 1.1 [4] (Singleton Bound) *Let q be a prime power and $2 \leq d_p \leq n$. If $\mathcal{C}$ is an (n, M, d_p) symbol-pair code over $\mathbb{F}_q$, then $M \leq q^{n-d_p+2}$. If $M = q^{n-d_p+2}$, then it is called an maximum distance separable (MDS) symbol-pair code.*

A q-ary MDS symbol-pair code with parameters (n, M, d_p) is simply called an MDS (n, d_p) symbol-pair code.

There are several works that have contributed to the constructions of MDS symbol-pair codes. Chee et al. [4, 5] obtained many classes of MDS symbol-pair codes from classical MDS codes and interleaving method of Cassuto and Blaum [1]. Moreover, they obtained nontrivial MDS symbol-pair codes with length $(q^2 + 2q)/2$ by employing classical MDS codes and Eulerian graphs of certain girth. Kai et al. [12] constructed MDS symbol-pair codes with $d_p = 5$ based on constacyclic codes. Later Kai et al. [13] derived three families of MDS symbol-pair codes by using repeated-root constacyclic codes. Ding et al. [7] obtained MDS symbol-pair codes with $d_p = 6$, whose lengths from 6 to $q^2 + 1$, moreover, they found some MDS symbol-pair codes with $d_p \geq 7$ utilizing elliptic curves. Then they investigated MDS b-symbol codes [8]. Li et al. [14] gave a number of MDS symbol-pair codes with $d_p = 7$ by analyzing some linear fractional transformations. Chen et al. [6] obtained MDS symbol-pair codes with $d_p = 8$ of length $3p$ from repeated-root cyclic codes. Recently, Ma and Luo [15] constructed two classes of MDS symbol-pair codes with $d_p = 10$ and $d_p = 12$ from repeated-root cyclic codes of length $3p$ over $\mathbb{F}_p$. However, it becomes difficult to find MDS symbol-pair codes possessing comparatively large length and minimum pair-distance.

In this paper, let p be a prime with $5|(p-1)$. Let S be a set of all repeated-root cyclic codes $\mathcal{C} = \langle g(x) \rangle$, $(x^5 - 1)|g(x)$, we present a method to find MDS symbol-pair codes of length $5p$ over $\mathbb{F}_p$. Moreover, by the method we can easily obtain the results in [15]. This paper is organized as follows. In Sect. 2, basic notations and results about cyclic codes and symbol-pair codes are provided. In Sect. 3, an unique class of MDS symbol-pair codes with $d_p = 12$ among all repeated-root cyclic codes whose Hamming distance is equal to 6 are investigated. In Sect. 4, we conclude this paper with remarks.

2 Preliminaries

In this section, we review some basic notations, results on cyclic codes, and symbol-pair codes over a finite field, which will be used to prove our main results in the sequel.

2.1 Cyclic code

Let $\mathbb{F}_q$ be a finite field with q elements, where $q = p^s$, p is a prime and s is a positive integer. Let $\mathcal{C}$ be an $[n, l]$ linear code over $\mathbb{F}_q$, i.e., it is an l-dimensional subspace of $\mathbb{F}_q^n$. If for each codeword $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, $(c_{n-1}, c_0, \ldots, c_{n-2})$ is also in $\mathcal{C}$, then we call $\mathcal{C}$ a cyclic code. We identify a codeword $\mathbf{c} = (\mathbf{c_0}, \mathbf{c_1}, \ldots, \mathbf{c_{n-1}})$ in $\mathcal{C}$ with the polynomial $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$ in $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$. A code $\mathcal{C}$ of length n over

$\mathbb{F}_q$ corresponds to a subset of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Then $\mathcal{C}$ is a cyclic code if and only if the corresponding subset is an ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Hence there exists a monic divisor $g(x)$ of $x^n - 1 \in \mathbb{F}_q[x]$ such that

$$\mathcal{C} = \langle g(x)\rangle = \{f(x)g(x) \pmod{x^n - 1} : f(x) \in \mathbb{F}_q[x]\}.$$

The $g(x)$ is called the generator polynomial of $\mathcal{C}$.

A cyclic code is called simple-root cyclic code if $\gcd(n, p) = 1$ and a repeated-root cyclic code if $p|n$. Castagnoli et al. in [2] studied the Hamming distance of repeated-root cyclic codes by using polynomial algebra, they showed that the Hamming distance of a repeated-root cyclic code $\mathcal{C}$ can be expressed in terms of $d_H(\overline{\mathcal{C}}_t)$, where $\overline{\mathcal{C}}_t$ are simple-root cyclic codes fully determined by $\mathcal{C}$.

Let $\mathcal{C} = \langle g(x)\rangle$ be a repeated-root cyclic code of length ℓp^s over $\mathbb{F}_q$, where $\ell > 1$ is a positive integer such that $\gcd(\ell, p) = 1$ and s is a positive integer. Suppose that $g(x) = \Pi_{i=1}^{s} m_i(x)^{e_i}$ is the factorization of $g(x)$ over $\mathbb{F}_q$, where $m_i(x), i = 1, \ldots, s$ are distinct monic irreducible polynomials of multiplicity e_i. Fixing an integer t, $0 \le t \le p^s - 1$, we define $\overline{\mathcal{C}}_t = \langle \overline{g}_t(x)\rangle$ a simple-root cyclic code of length ℓ over $\mathbb{F}_q$, where $\overline{g}_t(x)$ is the product of those irreducible factors $m_i(x)$ with $e_i > t$. If this product is equal to $x^\ell - 1$, i.e., $\overline{\mathcal{C}}_t$ contains only the zero codeword, then $d_H(\overline{\mathcal{C}}_t) = \infty$. If all e_i satisfy $e_i \le t$, then $\overline{g}_t(x) = 1$ and $d_H(\overline{\mathcal{C}}_t) = 1$.

The following lemma will be used to determine the Hamming distance of repeated-root cyclic codes $\mathcal{C}$, which obtained from [2].

Lemma 2.1 [2] *Let $\mathcal{C} = \langle g(x)\rangle$ be a repeated-root cyclic code of length ℓp^s over $\mathbb{F}_q$, where p is a prime with* $\gcd(\ell, p) = 1$ *and s is a positive integer. Then*

$$d_H(\mathcal{C}) = \min\{P_t \cdot d_H(\overline{\mathcal{C}}_t) : t \in T\},$$

where for each $t \in T = \{t : 0 \le t \le p^s - 1\}$, $t = t_0 + t_1 p + \cdots + t_{s-1} p^{s-1}$ is the p-adic representation and $P_t = \prod_{m=0}^{s-1}(t_m + 1) = w_H((x-1)^t)$.

2.2 Symbol-pair codes

For $x = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_q^n$, the symbol-pair read vector of x is

$$\pi_p(x) = ((x_0, x_1), (x_1, x_2), \ldots, (x_{n-1}, x_0)).$$

For a code $\mathcal{C} \subset \mathbb{F}_q^n$, there is the symbol-pair code generated by $\mathcal{C}$:

$$\pi_p(\mathcal{C}) := \{\pi_p(x) : x \in \mathcal{C}\}.$$

Let $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_q^n$. Recall that the Hamming weight of the vector x is defined as $w_H(x) = |\{i : x_i \neq 0, 0 \le i \le n-1\}|$ and the Hamming distance between x and y is defined as $d_H(x, y) = |\{i : x_i \neq y_i, 0 \le i \le n-1\}|$. Define the symbol-pair weight of x as

$$w_p(x) = w_H(\pi_p(x)) = |\{(x_i, x_{i+1}) : (x_i, x_{i+1}) \neq (0, 0), 0 \le i \le n-1\}|,$$

define the symbol-pair distance between x and y as

$$\begin{aligned} d_p(x, y) &= d(\pi_p(x), \pi_p(y)) \\ &= |\{i : (x_i, x_{i+1}) \neq (y_i, y_{i+1}), 0 \le i \le n-1\}|, \end{aligned}$$

where the subscripts $i + 1$ are reduced modulo n.

An (n, M, d_p) symbol-pair code $\pi_p(\mathcal{C})$ generated by $\mathcal{C} \subset \mathbb{F}_q^n$ has size M and minimum symbol-pair distance d_p, where $d_p = \min\{d_p(x, y) : x, y \in \mathcal{C}, x \neq y\}$. Similar to the classical case, if $\mathcal{C}$ is a linear code, then the minimum symbol-pair distance of $\pi_p(\mathcal{C})$ is the smallest symbol-pair weight of nonzero codewords of $\pi_p(\mathcal{C})$, that is

$$d_p(\mathcal{C}) = \min\{w_p(x) : x \in \mathcal{C}, x \neq 0\}.$$

It is known in [1] that for any $0 < d_H(\mathcal{C}) < n$,

$$d_H(\mathcal{C}) + 1 \leq d_p(\mathcal{C}) \leq 2d_H(\mathcal{C}).$$

Let $S = \{(x_i, x_{i+1}) : 0 \leq i \leq n-1\}$ be the set from the vector x. There are two subsets of S:

$$S_0 = \{(x_i, x_{i+1}) \in S : x_i \neq 0\}$$

and

$$S_1 = \{(x_i, x_{i+1}) \in S : x_i = 0, x_{i+1} \neq 0\}.$$

It is obvious that $w_H(x) = |S_0|$ and

$$w_p(x) = |S_0| + L, \tag{2.1}$$

where $L = |S_1|$. In fact if $x = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_q^n$ is viewed as a cycle of length n, then L is the number of a sequence of 0's in the cyclic of x. For example, in $x = (1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$ and $y = (0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \in \mathbb{F}_2^{10}$, we have $L = 3$ and $L = 4$, respectively.

In this paper, we will utilize repeated-root cyclic codes to obtain a class of new MDS symbol-pair codes. A simple notation is given below.

Definition 2.2 The support of a polynomial $f(y) = \sum_{i=0}^{\ell-1} a_i y^i$ is the set

$$supp(f) = \{i : a_i \neq 0, 0 \leq i \leq \ell - 1\},$$

and denote the number of elements in $supp(f)$ by N.

3 MDS symbol-pair codes

In this section, we always assume that p is a prime number and $5|(p-1)$. There is an irreducible factorization over $\mathbb{F}_p$:

$$x^{5p} - 1 = \prod_{i=0}^{4} (x - \zeta^i)^p,$$

where ζ ia a primitive 5-th root of unity in $\mathbb{F}_p$.

Let

$$S = \left\{ \mathcal{C} = \langle g(x) \rangle : g(x) = \prod_{i=0}^{4} (x - \zeta^i)^{j_i}, p \geq j_0 \geq j_1 \geq j_2 \geq j_3 \geq j_4 \geq 1 \right\} \tag{3.1}$$

be a set of nontrivial cyclic codes with length $5p$ over $\mathbb{F}_p$.

First, we shall find MDS symbol-pair codes from all repeated-root cyclic codes of length $5p$ with $d_H(\mathcal{C}) \leq 7$ defined as (3.1).

Theorem 3.1 *If $\mathcal{C} = \langle g(x)\rangle \in S$, $d_H(\mathcal{C}) \leq 7$, and $\mathcal{C}$ is an MDS symbol-pair code. Then there is a unique possible code as follows: $d_H(\mathcal{C}) = 6$ and*

$$g(x) = (x-1)^5(x-\zeta)^2(x-\zeta^2)(x-\zeta^3)(x-\zeta^4). \tag{3.2}$$

Proof Suppose that $\mathcal{C} = \langle g(x)\rangle$ is a $[5p, l, d_H(\mathcal{C})]$ cyclic code with MDS symbol-pair. Then $d_p(\mathcal{C}) = 5p - l + 2$ with $l = 5p - \deg(g(x))$, so

$$d_p(\mathcal{C}) = \deg(g(x)) + 2. \tag{3.3}$$

In (3.1), $(x^5-1)|g(x)$ and $\deg(g(x)) \geq 5$. Recall that $d_p(\mathcal{C}) \leq 2d_H(\mathcal{C})$. Then $d_H(\mathcal{C}) \geq 4$.

By Lemma 2.1, $d_H(\mathcal{C}) = \min\{P_t \cdot d_H(\overline{\mathcal{C}}_t) : t = 1, 2, \ldots, p-1\}$, where $\overline{\mathcal{C}}_t = \langle g_t(x)\rangle$, it is clear that $g_0(x) = x^5 - 1$ and $P_0 \cdot d_H(\overline{\mathcal{C}}_0) = \infty$. So we only consider $1 \leq t \leq p-1$ and $P_t = t + 1$.

(1) Suppose that $d_H(\mathcal{C}) = 4$. Then $d_p(\mathcal{C}) \leq 8$.

If $t = 1$, then $d_H(\overline{\mathcal{C}}_1) \geq 2$ and $g_1(x)$ has at least one factor: $x - 1$, this means $j_0 \geq 2$.

If $t = 2$, then $d_H(\overline{\mathcal{C}}_2) \geq 2$ and $g_2(x)$ has at least one factor: $x - 1$, this means $j_0 \geq 3$.

Thus $j_0 \geq 3$ and $j_1 \geq j_2 \geq j_3 \geq j_4 \geq 1$ and $\deg(g(x)) \geq 7$, which is a contradiction.

(2) Suppose that $d_H(\mathcal{C}) = 5$. Then $d_p(\mathcal{C}) \leq 10$.

If $t = 1$, then $d_H(\overline{\mathcal{C}}_1) \geq 3$ and $g_1(x)$ has at least two factors: $x - 1$ and $x - \zeta$, this means $j_0 \geq 2$ and $j_1 \geq 2$.

If $t = 2$, then $d_H(\overline{\mathcal{C}}_2) \geq 2$ and $g_2(x)$ has at least one factor: $x - 1$, this means $j_0 \geq 3$.

If $t = 3$, then $d_H(\overline{\mathcal{C}}_3) \geq 2$ and $g_2(x)$ has at least one factor: $x - 1$, this means $j_0 \geq 4$.

Thus $j_0 \geq 4$, $j_1 \geq 2$, and $j_2 \geq j_3 \geq j_4 \geq 1$, and $\deg(g(x)) \geq 9$, which is a contradiction.

(3) Suppose that $d_H(\mathcal{C}) = 7$. Then $d_p(\mathcal{C}) \leq 14$.

If $t = 1$, then $d_H(\overline{\mathcal{C}}_1) \geq 4$ and $g_1(x)$ has at least three factors: $x - 1$, $x - \zeta$, and $x - \zeta^2$, this means $j_0 \geq 2$, $j_1 \geq 2$, $j_2 \geq 2$.

If $t = 2$, then $d_H(\overline{\mathcal{C}}_2) \geq 3$ and $g_2(x)$ has at least two factors: $x - 1$ and $x - \zeta$, this means $j_0 \geq 3$ and $j_1 \geq 3$.

If $t = 3$, then $d_H(\overline{\mathcal{C}}_3) \geq 2$ and $g_2(x)$ has at least one factor: $x - 1$, this means $j_0 \geq 4$.

If $t = 4$, then $d_H(\overline{\mathcal{C}}_4) \geq 2$ and $g_2(x)$ has at least one factor: $x - 1$, this means $j_0 \geq 5$.

If $t = 5$, then $d_H(\overline{\mathcal{C}}_5) \geq 2$ and $g_2(x)$ has at least one factor: $x - 1$, this means $j_0 \geq 6$.

Thus $j_0 \geq 6$, $j_1 \geq 3$, $j_2 \geq 2$, and $j_3 \geq j_4 \geq 1$, and $\deg(g(x)) \geq 13$, which is a contradiction.

(4) Suppose that $d_H(\mathcal{C}) = 6$. Then $d_p(\mathcal{C}) \leq 12$.

If $t = 1$, then $d_H(\overline{\mathcal{C}}_1) \geq 3$ and $g_1(x)$ has at least two factors: $x - 1$ and $x - \zeta$, this means $j_0 \geq 2$ and $j_1 \geq 2$.

If $t = 2$, then $d_H(\overline{\mathcal{C}}_2) \geq 2$ and $g_2(x)$ at least one factor: $x - 1$, this means $j_0 \geq 3$.

If $t = 3$ and $t = 4$, then either $g_3(x)$ or $g_4(x)$ has at least one factor: $x - 1$, this means $j_0 \geq 5$.

Thus $j_0 \geq 5$, $j_1 \geq 2$, and $j_2 \geq j_3 \geq j_4 \geq 1$. Then

$$g(x) = (x-1)^{5+j_0'}(x-\zeta)^{2+j_1'}(x-\zeta^2)^{1+j_2'}(x-\zeta^3)^{1+j_3'}(x-\zeta^4)^{1+j_4'},$$

where for $0 \leq i \leq 4$, j_i' is a positive integer, and $\deg(g(x)) = 10 + \sum_{i=0}^{4} j_i'$.

By (3.3), we have

$$d_p(\mathcal{C}) = 10 + \sum_{i=0}^{4} j_i' + 2 \leq 12,$$

it can only have

$$j_0' = j_1' = j_2' = j_3' = j_4' = 0.$$

Hence if $\mathcal{C} = \langle g(x)\rangle \in S$ and $\mathcal{C}$ is an MDS symbol-pair code, then there is a unique possible code as follows: $d_H(\mathcal{C}) = 6$ and

$$g(x) = (x-1)^5(x-\zeta)^2(x-\zeta^2)(x-\zeta^3)(x-\zeta^4).$$

This is completed the proof. □

Next, we shall verify that the code in Theorem 3.1 is just MDS symbol-pair with $d_H(\mathcal{C}) = 6$.

Suppose that $c(x)$ is a nonzero code polynomial of $\mathcal{C} = \langle g(x)\rangle \in S$. Then $g(x)|c(x)$ and $c(x)$ can be written as the form $c(x) = \sum_{i=0}^{4} x^i V_i(x^5)$, for convenience, we write

$$c(x) = (V_0(x^5), V_1(x^5), V_2(x^5), V_3(x^5), V_4(x^5)),$$

where $V_i(x^5)$ is a polynomial of x^5. Let $N_i = |supp(V_i(x^5))|, 0 \le i \le 4$, where each $supp(V_i(x^5)$ is in Definition 2.2.

By $c(1) = c(\zeta) = \cdots = c(\zeta^4) = 0$, we obtain a system of 5 equations over $\mathbb{F}_p$ as follows:

$$\begin{pmatrix} (\zeta^0)^0 & (\zeta^0)^1 & \ldots & (\zeta^0)^4 \\ (\zeta^1)^0 & (\zeta^1)^1 & \ldots & (\zeta^1)^4 \\ \vdots & \vdots & & \vdots \\ (\zeta^4)^0 & (\zeta^4)^1 & \ldots & (\zeta^4)^4 \end{pmatrix} \begin{pmatrix} V_0(1) \\ V_1(1) \\ \vdots \\ V_4(1) \end{pmatrix} = 0. \tag{3.4}$$

It is easy to check that the coefficient matrix of (3.4) is nonsingular. Then

$$V_0(1) = V_1(1) = \cdots = V_4(1) = 0,$$

it is implied that $(x^5-1)|V_i(x^5)$ for each $0 \le i \le 4$. Suppose that $V_i(x^5) = \sum_{j=0}^{n} a_j (x^5)^j$, it follows from $V_i(1) = 0$ that $a_0 = -(a_1 + \ldots + a_n)$.

Theorem 3.2 *Let $g(x)$ be defined as (3.2) and $\mathcal{C} = \langle g(x)\rangle$. Then $\mathcal{C}$ is an MDS symbol-pair codes with $d_H(\mathcal{C}) = 6$.*

Now we give some lemmas to prove Theorem 3.2.

Lemma 3.3 *If $w_H(c(x)) = 6$, then $w_p(c(x)) = 12$.*

Proof We divide into three cases to investigate $w_p(c(x))$ with $w_H(c(x)) = 6$.

Case 1: If $c(x) = (V_i(x^5), V_j(x^5))$ with $(N_i, N_j) = (4, 2)$ and $0 \le i < j \le 4$. Since $w_H(x^i V_i(x^5)) = w_H(V_i(x^5))$, without loss of generality, we consider $c(x) = (V_0(x^5), V_k(x^5))$ with $1 \le k \le 4$.

Suppose that $k \in \{2, 3\}$. Then $L = 6$ and $w_p(c(x)) = 12$.

Suppose that $k = 1$. Let $V_0(x^5) = a_0 + a_1x^{5r_1} + a_2x^{5r_2} + a_3x^{5r_3}$ with $1 \le r_1 < r_2 < r_3 < p$ and $V_1(x^5) = b_1(x^{5r_4} - 1)$, $1 \le r_4 < p$. Then

$$\begin{aligned} c(x) &= a_0 + a_1x^{5r_1} + a_2x^{5r_2} + a_3x^{5r_3} + x(-b_1 + b_1x^{5r_4}) \\ &= a_0 - b_1x + a_1x^{5r_1} + a_2x^{5r_2} + a_3x^{5r_3} + b_1x^{5r_4+1} \in \mathbb{F}_p^*[x]. \end{aligned}$$

The first, the second and the third formal derivative of $c(x)$ respectively gives

$$\begin{aligned} c^{(1)}(x) &= -b_1 + 5r_1a_1x^{5r_1-1} + 5r_2a_2x^{5r_2-1} + 5r_3a_3x^{5r_3-1} \\ &\quad +(5r_4+1)b_1x^{5r_4}, \\ c^{(2)}(x) &= 5r_1(5r_1-1)a_1x^{5r_1-2} + 5r_2(5r_2-1)a_1x^{5r_2-2} \\ &\quad +5r_3(5r_3-1)a_1x^{5r_3-2} + 5(5r_4+1)r_4b_1x^{5r_4-1}, \end{aligned}$$

and

$$c^{(3)}(x) = 5r_1(5r_1-1)(5r_1-2)a_1x^{5r_1-3} + 5r_2(5r_2-1)(5r_2-2)a_1x^{5r_2-3} \\ +5r_3(5r_3-1)(5r_3-2)a_1x^{5r_3-3} + 5(5r_4+1)(5r_4-1)r_4b_1x^{5r_4-2}.$$

Since $(x-1)^5$ and $(x-\zeta)^2$ are divisors of $c(x)$, it follows from $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = c^{(3)}(1) = 0$, note that $a_0 = -(a_1 + a_2 + a_3)$, that

$$B(a_1, a_2, a_3, b_1)^\top = 0, \tag{3.5}$$

where $B = (B_1, B_2, B_3, B_4)$, and for $1 \le i \le 3$,

$$B_i = \begin{pmatrix} r_i \\ r_i\zeta^{-1} \\ r_i(5r_i-1) \\ r_i(5r_i-1)(5r_i-2) \end{pmatrix} \tag{3.6}$$

and

$$B_4 = \begin{pmatrix} r_4 \\ r_4 \\ r_4(5r_4+1) \\ r_4(25r_4^2-1) \end{pmatrix}. \tag{3.7}$$

We make some elementary transformations:

$$B \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 5(r_2-r_1) & 5(r_3-r_1) & 5r_4+1 \\ 0 & 0 & 25(r_3-r_2)(r_3-r_1) & \lambda \end{pmatrix},$$

where $\lambda = (5r_4+1)(5r_4-5r_1-5r_2+2)$. Since $1 \le r_1 < r_2 < r_3 < p$, we can verfy that the matrix B is nonsingular, thus $a_1 = a_2 = a_3 = b_1 = 0$, which contradicts with that $b_1, a_j \in \mathbb{F}_p^*$, $0 \le j \le 3$.

Suppose that $k = 4$, that is

$$c(x) = a_0 - b_1x^4 + a_1x^{5r_1} + a_2x^{5r_2} + a_3x^{5r_3} + b_1x^{5r_4+4} \in \mathbb{F}_p^*[x],$$

similarly, by $c(1) = 0$ and $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = c^{(3)}(1) = 0$, then we derive a contradiction.

Hence if $c(x) = (V_i(x^5), V_j(x^5))$ with $(N_i, N_j) = (4, 2)$, then $w_p(c(x)) = 12$.

Case 2: If $c(x) = (V_0(x^5), V_k(x^5))$, $1 \le k \le 4$, with $(N_0, N_k) = (3, 3)$.

Let $V_0(x^5) = a_0 + a_1x^{5r_1} + a_2x^{5r_2}$ with $1 \le r_1 < r_2 < p$ and $V_k(x^5) = b_0 + b_1x^{5r_3} + b_2x^{5r_4}$ with $1 \le r_3 < r_4 < p$, where $a_0 = -a_1 - a_2$ and $b_0 = -b_1 - b_2$. Then

$$c(x) = a_0 + a_1x^{5r_1} + a_2x^{5r_2} + x^k(b_0 + b_1x^{5r_3} + b_2x^{5r_4}) \\ = a_0 + b_0x^k + a_1x^{5r_1} + a_2x^{5r_2} + b_1x^{5r_3+k} + b_2x^{5r_4+k} \in \mathbb{F}_p^*[x].$$

It is obvious that if $k \in \{2, 3\}$, then $L = 6$ and $w_p(c(x)) = 12$.

Suppose that $k = 1$. Then

$$c(x) = -(a_1 + a_2) - (b_1 + b_2)x + a_1x^{5r_1} + a_2x^{5r_2} + b_1x^{5r_3+1} + b_2x^{5r_4+1},$$

by $c^{(1)}(1)=c^{(1)}(\zeta)=c^{(2)}(1)=c^{(3)}(1)=0$, we have

$$(B_1, B_2, B_3', B_4)\begin{pmatrix}a_1\\ a_2\\ b_1\\ b_2\end{pmatrix}=0,$$

where B_1, B_2, B_4 are defined as (3.6), (3.7) and B_3' is given by changing r_4 into r_3 in B_4. Note that $1\le r_1<r_2$ and $1\le r_3<r_4$, we can obtain that the determinant of $B=(B_1, B_2, B_3', B_4)$ is not equal to 0. Hence $k=1$ is impossible.

Suppose that $k=4$, then

$$c(x)=-(a_1+a_2)-(b_1+b_2)x^4+a_1x^{5r_1}+a_2x^{5r_2}+b_1x^{5r_3+4}+b_2x^{5r_4+4},$$

similar to the argument with $k=1$, we know that $k=4$ is also impossible.

Case 3: If $c(x)=(V_0(x^5), V_i(x^5), V_j(x^5))$ with $(N_0, N_i, N_j)=(2,2,2)$ and $1\le i<j\le 4$.

Let $V_0(x^5)=a_1(x^{5r_1}-1)$, $V_i(x^5)=a_2(x^{5r_2}-1)$, and $V_j(x^5)=a_3(x^{5r_3}-1)$. Then

$$\begin{aligned}c(x)&=a_1(x^{5r_1}-1)+x^ia_2(x^{5r_2}-1)+x^ja_3(x^{5r_3}-1)\\ &=-a_1-a_2x^i-a_3x^j+a_1x^{5r_1}+a_2x^{5r_2+i}+a_3x^{5r_3+j}\in\mathbb{F}_p^*[x].\end{aligned}$$

Note that $1\le i<j\le 4$, then

$$(i,j)\in\{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}.$$

The first and the second formal derivative of $c(x)$ respectively gives

$$\begin{aligned}c^{(1)}(x)=&-ia_2x^{i-1}-ja_3x^{j-1}+5r_1a_1x^{5r_1-1}+(5r_2+i)a_2x^{5r_2+i-1}\\ &+(5r_3+j)a_3x^{5r_3+j-1},\end{aligned}$$

and

$$\begin{aligned}c^{(2)}(x)=&-i(i-1)a_2x^{i-2}-j(j-1)a_3x^{j-2}+5r_1(5r_1-1)a_1x^{5r_1-2}\\ &+(5r_2+i)(5r_2+i-1)a_2x^{5r_2+i-2}+(5r_3+j)(5r_3+j-1)a_3x^{5r_3+j-2}.\end{aligned}$$

(1) Suppose that $(i,j)=(1,2)$. Since $(x-1)^5$ and $(x-\zeta)^2$ are divisors of $c(x)$, $c^{(1)}(1)=c^{(1)}(\zeta)=c^{(2)}(1)=0$. Then

$$(B_1, B_2, B_3)\begin{pmatrix}a_1\\ a_2\\ a_3\end{pmatrix}=0, \tag{3.8}$$

where

$$B_1=\begin{pmatrix}r_1\\ r_1\zeta^{-1}\\ r_1(5r_1-1)\end{pmatrix}, B_2=\begin{pmatrix}r_2\\ r_2\\ r_2(5r_2+1)\end{pmatrix}, B_3=\begin{pmatrix}r_3\\ r_3\zeta\\ r_3(5r_3+3)\end{pmatrix}. \tag{3.9}$$

We make some elementary transformations:

$$(B_1, B_2, B_3)\sim\begin{pmatrix}1 & 0 & 0\\ 0 & 1-\zeta^{-1} & \zeta-\zeta^{-1}\\ 0 & 5(r_2-r_1)+2 & 5(r_3-r_1)+4\end{pmatrix}.$$

Note that $1 \le r_1, r_2, r_3 < p$ are positive integers, we conclude that

$$\begin{vmatrix} 1-\zeta^{-1} & \zeta-\zeta^{-1} \\ 5(r_2-r_1)+2 & 5(r_3-r_1)+4 \end{vmatrix}$$
$$= 5r_3 - 5r_1 + 4 - (5r_2 - 5r_1 + 2)\zeta + (5r_2 - 5r_3 - 2)\zeta^{-1} \neq 0.$$

The solution of Eq. (3.8) has only zero, which is a contradiction.

(2) Suppose that $(i, j) = (1, 3)$. By $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = 0$, then

$$(B_1, B_2, B_3') \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = 0, \tag{3.10}$$

where B_1, B_2 are defined as (3.9) and

$$B_3' = \begin{pmatrix} r_3 \\ r_3\zeta^2 \\ r_3(5r_3+5) \end{pmatrix}. \tag{3.11}$$

(3) Suppose that $(i, j) = (1, 4)$. By $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = 0$, then

$$(B_1, B_2, B_4) \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = 0, \tag{3.12}$$

where B_1, B_2 are defined as (3.9) and

$$B_4 = \begin{pmatrix} r_3 \\ r_3\zeta^3 \\ r_3(5r_3+7) \end{pmatrix}. \tag{3.13}$$

(4) Suppose that $(i, j) = (2, 3)$. By $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = 0$, then

$$(B_1, B_2', B_3') \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = 0, \tag{3.14}$$

where B_1, B_3' is defined as (3.9), (3.11), respectively, and

$$B_2' = \begin{pmatrix} r_2 \\ r_2\zeta \\ r_2(5r_2+3) \end{pmatrix}. \tag{3.15}$$

(5) Suppose that $(i, j) = (2, 4)$. By $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = 0$, then

$$(B_1, B_2', B_4) \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = 0, \tag{3.16}$$

where B_1, B_2', and B_4 is defined as (3.9), (3.15), and (3.13), respectively.

(6) Suppose that $(i, j) = (3, 4)$. By $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = 0$, then

$$(B_1, B_2'', B_4) \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = 0, \tag{3.17}$$

where B_1 and B_4 is defined as (3.9) and (3.13), respectively, B_2'' is replaced r_3 by r_2 in B_3' defined as (3.11).

Similar to the case $i = 1$ and $j = 2$, the solutions of (3.10), (3.12), (3.14), (3.16) and (3.17) are zero, which are contradictions.

Hence if $w_H(c(x)) = 6$, then $w_p(c(x)) = 12$. □

Lemma 3.4 *If $w_H(c(x)) = 7$, then $w_p(c(x)) \geq 12$.*

Proof We divide into three cases to investigate $w_p(c(x))$ with $w_H(c(x)) = 7$.

Case 1: If $c(x) = (V_0(x^5), V_k(x^5))$, $1 \leq k \leq 4$, with $(N_0, N_k) = (4, 3)$.

Let $V_0(x^5) = a_0 + a_1x^{5r_1} + a_2x^{5r_2} + a_3x^{5r_3}$ with $1 \leq r_1 < r_2 < r_3 < p$ and $V_k(x^5) = b_0 + b_1x^{5r_4} + b_2x^{5r_5}$ with $1 \leq r_4 < r_5 < p$. Then

$$\begin{aligned} c(x) &= a_0 + a_1x^{5r_1} + a_2x^{5r_2} + a_3x^{5r_3} + x^k(b_0 + b_1x^{5r_4} + b_2x^{5r_5}) \\ &= a_0 + b_0x^k + a_1x^{5r_1} + a_2x^{5r_2} + a_3x^{5r_3} + b_1x^{5r_4+k} + b_2x^{5r_5+k} \in \mathbb{F}_p^*[x]. \end{aligned}$$

It is obvious that if $k \in \{2, 3\}$, then $L = 7$ and $w_p(c(x)) = 14$.

Suppose that $k = 1$. Then

$$c(x) = a_0 + b_0x + a_1x^{5r_1} + a_2x^{5r_2} + a_3x^{5r_3} + b_1x^{5r_4+1} + b_2x^{5r_5+1},$$

then $w_p(c(x)) \geq 12$ except $(r_4, r_5) \in \{(r_1, r_2), (r_1, r_3), (r_2, r_3)\}$. Without loss of generality, we assume that $r_4 = r_1$ and $r_5 = r_2$. That is

$$c(x) = a_0 + b_0x + a_1x^{5r_1} + b_1x^{5r_1+1} + a_2x^{5r_2} + b_2x^{5r_2+1} + a_3x^{5r_3},$$

in this case $L = 4$ and $w_p(c(x)) = 11$. But, this is impossible. The details are the below.

The i-th $1 \leq i \leq 4$, formal derivative of $c(x)$ respectively gives

$$\begin{aligned} c^{(1)}(x) &= b_0 + 5r_1a_1x^{5r_1-1} + 5r_2a_2x^{5r_2-1} + 5r_3a_3x^{5r_3-1} \\ &\quad +(5r_1+1)b_1x^{5r_1} + (5r_2+1)b_2x^{5r_2}, \\ c^{(2)}(x) &= 5r_1(5r_1-1)a_1x^{5r_1-2} + 5r_2(5r_2-1)a_1x^{5r_2-2} + 5r_3(5r_3-1)a_1x^{5r_3-2} \\ &\quad +5(5r_1+1)r_1b_1x^{5r_1-1} + 5(5r_2+1)r_2b_2x^{5r_2-1}, \\ c^{(3)}(x) &= 5r_1(5r_1-1)(5r_1-2)a_1x^{5r_1-3} + 5r_2(5r_2-1)(5r_2-2)a_1x^{5r_2-3} \\ &\quad +5r_3(5r_3-1)(5r_3-2)a_1x^{5r_3-3} + 5(5r_1+1)(5r_1-1)r_1b_1x^{5r_1-2} \\ &\quad +5(5r_2+1)(5r_2-1)r_2b_2x^{5r_2-2}, \end{aligned}$$

and

$$\begin{aligned} c^{(4)}(x) &= 5r_1(5r_1-1)(5r_1-2)(5r_1-3)a_1x^{5r_1-4} + 5r_2(5r_2-1)(5r_2-2)(5r_2-3)a_1x^{5r_2-4} \\ &\quad +5r_3(5r_3-1)(5r_3-2)(5r_3-3)a_1x^{5r_3-4} + 5(5r_1+1)(5r_1-1)(5r_1-2)r_1b_1x^{5r_1-3} \\ &\quad +5(5r_2+1)(5r_2-1)(5r_2-2)r_2b_2x^{5r_2-3}, \end{aligned}$$

Since $(x-1)^5$ and $(x-\zeta)^2$ are divisors of $c(x)$, it follows from $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = c^{(3)}(1) = c^{(4)}(1) = 0$, note that $a_0 = -(a_1 + a_2 + a_3)$ and $b_0 = -(b_1 + b_2)$, that

$$\begin{pmatrix} B & \alpha \\ \beta & a_{55} \end{pmatrix} (a_1, a_2, a_3, b_1, b_2)^\top = 0, \tag{3.18}$$

where B is defined as (3.5), $\alpha = (r_2, r_2, r_2(5r_2+1), r_2(25r_2^2-1))^\top$, $\beta = (r_1(5r_1-1)(5r_1-2)(5r_1-3), r_2(5r_2-1)(5r_2-2)(5r_2-3), r_3(5r_3-1)(5r_3-2)(5r_3-3), r_1(25r_1^2-1)(5r_1-2))$, and $a_{55} = r_2(25r_2^2 - 1)(5r_2 - 2)$. By make some elementary transformations, note that $1 \leq r_1 < r_2 < r_3 < p$ and $1 \leq r_4 < r_5 < p$, we can check that the matrix $\begin{pmatrix} B & \alpha \\ \beta & a_{55} \end{pmatrix}$ is nonsingular, hence the solution of (3.18) is zero, which is a contradiction.

Suppose that $k = 4$. Then

$$c(x) = a_0 + b_0x^4 + a_1x^{5r_1} + a_2x^{5r_2} + a_3x^{5r_3} + b_1x^{5r_4+4} + b_2x^{5r_5+4},$$

then $w_p(c(x)) \geq 12$ except $r_1 = 1$ and $(r_4, r_5) = (r_2 - 1, r_3 - 1)$. That is

$$c(x) = a_0 + b_0x^4 + a_1x^5 + b_1x^{5r_2-1} + a_2x^{5r_2} + b_2x^{5r_3-1} + a_3x^{5r_3},$$

using arguments similar to the above, $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = c^{(3)}(1) = c^{(4)}(1) = 0$, we derive a contradiction.

Hence if $c(x) = (V_0(x^5), V_k(x^5))$, $1 \leq k \leq 4$ with $(N_0, N_k) = (4, 3)$, then $w_p(c(x)) \geq 12$.

Case 2: If $c(x) = (V_0(x^5), V_k(x^5))$, $1 \leq k \leq 4$, with $(N_0, N_k) = (5, 2)$. It is easy to see that $L \geq 5$ and $w_p(c(x)) \geq 12$.

Case 3: If $c(x) = (V_0(x^5), V_i(x^5), V_j(x^5))$ with $(N_0, N_i, N_j) = (2, 2, 3)$ and $1 \leq i < j \leq 4$.

Let $V_0(x^5) = a_1(x^{5r_1} - 1)$, $V_i(x^5) = a_2(x^{5r_2} - 1)$, and $V_j(x^5) = b_0 + b_1x^{5r_3} + b_2x^{5r_4}$, where $1 \leq r_3 < r_4 < p$. Then

$$\begin{aligned} c(x) &= a_1(x^{5r_1} - 1) + x^i a_2(x^{5r_2} - 1) + x^j(b_0 + b_1x^{5r_3} + b_2x^{5r_4}) \\ &= -a_1 - a_2x^i + b_0x^j + a_1x^{5r_1} + a_2x^{5r_2+i} + b_1x^{5r_3+j} + b_2x^{5r_4+j} \in \mathbb{F}_p^*[x]. \end{aligned}$$

Note that $1 \leq i < j \leq 4$, it is easy to check that $w_p(c(x)) \geq 12$ except

$$(i, j) \in \{(1, 2), (1, 4), (3, 4)\}.$$

In the following, we discuss the subcases: (1) $i = 1$ and $j = 2$; (2) $i = 1$ and $j = 4$; (3) $i = 3$ and $j = 4$.

The first, the second, and the third formal derivative of $c(x)$ respectively gives

$$\begin{aligned} c^{(1)}(x) &= -ia_2x^{i-1} + jb_0x^{j-1} + 5r_1a_1x^{5r_1-1} + (5r_2 + i)a_2x^{5r_2+i-1} \\ &\quad + (5r_3 + j)b_1x^{5r_3+j-1} + (5r_4 + j)b_2x^{5r_4+j-1}, \\ c^{(2)}(x) &= -i(i - 1)a_2x^{i-2} + j(j - 1)b_0x^{j-2} + 5r_1(5r_1 - 1)a_1x^{5r_1-2} \\ &\quad + (5r_2 + i)(5r_2 + i - 1)a_2x^{5r_2+i-2} + (5r_3 + j)(5r_3 + j - 1)b_1x^{5r_3+j-2} \\ &\quad + (5r_4 + j)(5r_4 + j - 1)b_2x^{5r_4+j-2}. \\ c^{(3)}(x) &= -i(i - 1)(i - 2)a_2x^{i-3} + j(j - 1)(j - 2)b_0x^{j-3} + 5r_1(5r_1 - 1)(5r_1 - 2)a_1x^{5r_1-3} \\ &\quad + (5r_2 + i)(5r_2 + i - 1)(5r_2 + i - 2)a_2x^{5r_2+i-3} \\ &\quad + (5r_3 + j)(5r_3 + j - 1)(5r_3 + j - 2)b_1x^{5r_3+j-3} \\ &\quad + (5r_4 + j)(5r_4 + j - 1)(5r_4 + j - 2)b_2x^{5r_4+j-3}. \end{aligned}$$

(1) Suppose that $(i, j) = (1, 2)$. Since $(x - 1)^5$ and $(x - \zeta)^2$ are divisors of $c(x)$, $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = c^{(3)}(1) = 0$. Then

$$(B_1, B_2, B_3, B_4)\begin{pmatrix} a_1 \\ a_2 \\ b_1 \\ b_2 \end{pmatrix} = 0, \tag{3.19}$$

where

$$B_1 = \begin{pmatrix} r_1 \\ r_1\zeta^{-1} \\ r_1(5r_1-1) \\ r_1(5r_1-1)(5r_1-2) \end{pmatrix}, B_2 = \begin{pmatrix} r_2 \\ r_2 \\ r_2(5r_2+1) \\ r_2(5r_2+1)(5r_2-1) \end{pmatrix}, \tag{3.20}$$

and

$$B_3 = \begin{pmatrix} r_3 \\ r_3\zeta \\ r_3(5r_3+3) \\ r_3(5r_3+2)(5r_3+1) \end{pmatrix}, B_4 = \begin{pmatrix} r_4 \\ r_4\zeta \\ r_4(5r_4+3) \\ r_4(5r_4+2)(5r_4+1) \end{pmatrix}. \tag{3.21}$$

Note that $r_1, r_2, r_3 < r_4 < p$ are positive integers and ζ is a primitive 5-th root of unity in $\mathbb{F}_p$, by making some elementary transformations, we obtain (B_1, B_2, B_3, B_4) is nonsingular. The solution of Eq. (3.19) has only zero, which is a contradiction.

(2) Suppose that $(i, j) = (1, 4)$. By $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = c^{(3)}(1) = 0$, then

$$(B_1, B_2, B_3', B_4') \begin{pmatrix} a_1 \\ a_2 \\ b_1 \\ b_2 \end{pmatrix} = 0, \tag{3.22}$$

where B_1, B_2 are defined as (3.20) and

$$B_3' = \begin{pmatrix} r_3 \\ r_3\zeta^3 \\ r_3(5r_3+7) \\ r_3((5r_3+5)(5r_3+4)+6) \end{pmatrix}, B_4' = \begin{pmatrix} r_4 \\ r_4\zeta^3 \\ r_4(5r_4+7) \\ r_4((5r_4+5)(5r_4+4)+6) \end{pmatrix}. \tag{3.23}$$

(3) Suppose that $(i, j) = (3, 4)$. By $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = c^{(3)}(1) = 0$, then

$$(B_1, B_2', B_3', B_4') \begin{pmatrix} a_1 \\ a_2 \\ b_1 \\ b_2 \end{pmatrix} = 0, \tag{3.24}$$

where B_1 and B_3', B_4' is defined as (3.20) and (3.23), respectively, and

$$B_2' = \begin{pmatrix} r_2 \\ r_2\zeta^2 \\ r_2(5r_2+5) \\ r_2((5r_2+1)(5r_2+5)+6) \end{pmatrix}.$$

Similar to the case $i = 1$ and $j = 2$, the solutions of (3.22) and (3.24) have zero, a contradiction.

Hence if $w_H(c(x)) = 7$, then $w_p(c(x)) \geq 12$. □

Lemma 3.5 *If $w_H(c(x)) = 8$, then $w_p(c(x)) \geq 12$.*

Proof If $w(c(x)) = 8$. Suppose that $c(x) = (V_0(x^5), V_k(x^5))$, $1 \leq k \leq 4$, with $(N_0, N_k) \in \{(2, 6), (3, 5), (4, 4)\}$. Then $w_p(c(x)) \geq 12$. We only need to consider the following two cases.

Case 1: If $c(x) = (V_0(x^5), V_i(x^5), V_j(x^5))$ with $(N_0, N_i, N_j) = (3, 3, 2)$ and $1 \le i < j \le 4$.

Let $V_0(x^5) = a_0 + a_1x^{5r_1} + a_2x^{5r_2}$ with $1 \le r_1 < r_2 < p$, $V_i(x^5) = b_0 + b_1x^{5r_3} + b_2x^{5r_4}$ with $1 \le r_3 < r_4 < p$, and $V_j(x^5) = b_3(x^{5r_5} - 1)$, where $a_0 = -a_1 - a_2$ and $b_0 = -b_1 - b_2$. Then

$$\begin{aligned} c(x) &= a_0 + a_1x^{5r_1} + a_2x^{5r_2} + x^i(b_0 + b_1x^{5r_3} + b_2x^{5r_4}) + x^j b_3(x^{5r_5} - 1) \\ &= a_0 + b_0x^i - b_3x^j + a_1x^{5r_1} + b_1x^{5r_3+i} + b_3x^{5r_3+j} + a_2x^{5r_2} + b_2x^{5r_4+i} \in \mathbb{F}_p^*[x]. \end{aligned}$$

Note that $1 \le i < j \le 4$, then

$$(i, j) \in \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}.$$

We can quickly check that $d_p(c(x)) \ge 12$ except $(i, j) \in \{(1, 2), (1, 4)\}$.

(1) Suppose that $(i, j) = (1, 2)$. We can now see that if $r_1 = r_3$ and $r_2 = r_4$, then $w_p(c(x)) = 8 + 3 = 11$; otherwise, $w_p(c(x)) \ge 12$. Without loss of generality, we assume that $r_1 = r_3 = 1$ and $r_2 = r_4 = 2$. Then

$$c(x) = a_0 + b_0x - b_3x^2 + a_1x^5 + b_1x^6 + b_3x^7 + a_2x^{10} + b_2x^{11} \in \mathbb{F}_p^*[x].$$

By $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = c^{(3)}(1) = c^{(4)}(1) = 0$, note that $a_0 = -(a_1 + a_2)$ and $b_0 = -(b_1 + b_2)$, we have

$$\begin{pmatrix} 1 & 2 & 1 & 2 & 1 \\ \zeta^4 & 2\zeta^4 & 1 & 2 & \zeta \\ 2 & 9 & 3 & 11 & 4 \\ 2 & 24 & 4 & 33 & 7 \\ 2 & 126 & 9 & 198 & 21 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = 0,$$

it is easy to verify the solution of the above equation is zero, which is a contradiction.

(2) Suppose that $(i, j) = (1, 4)$. We can easily observe that $w_p(c(x)) \ge 12$ except the case $r_1 = r_3 = 1$ and $r_2 = r_4 = 2$. In a similar way, by $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = c^{(3)}(1) = c^{(4)}(1) = 0$, this is also a contradiction.

Case 2: If $c(x) = (V_0(x^5), V_i(x^5), V_j(x^5), V_k(x^5))$ with $(N_0, N_i, N_j, N_k) = (2, 2, 2, 2)$ and $1 \le i < j < k \le 4$.

Let $V_0(x^5) = a_1(x^{5r_1} - 1)$, $V_i(x^5) = a_2(x^{5r_2} - 1)$, $V_j(x^5) = a_3(x^{5r_3} - 1)$, and $V_k(x^5) = a_4(x^{5r_4} - 1)$. Then

$$\begin{aligned} c(x) &= a_1(x^{5r_1} - 1) + a_2x^i(x^{5r_2} - 1) + a_3x^j(x^{5r_3} - 1) + a_4x^k(x^{5r_4} - 1) \\ &= -a_1 - a_2x^i - a_3x^j - a_4x^k + a_1x^{5r_1} + a_2x^{5r_2+i} + a_3x^{5r_3+j} + a_4x^{5r_4+k}. \end{aligned} \tag{3.25}$$

Note that $1 \le i < j < k \le 4$. Then

$$(i, j, k) \in \{(1, 2, 4), (1, 3, 4), (2, 3, 4), (1, 2, 3)\}.$$

(1) Suppose that $(i, j, k) = (1, 2, 4)$. It follows from (3.25) that $w_p(c(x)) \ge 12$ except $r_1 = r_2 = r_3 = 1$.

If $(i, j, k) = (1, 2, 4)$ and $r_1 = r_2 = r_3 = 1$, then

$$c(x) = -a_1 - a_2x - a_3x^2 - a_4x^4 + a_1x^5 + a_2x^6 + a_3x^7 + a_4x^{5r_4+4} \in \mathbb{F}_p^*[x].$$

By $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = c^{(3)}(1) = 0$, we have

$$\begin{pmatrix} 1 & 1 & 1 & r_4 \\ \zeta^4 & 1 & \zeta & r_4\zeta^3 \\ 4 & 6 & 8 & r_4(5r_4+7) \\ 12 & 24 & 42 & \mu \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = 0,$$

where $\mu = r_4((5r_4+4)(5r_4+5)+6)$. The solution of the above equation has only zero, which is a contradiction.

(2) Suppose that $(i, j, k) = (1, 3, 4)$. It follows from (3.25) that $w_p(c(x)) \geq 12$ except $r_1 = r_2 = 1$ and $r_3 = r_4 < p$.

If $(i, j, k) = (1, 3, 4)$, $r_1 = r_2 = 1$, and $r_3 = r_4$, then

$$c(x) = -a_1 - a_2x - a_3x^3 - a_4x^4 + a_1x^5 + a_2x^6 + a_3x^{5r_3+3} + a_4x^{5r_3+4} \in \mathbb{F}_p^*[x].$$

A similar argument to the above, by $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = c^{(3)}(1) = 0$, we conclude that if $(i, j, k) = (1, 3, 4)$ and $r_1 = r_2 = 1$ and $r_3 = r_4 < p$ is impossible.

(3) Suppose that $(i, j, k) = (2, 3, 4)$. It follows from (3.25) that $w_p(c(x)) \geq 12$ except $r_1 = 1$ and $r_2 = r_3 = r_4 < p$.

If $(i, j, k) = (2, 3, 4)$, $r_1 = 1$, and $r_2 = r_3 = r_4$, then

$$c(x) = -a_1 - a_2x^2 - a_3x^3 - a_4x^4 + a_1x^5 + a_2x^{5r_2+2} + a_3x^{5r_2+3} + a_4x^{5r_2+4} \in \mathbb{F}_p^*[x].$$

A similar argument to the above, by $c^{(1)}(1) = c^{(1)}(\zeta) = c^{(2)}(1) = c^{(3)}(1) = 0$, we know that if $(i, j, k) = (2, 3, 4)$ and $r_1 = 1$ and $r_2 = r_3 = r_4$ is impossible.

(4) Suppose that $(i, j, k) = (1, 2, 3)$. It follows from (3.25) that $w_p(c(x)) \geq 12$ except $r_1 = r_2 = r_3 < p$ or $r_2 = r_3 = r_4 < p$ or $r_1 = r_2 < p, r_3 = r_4 < p$. But the three cases are not happen.

Hence if $w_H(c(x)) = 8$ then $w_p(c(x)) \geq 12$. □

Now we are ready to complete the proof of Theorem 3.2.

Proof From Lemmas 3.3, 3.4, 3.5, we know that for $0 \neq c(x) \in \mathcal{C}$, if $6 \leq w_H(c(x)) \leq 8$, then $w_p(c(x)) \geq 12$. Furthermore, if $w_H(c(x)) \geq 9$, then by (2.1), it is easy to verify that no such codeword $c(x)$ in $\mathcal{C}$ exists such that $w_p(c(x)) < 12$. Hence we conclude that $d_p(\mathcal{C}) = 12$.

Therefore, if $g(x) = (x-1)^5(x-\zeta)^2(x-\zeta^2)(x-\zeta^3)(x-\zeta^4)$, then $\mathcal{C} = \langle g(x) \rangle$ is a $(5p, 12)$ MDS symbol-pair code. This completes the proof of Theorem 3.2. □

Example 3.6 Let $p = 11$ and $g(x) = (x-1)^5(x-3)^2(x-9)(x-5)(x-4)$. Then $\mathcal{C} = \langle g(x) \rangle$ is a $[55, 45, 6]$ cyclic code. By Theorem 3.2, its minimum symbol-pair distance is 12. The code $\mathcal{C}$ is an MDS symbol-pair code.

Example 3.7 Let $p = 31$ and $g(x) = (x-1)^5(x-4)^2(x-16)(x-2)(x-8)$. Then $\mathcal{C} = \langle g(x) \rangle$ is a $[155, 45, 6]$ cyclic code. By Theorem 3.2, its minimum symbol-pair distance is 12. The code $\mathcal{C}$ is an MDS symbol-pair code.

Suppose that $3|(p-1)$. Let

$$S' = \{\mathcal{C} = \langle g(x) \rangle : g(x) = (x-1)^{j_0}(x-\omega)^{j_1}(x-\omega^2)^{j_2}, p \geq j_0 \geq j_1 \geq j_2 \geq 1\}$$

be a set of nontrivial cyclic codes of length $3p$ over $\mathbb{F}_p$, where ω is a primitive 3-th root of unity in $\mathbb{F}_p$. From the proof of Theorem 3.1 and the results in [15], we have the following results.

Theorem 3.8 *Let $\mathcal{C} = \langle g(x)\rangle \in S'$ and $d_H(\mathcal{C}) = 5$. Then there is a unique MDS symbol-pair code of length $3p$ over $\mathbb{F}_p$ as follows:*

$$g(x) = (x-1)^4(x-\omega)^2(x-\omega^2)^2.$$

Let $\mathcal{C} = \langle g(x)\rangle \in S'$ and $d_H(\mathcal{C}) = 6$. Then there is a unique MDS symbol-pair code of length $3p$ over $\mathbb{F}_p$ as follows:

$$g(x) = (x-1)^5(x-\omega)^3(x-\omega^2)^2.$$

Furthermore, by the proof of Theorem 3.1, we know the following results.

Proposition 3.9 (1) *If $\mathcal{C} = \langle g(x)\rangle \in S$, $d_H(\mathcal{C}) = 8$, and $\mathcal{C}$ is an MDS symbol-pair code of length $5p$ over $\mathbb{F}_p$. Then there is a unique possible code as follows:*

$$g(x) = (x-1)^7(x-\zeta)^3(x-\zeta^2)^2(x-\zeta^3)(x-\zeta^4).$$

(2) *If $\mathcal{C} = \langle g(x)\rangle \in S'$, $d_H(\mathcal{C}) = 7$, and $\mathcal{C}$ is an MDS symbol-pair code of length $3p$ over $\mathbb{F}_p$. Then there is a unique possible code as follows:*

$$g(x) = (x-1)^6(x-\omega)^3(x-\omega^2)^3.$$

Question 3.10 *In Proposition 3.9, are two codes MDS symbol-pair codes?*

4 Concluding remarks

Let p be a prime and $5|(p-1)$. Let S be a set of all repeated-root cyclic codes $\mathcal{C} = \langle g(x)\rangle$, $(x^5-1)|g(x)$, of length $5p$ over a field field $\mathbb{F}_p$. In this paper, we provided a method to find MDS symbol-pair codes in S whose Hamming distance is 6. By the method we can easily obtain the results in [15] and new MDS symbol-pair codes of length ℓp over $\mathbb{F}_p$, where ℓ is a positive integer with $\ell|(p-1)$ and $(x^\ell-1)|g(x)$.

Acknowledgements The author is very grateful to the reviewers and the editor for their valuable comments and suggestions that much improved the quality of this paper.

References

1. Cassuto Y., Blaum M.: Codes for symbol-pair read channels. IEEE Trans. Inf. Theory **57**(12), 8011–8020 (2011).
2. Castagnoli G., Massey J.L., Schoeller P.A., von Seemann N.: On repeated-root cyclic codes. IEEE Trans. Inf. Theory **37**(2), 337–342 (1991).
3. Cassuto Y. Litsyn S.: Symbol-pair codes: algebraic constructions and asymptotic bounds. In: Proceedings of the IEEE International Symposium on Information Theory, Saint Petersburg, Russia, pp. 2348–2352 (2011)
4. Chee Y.M., Ji L., Kiah H.M., Wang C., Yin J.: Maximum distance separable codes for symbol-pair read channels. IEEE Trans. Inf. Theory **59**(11), 7259–7267 (2013).
5. Chee Y.M., Kiah, H.M., Wang, C.: Maximum distance separable symbol-pair codes. In: Proceedings of IEEE International Symposium Information Theory (ISIT), pp. 2886–2890 (2012).
6. Chen B., Lin L., Liu H.: Constacyclic symbol-pair codes: lower bounds and optimal constructions. IEEE Trans. Inf. Theory **63**(12), 7661–7666 (2017).
7. Ding B., Ge G., Zhang J., Zhang T., Zhang Y.: New constructions of MDS symbol-pair codes. Des. Codes Cryptogr. **86**, 841–859 (2018).
8. Ding B., Zhang T., Ge G.: Maximum distance separable codes for *b*-symbol read channels. Finite Fields Appl. **49**, 180–197 (2018).

9. Dinh H.Q., Nguyen B.T., Singh A.K., Sriboonchitta S.: On the symbol-pair distance of repeated-root constacyclic codes of prime power lengths. IEEE Trans. Inf. Theory **64**(4), 2417–2430 (2018).
10. Dinh H.Q., Wang X., Liu H., Sriboonchitta S.: On the symbol-pair distance of repeated-root constacyclic codes of length $2p^s$. Discret. Math. **342**(11), 3062–3078 (2019).
11. Dinh H.Q., Wang X., Liu H., Sriboonchitta S.: On the *b*-distance of repeated-root constacyclic codes of prime power lengths. Discret. Math. **343**(4), 111780 (2020).
12. Kai X., Zhu S., Li P.: A construction of new MDS symbol-pair codes. IEEE Trans. Inf. Theory **61**(11), 5828–5834 (2015).
13. Kai X., Zhu S., Zhao Y., Luo H., Chen Z.: New MDS symbol-pair codes from repeated-root codes. IEEE Commun. Lett. **22**(3), 462–465 (2018).
14. Li S., Ge G.: Constructions of maximum distance separable symbol-pair codes using cyclic and constacyclic codes. Des. Codes Cryptogr. **84**(3), 359–372 (2017).
15. Ma J., Luo J.: MDS symbol-pair codes from repeated-root cyclic codes. Des. Codes Cryptogr. **90**, 121–137 (2022).
16. Yaakobi E., Bruck J., Siegel P.H.: Constructions and decoding of cyclic codes over *b*-symbol read channels. IEEE Trans. Inf. Theory **62**(4), 1541–1551 (2016).