Designs, Codes and Cryptography (2022) 90:2337–2359
https://doi.org/10.1007/s10623-022-01081-9

Constructions of MDS symbol-pair codes with minimum distance seven or eight

Junru Ma[1] · **Jinquan Luo**[2]

Received: 22 November 2021 / Revised: 4 April 2022 / Accepted: 15 June 2022 /
Published online: 24 July 2022

Abstract
Symbol-pair codes are proposed to guard against pair-errors in symbol-pair read channels. The minimum symbol-pair distance plays a vital role in determining the error-correcting capability and the constructions of symbol-pair codes with largest possible minimum symbol-pair distance is of great importance. Maximum distance separable (MDS) symbol-pair codes are optimal in the sense that such codes can acheive the Singleton bound. In this paper, for length $5p$, two new classes of MDS symbol-pair codes with minimum symbol-pair distance seven or eight are constructed by utilizing repeated-root cyclic codes over $\mathbb{F}_p$, where p is a prime. In addition, we derive a class of MDS symbol-pair codes with minimum symbol-pair distance seven and length $4p$.

Keywords MDS symbol-pair codes · Minimum symbol-pair distance · Constacyclic codes · Repeated-root cyclic codes

Mathematics Subject Classification 94B15 · 94B05

1 Introduction

With the development of modern high density data storage systems, symbol-pair code was proposed by Cassuto and Blaum to combat against pair-errors over symbol-pair read channels in [1, 2]. They also showed that a code $\mathcal{C}$ with minimum symbol-pair distance d_p can correct up to $\lfloor (d_p-1)/2 \rfloor$ symbol-pair errors [1, 2]. Later, Cassuto and Litsyn [3] showed that

Communicated by G. Ge.

✉ Jinquan Luo
luojinquan@mail.ccnu.edu.cn

Junru Ma
majunru@hubu.edu.cn

1 Faculty of Mathematics and Statistics, Hubei Key Laboratory of Applied Mathematics, Hubei University, Wuhan 430062, Hubei, China

2 School of Mathematics and Statistics, Hubei Key Laboratory of Mathematical Sciences, Central China Normal University, Wuhan 430079, Hubei, China

codes for correcting pair-errors exist with strictly higher rates compared to codes for the Hamming metric with the same relative distance. In [6], Chee, Kiah and Wang established a Singleton-type bound on symbol-pair codes. Similar to classical codes, symbol-pair codes meeting the Singleton-type bound are called MDS symbol-pair codes and the error-correcting capability of MDS symbol-pair codes is optimal. Later, Ding, Zhang and Ge extended the Singleton-type bound to the b-symbol case in [9].

Many attempts have been made in the constructions of MDS symbol-pair codes. In [17], Kai, Zhu and Li provided MDS symbol-pair codes with length q^2+q+1 through constacyclic codes over $\mathbb{F}_q$. Later, Li and Ge [19] generalized the results in [17] and they also constructed a number of MDS symbol-pair codes with minimum symbol-pair distance seven by analyzing certain linear fractional transformations. Shortly afterwards, Chen, Lin and Liu [7] constructed several MDS symbol-pair codes with length $3p$ from repeated-root cyclic codes over $\mathbb{F}_p$. In 2018, Ding et al. [8] obtained some MDS symbol-pair codes over $\mathbb{F}_q$ with larger minimum symbol-pair distance based on elliptic curves and the lengths of these codes are bounded by $q+2\sqrt{q}$. In the same year, Kai et al. [18] constructed three classes of MDS symbol-pair codes using repeated-root constacyclic codes over $\mathbb{F}_p$, see Table 1. Recently, some new results on constructing symbol-pair codes were presented in [12, 14, 21]. Moreover, some decoding algorithms of symbol-pair codes were proposed by various researchers in [15, 20, 25, 27, 28] and the symbol-pair weight distributions of some linear codes over finite fields were studied in [10, 11, 13, 22, 26] and the references therein.

In Table 1, we summarize some known MDS symbol-pair codes from constacyclic codes.

Table 1 Some known MDS symbol-pair codes from constacyclic codes

Values of $(n, d_p)_q$	Conditions	References
$(n, 5)_q$	$n \mid \left(q^2+q+1\right)$	[17],[19]
$(n, 6)_q$	$n \mid \left(q^2+1\right)$	[17],[19]
$(n, 6)_q$	$n \mid \left(q^2-1\right)$, n odd or n even and $v_2(n) < v_2\left(q^2-1\right)$	[19]
$(n, 6)_q$	$q \geq 3,\ n \geq q+4,\ n \mid \left(q^2-1\right)$	[7]
$(lp, 5)_p$	$p \geq 5,\ l > 2,\ \gcd(l, p)=1,\ l \mid (p-1)$	[7]
$\left(p^2+p, 6\right)_p$	$p \geq 3$	[18]
$\left(2p^2-2p, 6\right)_p$	$p \geq 3$	[18]
$(3p, 6)_p$	$p \geq 5$	[7]
$(3p, 7)_p$	$p \geq 5$	[7]
$(3p, 8)_p$	$3 \mid (p-1)$	[7]
$(3p, 10)_p$	$3 \mid (p-1)$	[21]
$(3p, 12)_p$	$3 \mid (p-1)$	[21]
$(4p, 7)_p$	$p \equiv 3 \pmod 4$	[18]
$(4p, 7)_p$	$p \equiv 1 \pmod 4$	Theorem 3
$(5p, 7)_p$	$5 \mid (p-1),\ p \neq 41$	Theorem 1
$(5p, 8)_p$	$5 \mid (p-1)$	Theorem 2
	Where q is a power of a prime p.	

Observe that there exists only one class of codes with length $5p$ and minimum symbol-pair distance five in Table 1. The constructions of symbol-pair codes with comparatively large minimum symbol-pair distance is an interesting topic. This paper focuses on further constructions of MDS symbol-pair codes with length $5p$. Precisely, two new classes of MDS symbol-pair codes with minimum symbol-pair distance seven or eight are constructed by utilizing repeated-root cyclic codes over $\mathbb{F}_p$. In addition, for $n = 4p$, we derive a class of MDS symbol-pair codes with $d_p = 7$, which generalizes the result in [18].

The remainder of this paper is organized as follows. In Section 2, we introduce some basic notation and results on symbol-pair codes and constacyclic codes. By exploiting repeated-root cyclic codes, for length $5p$, two new classes of MDS symbol-pair codes with minimum symbol-pair distance seven or eight are constructed in Section 3.1 and a class of MDS symbol-pair codes with length $4p$ is presented in Section 3.2. Section 4 concludes the paper.

2 Preliminaries

In this section, we introduce some notations and auxiliary tools on symbol-pair codes and constacyclic codes, which will be used to prove our main results in the sequel.

2.1 Symbol-pair codes

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a prime power. Let n be a positive integer and $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1})$ be a vector in $\mathbb{F}_q^n$. Then the *symbol-pair read vector* of $\mathbf{x}$ is

$$\pi(\mathbf{x}) = ((x_0,\ x_1),\ (x_1,\ x_2),\cdots,(x_{n-2},\ x_{n-1}),\ (x_{n-1},\ x_0)).$$

Obviously, each vector $\mathbf{x} \in \mathbb{F}_q^n$ has a unique pair representation $\pi(\mathbf{x})$. Recall that the *Hamming weight* of $\mathbf{x}$ is

$$w_H(\mathbf{x}) = \left|\left\{i \in \mathbb{Z}_n \,\middle|\, x_i \neq 0\right\}\right|$$

where $\mathbb{Z}_n$ denotes the residue class ring $\mathbb{Z}/n\mathbb{Z}$. Correspondingly, the *symbol-pair weight* of $\mathbf{x}$ is

$$w_p(\mathbf{x}) = \left|\left\{i \in \mathbb{Z}_n \,\middle|\, (x_i,\ x_{i+1}) \neq (0,\ 0)\right\}\right|.$$

For any two vectors $\mathbf{x},\ \mathbf{y} \in \mathbb{F}_q^n$, the *symbol-pair distance* from $\mathbf{x}$ to $\mathbf{y}$ is defined as

$$d_p\left(\mathbf{x},\ \mathbf{y}\right) = \left|\left\{i \in \mathbb{Z}_n \,\middle|\, (x_i,\ x_{i+1}) \neq (y_i,\ y_{i+1})\right\}\right|.$$

A code $\mathcal{C}$ over $\mathbb{F}_q$ of length n is a nonempty subsets of $\mathbb{F}_q^n$. Elements of $\mathcal{C}$ are called *codewords* in $\mathcal{C}$. The *minimum symbol-pair distance* of $\mathcal{C}$ is

$$d_p(\mathcal{C}) = \min\left\{d_p\left(\mathbf{x},\ \mathbf{y}\right) \,\middle|\, \mathbf{x},\ \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\right\}$$

and we refer such a code as an $\left(n,\ d_p(\mathcal{C})\right)_q$ *symbol-pair code*. A well-known relationship between $d_H(\mathcal{C})$ and $d_p(\mathcal{C})$ in [1, 2] states that for any $0 < d_H(\mathcal{C}) < n$,

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

The following lemma reveals a connection between the symbol-pair distance and the Hamming distance of a code $\mathcal{C}$.

Lemma 1 [1, 2] *For any* $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ *with* $\mathbf{x} = (x_0, \cdots, x_{n-1})$ *and* $\mathbf{y} = (y_0, \cdots, y_{n-1})$. *Define* $S = \{i \in \mathbb{Z}_n \mid x_i \neq y_i\}$. *Let* $S = \bigcup_{i=1}^{L} S_i$ *be a partition of* S, *which satisfies:*

(1) *the elements of each subset S_i are consecutive in the sense of modulo n;*
(2) *for any different $i,\ j \in [1, L]$ and $a \in S_i,\ b \in S_j$, a and b are not consecutive.*

Then

$$d_p\left(\mathbf{x},\ \mathbf{y}\right) = d_H\left(\mathbf{x},\ \mathbf{y}\right) + L.$$

In contrast to classical error-correcting codes, the size of symbol-pair codes satisfies the following Singleton bound.

Lemma 2 [5] *Let $q \geq 2$ and $2 \leq d_p \leq n$. If $\mathcal{C}$ is a symbol-pair code with length n and minimum symbol-pair distance d_p, then $|\mathcal{C}| \leq q^{n-d_p+2}$.*

The symbol-pair code achieving the Singleton bound is called a *maximum distance separable* (MDS) symbol-pair code.

2.2 Constacyclic codes

In this subsection, we introduce some notations of constacyclic codes. For a fixed nonzero element η in $\mathbb{F}_q$, the η-constacyclic shift τ_η on $\mathbb{F}_q^n$ is

$$\tau_\eta\left(x_0,\ x_1, \cdots, x_{n-1}\right) = \left(\eta\, x_{n-1},\ x_0, \cdots, x_{n-2}\right).$$

A linear code $\mathcal{C}$ is called an *η-constacyclic code* if $\tau_\eta\left(\mathbf{c}\right) \in \mathcal{C}$ for any codeword $\mathbf{c} \in \mathcal{C}$. An η-constacyclic code is a *cyclic code* if $\eta = 1$ and a *negacyclic code* if $\eta = -1$. It should be noted that each codeword $\mathbf{c} = \left(c_0,\ c_1, \cdots, c_{n-1}\right) \in \mathcal{C}$ is identical to its polynomial representation

$$c(x) = c_0 + c_1\, x + \cdots + c_{n-1}\, x^{n-1}.$$

For convenience, we always regard the codeword $\mathbf{c}$ in $\mathcal{C}$ as the corresponding polynomial $c(x)$ in this paper. Notice that a linear code $\mathcal{C}$ is an η-constacyclic code if and only if it is an ideal of the principle ideal ring $\mathbb{F}_q[x]/\langle x^n - \eta\rangle$. As a consequence, there exists a unique monic divisor $g(x) \in \mathbb{F}_q[x]$ of $x^n - \eta$ such that

$$\mathcal{C} = \langle g(x)\rangle = \left\{ f(x)\, g(x) \left(\mathrm{mod}\left(x^n - \eta\right)\right) \,\middle|\, f(x) \in \mathbb{F}_q\left[x\right]\right\}.$$

The polynomial $g(x)$ is called the *generator polynomial* of $\mathcal{C}$ and the dimension of $\mathcal{C}$ is $n - k$, where k is the degree of $g(x)$.

Recall that a q-ary η-constacyclic code of length n is a *simple-root* constacyclic code if $\gcd\left(n,\ q\right) = 1$ and a *repeated-root* constacyclic code if $p \mid n$, where p is the characteristic of $\mathbb{F}_q$. Simple-root constacyclic codes can be characterized by their defining sets [16, 23]. Compared to simple-root cyclic codes, repeated-root cyclic codes are no longer characterized by its set of zeros. Let $\mathcal{C} = \langle g(x)\rangle$ be a repeated-root cyclic code of length lp^e over $\mathbb{F}_q$, where l and e are positive integers with $\gcd\left(l,\ p\right) = 1$. It is shown in [4] that the minimum Hamming distance of $\mathcal{C}$ can be derived from $d_H(\overline{\mathcal{C}}_t)$. Here $\overline{\mathcal{C}}_t$ is a simple-root cyclic code fully determined by $\mathcal{C}$ as follows.

More precisely, assume that

$$g(x) = \prod_{i=1}^{r} m_i\left(x\right)^{e_i}$$

where each $m_i(x)$ is a monic irreducible polynomial over $\mathbb{F}_q$ and e_i are positive integers. For a fixed t with $0 \leq t \leq p^e - 1$, $\overline{\mathcal{C}}_t$ is defined to be a simple-root cyclic code of length l over $\mathbb{F}_q$ with the generator polynomial

$$\overline{g}_t(x) = \prod_{1\leq i\leq r,\, e_i>t} m_i(x).$$

If $\overline{g}_t(x) = x^l - 1$, then $\overline{\mathcal{C}}_t$ contains only the all-zero codeword and we set $d_H(\overline{\mathcal{C}}_t) = \infty$. If each $e_i \leq t$, then $\overline{g}_t(x) = 1$ and $d_H(\overline{\mathcal{C}}_t) = 1$.

The following lemma reveals that the minimum Hamming distance of repeated-root cyclic codes can be determined by the polynomial algebra, which will be applied to derive the minimum Hamming distance of codes in this paper.

Lemma 3 [4] *Let $\mathcal{C}$ be a repeated-root cyclic code of length lp^e over $\mathbb{F}_q$, where l and e are positive integers with* $\gcd(l, p) = 1$. *Then*

$$d_H(\mathcal{C}) = \min\left\{P_t \cdot d_H\left(\overline{\mathcal{C}}_t\right) \,\middle|\, 0 \leq t \leq p^e - 1\right\} \tag{1}$$

where

$$P_t = w_H\left((x-1)^t\right) = \prod_i (t_i + 1) \tag{2}$$

with t_i's being the coefficients of the p-adic expansion of t.

In this paper, we will employ repeated-root cyclic codes to construct new MDS symbol-pair codes. The following lemmas are very useful.

Lemma 4 [7] *Let $\mathcal{C}$ be an $[n, k, d_H(\mathcal{C})]$ constacyclic code over $\mathbb{F}_q$ with $2 \leq d_H(\mathcal{C}) < n$. Then we have $d_p(\mathcal{C}) \geq d_H(\mathcal{C})+2$ if and only if $\mathcal{C}$ is not an MDS code, i.e., $k < n-d_H(\mathcal{C})+1$.*

Lemma 5 *Let $\mathcal{C} = \langle g(x)\rangle$ be a repeated-root cyclic code of length lp^e over $\mathbb{F}_q$ and $c(x) = \left(x^l - 1\right)^t v(x)$ a codeword in $\mathcal{C}$ with Hamming weight $d_H(\mathcal{C})$, where l and e are positive integers with* $\gcd(l, p) = 1$, $0 \leq t \leq p^e - 1$ *and* $\left(x^l - 1\right) \nmid v(x)$. *Then*

$$w_H\left(c(x)\right) = P_t \cdot N_v$$

where P_t is defined as (2) in Lemma 3 and $N_v = w_H\left(v(x) \bmod \left(x^l - 1\right)\right)$.

Proof Denote $\overline{v}(x) = \left(v(x) \bmod \left(x^l - 1\right)\right)$ and

$$\overline{c}_t(x) = \left(\left(x^l - 1\right)^t \cdot \overline{v}(x)^{p^e} \bmod \left(x^{lp^e} - 1\right)\right).$$

Assume that

$$g(x) = \prod_{i=1}^{r} m_i(x)^{e_i}$$

and

$$\overline{g}_t(x) = \prod_{1\leq i\leq r,\, e_i>t} m_i(x).$$

It follows from $x^{lp^e} - 1 = (x^l - 1)^{p^e}$, $\left(x^l - 1\right) \nmid v(x)$ and $g(x) \mid c(x)$ that $\overline{g}_t(x) \mid \overline{v}(x)$. Combining with $t < p^e$, one can obtain that for any $1 \leq i \leq r$,

$i)$ if $e_i > t$, then $m_i(x) \mid \overline{v}(x)$ and $m_i(x)$ is a factor of $\overline{c}_t(x)$ with multiplicity at least p^e;

$ii)$ if $e_i \leq t$, then $m_i(x)$ is a factor of $\overline{c}_t(x)$ with multiplicity at least t.

Hence $g(x) \mid \overline{c}_t(x)$.

Meanwhile, due to $\deg(\overline{v}(x)) < l$, there must exist a root of $x^l - 1$ whose multiplicity in $\overline{c}_t(x)$ is exactly t. This leads to $(x^{lp^e} - 1) \nmid \overline{c}_t(x)$ and then $\overline{c}_t(x)$ is a nonzero codeword in $\mathcal{C}$. It can be verified that

$$\begin{aligned} w_H(\overline{c}_t(x)) &= w_H\left(\left(x^l - 1\right)^t \cdot \overline{v}(x)^{p^e} \bmod \left(x^{lp^e} - 1\right)\right) \\ &\le w_H\left(\left(x^l - 1\right)^t \cdot \overline{v}(x)^{p^e}\right) \le w_H\left(\left(x^l - 1\right)^t\right) \cdot w_H\left(\overline{v}(x)^{p^e}\right) = P_t \cdot N_v. \end{aligned}$$

On the other hand, according to Theorem 6.3 in [24], we have

$$w_H(c(x)) \ge w_H\left((x^l - 1)^t\right) \cdot w_H\left(v(x) \bmod (x^l - 1)\right) = P_t \cdot N_v \ge w_H(\overline{c}_t(x)).$$

Since $w_H(c(x)) = d_H(\mathcal{C})$, one can immediately conclude that

$$w_H(c(x)) = w_H(\overline{c}_t(x)) = P_t \cdot N_v.$$

This completes the proof. □

The following lemma will be frequently used to prove our results.

Lemma 6 *Let p be a prime power with $5 \mid (p-1)$, β be a primitive 5-th root of unity in $\mathbb{F}_p$ and $a_i \in \mathbb{F}_p^*$ for $1 \le i \le 3$. Then*

$$\beta^2 + 3\beta + 1 \ne 0 \tag{3}$$

and for $(i, j) = (2, 3)$, $(2, 4)$ or $(3, 4)$, the solution of the $\mathbb{F}_p$-linear system of equations

$$\begin{cases} 1 + a_1 + a_2 + a_3 = 0, \\ 1 + a_1\beta + a_2\beta^i + a_3\beta^j = 0, \\ 1 + a_1\beta^2 + a_2\beta^{2i} + a_3\beta^{2j} = 0 \end{cases} \tag{4}$$

is given as

Value of (i, j)	Corresponding solution (a_1, a_2, a_3)
(2, 3)	$\left(-\frac{\beta^2+\beta+1}{\beta^2}, \frac{\beta^2+\beta+1}{\beta^3}, -\frac{1}{\beta^3}\right)$
(2, 4)	$\left(-\frac{1}{\beta}, -\frac{\beta}{\beta+1}, \frac{1}{\beta(\beta+1)}\right)$
(3, 4)	$\left(\frac{\beta^2}{\beta+1}, -\frac{1}{\beta+1}, -\beta\right)$.

Proof Assume that $\beta^2 + 3\beta + 1 = 0$. The fact β is a primitive 5-th root of unity indicates

$$0 = \beta^4 + \beta^3 + \beta^2 + \beta + 1 = -5(3\beta + 1)$$

which yields $\beta^2 = -3\beta - 1 = 0$, a contradiction.

If $(i, j) = (2, 3)$, then (4) can be transformed into

$$\begin{cases} 1 + a_1 + a_2 + a_3 = 0, \\ 1 + a_1\beta + a_2\beta^2 + a_3\beta^3 = 0, \\ 1 + a_1\beta^2 + a_2\beta^4 + a_3\beta = 0. \end{cases}$$

This leads to

$$a_1 = -\frac{\beta^2+\beta+1}{\beta^2}, \quad a_2 = \frac{\beta^2+\beta+1}{\beta^3}, \quad a_3 = -\frac{1}{\beta^3}.$$

Similarly, we can derive the solutions of (4) for $(i, j) = (2, 4)$ and $(3,4)$. This completes the proof. □

3 Constructions of MDS symbol-pair codes

In this section, we propose three new classes of MDS symbol-pair codes from repeated-root cyclic codes by analyzing the solutions of certain equations over $\mathbb{F}_p$. Firstly, for length $5p$, two classes of MDS symbol-pair codes with minimum symbol-pair distance 7 or 8 are constructed respectively. In addition, for $n = 4p$, we derive a class of MDS symbol-pair codes with $d_p = 7$.

From now on, we denote by $c^{(k)}(x)$ the k-th formal derivative of $c(x)$, where k is a positive integer and $c(x) \in \mathbb{F}_p[x]$. Let $\star$ denote an element in $\mathbb{F}_p^*$ and $\mathbf{0}$ is the zero vector. Due to the linearity and the cyclic shift property of cyclic codes, we assume that the constant term of $c(x)$ occurred in this paper is always 1.

3.1 MDS symbol-pair codes for $n = 5p$

In this subsection, two classes of MDS symbol-pair codes with length $5p$ are constructed.

Now we present a class of MDS symbol-pair codes with minimum symbol-pair distance 7 for any prime p with $5 \mid (p-1)$ and $p \neq 41$.

Theorem 1 *Let p be a prime with $5 \mid (p-1)$ and $p \neq 41$. Then there exists an MDS $(5p, 7)_p$ symbol-pair code.*

Proof Let $\mathcal{C}$ be a repeated-root cyclic code of length $5p$ over $\mathbb{F}_p$ with the generator polynomial

$$g(x) = (x-1)^3 (x-\beta) \left(x-\beta^2\right)$$

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

Note that $\mathcal{C}$ is a $[5p, 5p-5, 4]$ cyclic code due to Lemma 3. Indeed, recall that $\overline{g}_t(x)$ is the generator polynomial of $\overline{\mathcal{C}}_t$. If $t = 0$, then

$$\overline{g}_0(x) = (x-1)(x-\beta)\left(x-\beta^2\right)$$

and

$$P_0 \cdot d_H\left(\overline{\mathcal{C}}_0\right) = 1 \cdot 4 = 4.$$

If $t = 1$, then $\overline{g}_1(x) = x - 1$ and

$$P_1 \cdot d_H\left(\overline{\mathcal{C}}_1\right) = 2 \cdot 2 = 4.$$

If $t = 2$, then $\overline{g}_2(x) = x - 1$ and

$$P_2 \cdot d_H\left(\overline{\mathcal{C}}_2\right) = 3 \cdot 2 = 6.$$

If $3 \leq t \leq p-1$, then $\overline{g}_t(x) = 1$ and

$$P_t \cdot d_H\left(\overline{\mathcal{C}}_t\right) = (t+1) \cdot 1 = t + 1 \geq 4.$$

With the aid of the equality (1) in Lemma 3, one can immediately get $d_H(\mathcal{C}) = 4$.

Since $\mathcal{C}$ is not MDS, by Lemma 4, one can obtain that $d_p(\mathcal{C}) \geq 6$. Now we claim that there does not exist a codeword in $\mathcal{C}$ with $(w_H(c(x)),\ w_p(c(x))) = (5,\ 6)$. On the contrary, without loss of generality, we assume

$$c(x) = c_0 + c_1\,x + c_2\,x^2 + c_3\,x^3 + c_4\,x^4$$

where $c_i \in \mathbb{F}_p^*$ for any $0 \leq i \leq 4$. This is contradictory with

$$\deg(g(x)) = 5, \quad \deg(c(x)) \geq \deg(g(x)).$$

Thus, there does not exist a codeword in $\mathcal{C}$ with $(w_H(c(x)),\ w_p(c(x))) = (5,\ 6)$. To show that $\mathcal{C}$ is an MDS $(5p,\ 7)_p$ symbol-pair code, it is sufficient to verify that there does not exist a codeword in $\mathcal{C}$ with $(w_H(c(x)),\ w_p(c(x))) = (4,\ 6)$.

Let $c(x)$ be a codeword in $\mathcal{C}$ with Hamming weight 4. Suppose that $c(x)$ has the factorization $c(x) = \left(x^5 - 1\right)^t v(x)$, where $0 \leq t \leq p-1$, $\left(x^5 - 1\right) \nmid v(x)$ and

$$v(x) = v_0(x^5) + x\,v_1(x^5) + x^2\,v_2(x^5) + x^3\,v_3(x^5) + x^4\,v_4(x^5).$$

It follows from Lemma 5 that

$$4 = w_H\left(\left(x^5 - 1\right)^t\right) \cdot w_H\left(v(x) \bmod \left(x^5 - 1\right)\right) = (1+t)\,N_v$$

where $N_v = w_H\left(v(x) \bmod \left(x^5 - 1\right)\right)$. Then one can deduce that $(N_v,\ t) = (1,\ 3),\ (2,\ 1)$ or $(4,\ 0)$.

If $(N_v,\ t) = (1,\ 3)$, then it is obvious that the symbol-pair weight of $c(x)$ is greater than 6.

If $(N_v,\ t) = (2,\ 1)$ and $c(x)$ has symbol-pair weight 6, then Lemma 1 indicates that its certain cyclic shift must have the form

$$(\star,\ \star,\ \mathbf{0},\ \star,\ \star,\ \mathbf{0})\,.$$

Let

$$c(x) = 1 + a_1\,x + a_2\,x^{5i} + a_3\,x^{5i+1}$$

for some positive integer i with $1 \leq i \leq p-1$ and $a_1,\ a_2,\ a_3 \in \mathbb{F}_p^*$. It follows from $5 \mid (p-1)$ and $\gcd(i, p) = 1$ that $p \nmid 5i$. The fact $c\,(1) = c\,(\beta) = 0$ induces that

$$\begin{cases} 1 + a_1 + a_2 + a_3 = 0, \\ 1 + a_1\,\beta + a_2 + a_3\,\beta = 0 \end{cases}$$

which implies $a_1 = -a_3$ and $a_2 = -1$. Then $c^{(1)}\,(1) = c^{(2)}\,(1) = 0$ yields

$$\begin{cases} a_1 - 5i - (5i+1)\,a_1 = 0, \\ -5i\,(5i-1) - 5i\,(5i+1)\,a_1 = 0. \end{cases}$$

This indicates $a_1 = -1$ and then $2 = 0$, a contradiction.

If $(N_v,\ t) = (4,\ 0)$ and $c(x)$ has symbol-pair weight 6, then its corresponding cyclic shift must have the form

$$(\star,\ \star,\ \mathbf{0},\ \star,\ \star,\ \mathbf{0})$$

or

$$(\star,\ \star,\ \star,\ \mathbf{0},\ \star,\ \mathbf{0})\,.$$

In what follows, we discuss the above two cases one by one.

Case I For the case $(\star,\ \star,\ \mathbf{0},\ \star,\ \star,\ \mathbf{0})$, there are two subcases to be considered:

– For the subcase $c(x) = 1 + a_1 x + a_2 x^{5i+2} + a_3 x^{5i+3}$ with $1 \leq i \leq p-1$ and $a_1, a_2, a_3 \in \mathbb{F}_p^*$, it follows from $c(1) = c^{(1)}(1) = c^{(2)}(1) = 0$ that

$$\begin{cases} 1 + a_1 + a_2 + a_3 = 0, \\ a_1 + (5i+2)\, a_2 + (5i+3)\, a_3 = 0, \\ (5i+2)(5i+1)\, a_2 + (5i+3)(5i+2)\, a_3 = 0. \end{cases} \tag{5}$$

If $p \mid (5i+2)$, then (5) implies that $a_1 = -a_3$ and $a_2 = -1$. Then $c(\beta) = c\left(\beta^2\right) = 0$ yields

$$\begin{cases} 1 + a_1 \beta - \beta^2 - a_1 \beta^3 = 0, \\ 1 + a_1 \beta^2 - \beta^4 - a_1 \beta^6 = 0. \end{cases}$$

One can immediately obtain that

$$a_1 = \frac{\beta^2 - 1}{\beta - \beta^3} = \frac{\beta^4 - 1}{\beta^2 - \beta^6}.$$

This leads to $\beta = 1$, a contradiction.

If $p \nmid (5i+2)$, then (5) yields that $a_1 = -a_2$ and $a_3 = -1$. It follows from $c(\beta) = c\left(\beta^2\right) = 0$ that

$$\begin{cases} 1 + a_1 \beta - a_1 \beta^2 - \beta^3 = 0, \\ 1 + a_1 \beta^2 - a_1 \beta^4 - \beta^6 = 0. \end{cases}$$

Then one gets that

$$a_1 = \frac{\beta^3 - 1}{\beta - \beta^2} = \frac{\beta^6 - 1}{\beta^2 - \beta^4}$$

which induces

$$\beta^3 + 1 = \beta\,(\beta + 1)\,.$$

This implies $(\beta - 1)\left(\beta^2 - 1\right) = 0$, a contradiction.

– Consider the subcase $c(x) = 1 + a_1 x + a_2 x^{5i+3} + a_3 x^{5i+4}$ with $0 \leq i \leq p-2$ and $a_1, a_2, a_3 \in \mathbb{F}_p^*$. By arguments similar to the previous subcase of $c(x) = 1 + a_1 x + a_2 x^{5i+2} + a_3 x^{5i+3}$, one can also derive a contradiction and we omit the proof here.

Case II For the remaining case $(\star, \star, \star, \mathbf{0}, \star, \mathbf{0})$, there are also two subcases to be discussed:

– Consider the subcase $c(x) = 1 + a_1 x + a_2 x^2 + a_3 x^{5i+3}$ with $1 \leq i \leq p-1$ and $a_1, a_2, a_3 \in \mathbb{F}_p^*$. Notice that $c(1) = c(\beta) = c\left(\beta^2\right) = 0$ and Lemma 6 indicates

$$a_1 = -\frac{\beta^2 + \beta + 1}{\beta^2}, \quad a_2 = \frac{\beta^2 + \beta + 1}{\beta^3}, \quad a_3 = -\frac{1}{\beta^3}. \tag{6}$$

It follows from $c^{(1)}(1) = c^{(2)}(1) = 0$ that

$$\begin{cases} a_1 + 2\, a_2 + (5i+3)\, a_3 = 0, \\ 2\, a_2 + (5i+3)(5i+2)\, a_3 = 0. \end{cases} \tag{7}$$

Observe that (7) yields

$$\begin{cases} a_1 = (5i+3)(5i+1)\, a_3, \\ (5i+2)\, a_1 + 2\,(5i+1)\, a_2 = 0 \end{cases} \tag{8}$$

and the second equality in (7) indicates $p \nmid (5i+2)$. Let $t = 5i+2$. By (6) and (8), one can immediately have

$$\begin{cases} t^2 = \beta^3 + \beta^2 + \beta + 1, \\ t(\beta - 2) = 2. \end{cases} \tag{9}$$

The second equality in (9) indicates $\beta \neq 2$ and $t = -\frac{2}{\beta-2}$. By substituting the value of t into the first equality in (9), one can obtain

$$\frac{4\beta}{(\beta-2)^2} = (\beta^3 + \beta^2 + \beta + 1)\beta.$$

It follows from $\beta^4 + \beta^3 + \beta^2 + \beta + 1 = 0$ that $\beta^2 = -4$ and

$$\beta^4 + \beta^3 + \beta^2 + \beta + 1 = 13 - 3\beta = 0.$$

This leads to $\beta = \frac{13}{3}$ and then

$$\beta^2 = \frac{169}{9} = -4$$

implies $5 \cdot 41 = 0$, which is contradictory with $5 \mid (p-1)$ and $p \neq 41$.

- For the subcase $c(x) = 1 + a_1 x + a_2 x^2 + a_3 x^{5i+4}$ with $0 \le i \le p-2$ and $a_1,\ a_2,\ a_3 \in \mathbb{F}_p^*$, it follows from $c(1) = c(\beta) = c\left(\beta^2\right) = 0$ and Lemma 6 that

$$a_1 = -\frac{1}{\beta}, \quad a_2 = -\frac{\beta}{\beta+1}, \quad a_3 = \frac{1}{\beta(\beta+1)}. \tag{10}$$

On the other hand, $c^{(1)}(1) = c^{(2)}(1) = 0$ yields that

$$\begin{cases} a_1 + 2a_2 + (5i+4)\,a_3 = 0, \\ 2a_2 + (5i+4)(5i+3)\,a_3 = 0 \end{cases}$$

which is equivalent to

$$\begin{cases} a_1 + 2a_2 + (5i+4)\,a_3 = 0, \\ a_1 = (5i+4)(5i+2)\,a_3. \end{cases}$$

Let $t = 5i+3$. Together with (10), one can immediately obtain that

$$\begin{cases} t = 2\beta^2 + \beta, \\ t^2 + \beta = 0. \end{cases}$$

Then by substituting the value of t, one has

$$\beta^2 = 3\beta + 3 \tag{11}$$

and

$$0 = \beta^4 + \beta^3 + \beta^2 + \beta + 1 = 61\beta + 49.$$

If $p = 61$, then $49 = 0$, which is impossible. If $p \neq 61$, then $\beta = -\frac{49}{61}$. It follows from (11) that

$$\left(\frac{49}{61}\right)^2 = 3\left(-\frac{49}{61} + 1\right).$$

This implies $5 \cdot 41 = 0$, a contradiction similar as the previous subcase.

Therefore, $\mathcal{C}$ is an MDS $(5p,\ 7)_p$ symbol-pair code. This completes the proof. □

Another class of MDS symbol-pair codes with $n = 5p$ and $d_p = 8$ is proposed as follows.

Theorem 2 *Let p be a prime with $5 \mid (p-1)$. Then there exists an MDS $(5p, 8)_p$ symbol-pair code.*

Proof Let $\mathcal{C}$ be a repeated-root cyclic code of length $5p$ over $\mathbb{F}_p$ with the generator polynomial

$$g(x) = (x-1)^3 (x-\beta) \left(x-\beta^2\right)^2$$

where β is a primitive 5-th root of unity in $\mathbb{F}_p$. It can be verified that $\mathcal{C}$ is an MDS $(5p, 8)_p$ symbol-pair code by similar techniques used in the proof of Theorem 1. Since the proof is lengthy and some cases seem a bit cumbersome, we present it in the Appendix. □

Now we provide two examples to illustrate the constructions in Theorems 1 and 2.

Example 1 (1) Let $\mathcal{C}$ be a repeated-root cyclic code of length 55 over $\mathbb{F}_{11}$ with the generator polynomial

$$g(x) = (x-1)^3 (x-3) \left(x-3^2\right).$$

MAGMA experiments show that $\mathcal{C}$ is a $[55, 50, 4]$ code and the minimum symbol-pair distance of $\mathcal{C}$ is 7, which satisfies our result in Theorem 1.

(2) Let $\mathcal{C}$ be a repeated-root cyclic code of length 55 over $\mathbb{F}_{11}$ with the generator polynomial

$$g(x) = (x-1)^3 (x-3) \left(x-3^2\right)^2.$$

By a MAGMA program, it can be checked that $\mathcal{C}$ is a $[55, 49, 4]$ code and the minimum symbol-pair distance of $\mathcal{C}$ is 8, which is consistent with our result in Theorem 2.

3.2 MDS symbol-pair codes for $n = 4p$

In this subsection, we shall construct a class of MDS symbol-pair codes with $d_p = 7$, which generalizes Theorem 3.8 in [18].

Theorem 3 *Let p be an odd prime. Then there exists an MDS $(4p, 7)_p$ symbol-pair code.*

Proof The case $p \equiv 3 \pmod 4$ has been settled, see the result of Theorem 3.8 in [18]. For the case $p \equiv 1 \pmod 4$, let $\mathcal{C}$ be a repeated-root cyclic code of length $4p$ over $\mathbb{F}_p$ with the generator polynomial

$$g(x) = (x-1)^3 (x-\omega)(x+\omega)$$

where ω is a primitive 4-th root of unity in $\mathbb{F}_p$. In the following, we will claim that for $p \equiv 1 \pmod 4$, the code $\mathcal{C}$ is also an MDS $(4p, 7)_p$ symbol-pair code.

By Lemma 3, one can derive that the parameter of $\mathcal{C}$ is $[4p, 4p-5, 4]$. Since $\mathcal{C}$ is not MDS, by Lemma 4, we get $d_p(\mathcal{C}) \geq 6$. With a similar argument as Theorem 1, one can obtain that there does not exist a codeword $c(x)$ in $\mathcal{C}$ with $(w_H(c(x)), w_p(c(x))) = (5, 6)$. In order to show that $\mathcal{C}$ is an MDS $(4p, 7)_p$ symbol-pair code, we need to prove that there does not exist a codeword in $\mathcal{C}$ with $(w_H(c(x)), w_p(c(x))) = (4, 6)$.

Let $c(x)$ be a codeword in $\mathcal{C}$ with $(w_H(c(x)), w_p(c(x))) = (4, 6)$. Then Lemma 1 indicates that its certain cyclic shift must have the form

$$(\star, \star, \star, \mathbf{0}, \star, \mathbf{0})$$

or

$$(\star, \star, \mathbf{0}, \star, \star, \mathbf{0}).$$

For the case $(\star,\ \star,\ \star,\ \mathbf{0},\ \star,\ \mathbf{0})$, we assume that

$$c(x) = 1 + a_1\, x + a_2\, x^2 + a_3\, x^l$$

for some positive integer l with $4 \le l \le 4p - 2$ and $a_1,\ a_2,\ a_3 \in \mathbb{F}_p^*$. It follows from $c\,(1) = c^{(1)}\,(1) = c^{(2)}\,(1) = 0$ that

$$\begin{cases} 1 + a_1 + a_2 + a_3 = 0, \\ a_1 + 2\, a_2 + l\, a_3 = 0, \\ 2\, a_2 + l\,(l-1)\, a_3 = 0. \end{cases}$$

This yields

$$a_1 = -\frac{2l}{l-1}, \quad a_2 = \frac{l}{l-2}, \quad a_3 = -\frac{2}{(l-1)\,(l-2)}. \tag{12}$$

- If l is even, then we have

$$\begin{cases} 1 + a_1\, \omega - a_2 + a_3\, \omega^l = 0, \\ 1 - a_1\, \omega - a_2 + a_3\, \omega^l = 0 \end{cases}$$

  since $c\,(\omega) = c\,(-\omega) = 0$ and $\omega^2 = -1$. It follows that $a_1 = 0$, which is impossible.
- If l is odd, then $c\,(\omega) = c\,(-\omega) = 0$ induces that

$$\begin{cases} 1 + a_1\, \omega - a_2 + a_3\, \omega^l = 0, \\ 1 - a_1\, \omega - a_2 - a_3\, \omega^l = 0. \end{cases}$$

  This implies that $a_2 = 1$, which contradicts with the result in (12).

For the remaining case $(\star,\ \star,\ \mathbf{0},\ \star,\ \star,\ \mathbf{0})$, we suppose that

$$c(x) = 1 + a_1\, x + a_2\, x^l + a_3\, x^{l+1}$$

for some positive integer l with $3 \le l \le 4p-3$ and $a_1,\ a_2,\ a_3 \in \mathbb{F}_p^*$. Then $c\,(1) = c^{(1)}\,(1) = c^{(2)}\,(1) = 0$ indicates that

$$\begin{cases} 1 + a_1 + a_2 + a_3 = 0, \\ a_1 + l\, a_2 + (l+1)\, a_3 = 0, \\ l\,(l-1)\, a_2 + l\,(l+1)\, a_3 = 0. \end{cases} \tag{13}$$

It follows from $c\,(\omega) = c\,(-\omega) = 0$ that

$$\begin{cases} 1 + a_1\, \omega + a_2\, \omega^l + a_3\, \omega^{l+1} = 0, \\ 1 - a_1\, \omega + a_2\, (-\omega)^l + a_3\, (-\omega)^{l+1} = 0. \end{cases} \tag{14}$$

Now we divide the proof into the following two subcases:

- For the subcase $p \mid l$, (13) yields that

$$a_1 + a_3 = 0, \quad a_2 = -1. \tag{15}$$

  If l is even, then we have $l = 2p$ due to $3 \le l \le 4p - 3$. It follows from (14) and (15) that

$$1 = \omega^l = \omega^{2p} = (-1)^p$$

  which is impossible. Similarly, if l is odd, one can obtain that $\omega^{2l} = 1$, a contradiction.

– For the subcase $p \nmid l$, it follows from (13) that

$$a_1 = -\frac{l+1}{l-1}, \quad a_2 = \frac{l+1}{l-1}, \quad a_3 = -1. \tag{16}$$

If l is even, then by (14) and (16), one can deduce that

$$a_1 = \omega^l, \quad 1 + a_2\,\omega^l = 0.$$

Then one can obtain that

$$1 = a_1^2 = \left(-\frac{l+1}{l-1}\right)^2.$$

This implies $4l = 0$, a contradiction. By a similar manner, for odd l, one can derive that $\omega^{l+1} = \omega^{l-1} = 1$, which is impossible.

Consequently, $\mathcal{C}$ is an MDS $(4p,\ 7)_p$ symbol-pair code. This proves the desired conclusion. □

Now we give an example to illustrate the construction in Theorem 3.

Example 2 Let $\mathcal{C}$ be a repeated-root cyclic code of length 20 over $\mathbb{F}_5$ with the generator polynomial

$$g(x) = (x-1)^3\,(x-2)\,(x+2)\,.$$

It can be checked by MAGMA that $\mathcal{C}$ is a $[20,\ 15,\ 4]$ code and the minimum symbol-pair distance of $\mathcal{C}$ is 7, which coincides with our result in Theorem 3.

4 Conclusions and future work

In this paper, three new classes of MDS symbol-pair codes over $\mathbb{F}_p$ with p an odd prime were constructed from repeated-root cyclic codes. Firstly, for $n = 5p$, two classes of MDS symbol-pair codes with minimum symbol-pair distance seven or eight were presented. In addition, for length $n = 4p$, we derived a class of MDS symbol-pair codes with $d_p = 7$ and our construction extends the result in [18]. Note that by utilizing repeated-root cyclic codes, one can construct MDS symbol-pair codes by transforming the problem into analyzing the solutions of certain equations over finite fields.

However, it seems impracticable to construct $(5q,\ 7)_p$, $(5q,\ 8)_p$ and $(4q,\ 7)_p$ MDS symbol-pair codes with q being a power of p using the techniques in Theorems 1-3. For instance, for the case $q = p^2$, $5 \mid (q-1)$, let $\mathcal{C}$ be a repeated-root cyclic code of length $5q$ over $\mathbb{F}_q$ with the generator polynomial of the form

$$g(x) = (x-1)^{e_1}\,(x-\omega)^{e_2}\left(x-\omega^2\right)^{e_3}\left(x-\omega^3\right)^{e_4}\left(x-\omega^4\right)^{e_5}$$

where ω is a primitive 5-th root of unity in $\mathbb{F}_q$. It can be checked that $\mathcal{C}$ is not an MDS symbol-pair code. It needs further study to construct MDS symbol-pair codes with larger minimum symbol-pair distance and length lq, where $q = p^m$ with $m > 1$.

Acknowledgements This work was supported by National Natural Science Foundation of China (Nos. 12171191, 11871025, 61977036), in part by Hubei Provincial Science and Technology Innovation Base (Platform) Special Project (No. 2020DFH002) and Application Foundation Frontier Project of Wuhan Science and Technology Bureau (No. 2020010601012189).

Appendix Proof of Theorem 2:

Recall that $\mathcal{C}$ is a repeated-root cyclic code of length $5p$ over $\mathbb{F}_p$ with the generator polynomial

$$g(x) = (x-1)^3 (x-\beta) \left(x-\beta^2\right)^2$$

where β is a primitive 5-th root of unity in $\mathbb{F}_p$. By Lemma 3, one can derive that the parameter of $\mathcal{C}$ is $[5p, 5p-6, 4]$. Since $\mathcal{C}$ is not MDS, Lemma 4 yields that $d_p(\mathcal{C}) \geq 6$. Similar as Theorem 1, one can derive that there does not exist a codeword $c(x)$ in $\mathcal{C}$ with $(w_H(c(x)), w_p(c(x))) = (5, 6)$ or $(6, 7)$. To prove that $\mathcal{C}$ is an MDS $(5p, 8)_p$ symbol-pair code, it suffices to determine that there does not exist a codeword in $\mathcal{C}$ with $(w_H(c(x)), w_p(c(x))) = (4, 6), (4, 7)$ or $(5, 7)$.

Case I $(w_H(c(x)), w_p(c(x))) = (4, 6)$. Since $\mathcal{C}$ is the subcode of the code occurred in Theorem 1 and the proof of Theorem 1 indicates that there does not exist a codeword $c(x)$ in $\mathcal{C}$ with $(w_H(c(x)), w_p(c(x))) = (4, 6)$ unless $p = 41$. Now it is sufficient to show that for $p = 41$, there does not exist a codeword $c(x)$ in $\mathcal{C}$ with $(w_H(c(x)), w_p(c(x))) = (4, 6)$. More precisely, we just need to consider **Case II** in Theorem 1. There are two subcases to be discussed:

- Consider the subcase $c(x) = 1 + a_1 x + a_2 x^2 + a_3 x^{5i+3}$ with $1 \leq i \leq p-1$ and $a_1, a_2, a_3 \in \mathbb{F}_p^*$. Notice that $c(1) = c(\beta) = c\left(\beta^2\right) = 0$ and Lemma 6 induces

$$a_1 = -\frac{\beta^2+\beta+1}{\beta^2}, \quad a_2 = \frac{\beta^2+\beta+1}{\beta^3}, \quad a_3 = -\frac{1}{\beta^3}. \tag{17}$$

  It follows from $c^{(1)}(1) = c^{(1)}\left(\beta^2\right) = 0$ that

$$\begin{cases} a_1 + 2a_2 + (5i+3)a_3 = 0, \\ a_1 + 2a_2\beta^2 + (5i+3)a_3\beta^4 = 0 \end{cases}$$

  which yields

$$a_1\left(\beta^4 - 1\right) + 2a_2\left(\beta^4 - \beta^2\right) = 0.$$

  Combining with (17), one can get $(\beta-1)^2 = 0$, a contradiction.
- For the subcase $c(x) = 1 + a_1 x + a_2 x^2 + a_3 x^{5i+4}$ with $0 \leq i \leq p-2$ and $a_1, a_2, a_3 \in \mathbb{F}_p^*$, by $c(1) = c(\beta) = c\left(\beta^2\right) = 0$ and Lemma 6, one can obtain that

$$a_1 = -\frac{1}{\beta}, \quad a_2 = -\frac{\beta}{\beta+1}, \quad a_3 = \frac{1}{\beta(\beta+1)}. \tag{18}$$

  On the other hand, $c^{(1)}(1) = c^{(1)}\left(\beta^2\right) = 0$ that

$$\begin{cases} a_1 + 2a_2 + (5i+4)a_3 = 0, \\ a_1 + 2a_2\beta^2 + (5i+4)a_3\beta = 0 \end{cases}$$

  which induces

$$a_1(\beta - 1) = 2a_2\left(\beta^2 - \beta\right).$$

  Together with (18), one can immediately obtain that

$$2\beta^3 = \beta + 1.$$

  This leads to

$$(\beta-1)\left(2\beta^2 + 2\beta + 1\right) = 0.$$

The fact β is a primitive 5-th root of unity implies that $2\beta^2 + 2\beta + 1 = 0$ and then one has

$$\beta^2 + \beta = -\left(\beta^2 + \beta + 1\right) = \beta^4 + \beta^3$$

which is impossible.

Case II $(w_H(c(x)),\ w_p(c(x))) = (4,\ 7)$. For this case, Lemma 1 implies that the cyclic shift of $c(x)$ must have the form

$$(\star,\ \star,\ \mathbf{0},\ \star,\ \mathbf{0},\ \star,\ \mathbf{0})\,.$$

Assume that $c(x) = \left(x^5 - 1\right)^t v(x)$, where $0 \le t \le p-1$, $\left(x^5 - 1\right) \nmid v(x)$ and

$$v(x) = v_0(x^5) + x\, v_1(x^5) + x^2\, v_2(x^5) + x^3\, v_3(x^5) + x^4\, v_4(x^5).$$

Recall that $N_v = w_H\left(v(x) \bmod \left(x^5 - 1\right)\right)$. Then by Lemma 5, one can deduce that

$$4 = w_H\left(\left(x^5 - 1\right)^t\right) \cdot w_H\left(v(x) \bmod \left(x^5 - 1\right)\right) = (1+t)\, N_v.$$

If $(N_v,\ t) = (1,\ 3)$, then it is easily seen that the symbol-pair weight of $c(x)$ is greater than 7.

If $(N_v,\ t) = (2,\ 1)$, then there are three subcases to be discussed:
(1) For the subcase $c(x) = 1 + a_1\, x + a_2\, x^{5i} + a_3\, x^{5j}$ with $1 \le i < j \le p-1$ and $a_1,\ a_2,\ a_3 \in \mathbb{F}_p^*$, it can be verified that

$$\begin{cases} 1 + a_1\, \beta + a_2 + a_3 = 0, \\ 1 + a_1\, \beta^2 + a_2 + a_3 = 0 \end{cases}$$

since $c\,(\beta) = c\left(\beta^2\right) = 0$. Then one can obtain that $a_1 = 0$, a contradiction.
(2) For the subcase $c(x) = 1 + a_1\, x + a_2\, x^{5i+1} + a_3\, x^{5j+1}$ with $1 \le i < j \le p-1$ and $a_1,\ a_2,\ a_3 \in \mathbb{F}_p^*$, by $c\,(1) = c\,(\beta) = 0$, one can get

$$\begin{cases} 1 + a_1 + a_2 + a_3 = 0, \\ 1 + a_1\, \beta + a_2\, \beta + a_3\, \beta = 0. \end{cases}$$

This implies that $\beta = 1$, which is impossible.
(3) For the subcase $c(x) = 1 + a_1\, x + a_2\, x^{5i} + a_3\, x^{5j+1}$ with $1 \le i < j \le p-1$ and $a_1,\ a_2,\ a_3 \in \mathbb{F}_p^*$, it follows from $c^{(1)}\,(1) = c^{(1)}\left(\beta^2\right) = 0$ that

$$\begin{cases} a_1 + 5i\, a_2 + (5j+1)\, a_3 = 0, \\ a_1 + 5i\, a_2\, \beta^3 + (5j+1)\, a_3 = 0. \end{cases}$$

This leads to $\beta^3 = 1$, a contradiction.

If $(N_v,\ t) = (4,\ 0)$, then there are also three subcases to be considered:
(1) For the subcase $c(x) = 1 + a_1\, x + a_2\, x^{5i+2} + a_3\, x^{5j+3}$ with $1 \le i < j \le p-1$ and $a_1,\ a_2,\ a_3 \in \mathbb{F}_p^*$, by Lemma 6 and $c\,(1) = c\,(\beta) = c\left(\beta^2\right) = 0$, one can derive that

$$a_1 = -\frac{\beta^2 + \beta + 1}{\beta^2}, \quad a_2 = \frac{\beta^2 + \beta + 1}{\beta^3}, \quad a_3 = -\frac{1}{\beta^3}. \tag{19}$$

It follows from $c^{(1)}\,(1) = c^{(1)}\left(\beta^2\right) = 0$ that

$$\begin{cases} a_1 + (5i+2)\, a_2 + (5j+3)\, a_3 = 0, \\ a_1 + (5i+2)\, a_2\, \beta^2 + (5j+3)\, a_3\, \beta^4 = 0 \end{cases}$$

which indicates

$$\begin{cases} \left(\beta^4 - 1\right) a_1 + (\beta^4 - \beta^2)(5i + 2)\, a_2 = 0, \\ \left(\beta^2 - 1\right)(5i + 2)\, a_2 + (5j + 3)\left(\beta^4 - 1\right) a_3 = 0. \end{cases}$$

Together with (19), one can immediately obtain that

$$\begin{cases} \beta^2 + 1 = (5i + 2)\,\beta, \\ (5i + 2)\left(\beta^2 + \beta + 1\right) = (5j + 3)\left(\beta^2 + 1\right). \end{cases} \tag{20}$$

By substituting the value of $\beta^2 + 1$ in the first equality into the second equality of (20), we can get

$$(5i + 2)(5i + 3)\,\beta = (5i + 2)(5j + 3)\,\beta$$

which yields $i = j$ due to $p \nmid (5i + 2)$. This contradicts with $i < j$.
(2) Consider the subcase $c(x) = 1 + a_1 x + a_2 x^{5i+2} + a_3 x^{5j+4}$ with $1 \le i \le j \le p - 2$ and $a_1,\ a_2,\ a_3 \in \mathbb{F}_p^*$. The fact $c(1) = c(\beta) = c\left(\beta^2\right) = 0$ and Lemma 6 leads to

$$a_1 = -\frac{1}{\beta}, \quad a_2 = -\frac{\beta}{\beta + 1}, \quad a_3 = \frac{1}{\beta(\beta + 1)}. \tag{21}$$

It follows from $c^{(1)}(1) = c^{(1)}\left(\beta^2\right) = 0$ that

$$\begin{cases} a_1 = \beta(5i + 2)\, a_2, \\ (5i + 2)(\beta + 1)\, a_2 + (5j + 4)\, a_3 = 0. \end{cases}$$

By substituting (21), one can immediately derive that

$$\begin{cases} \beta + 1 = (5i + 2)\,\beta^3, \\ (5i + 2)\,\beta^2(\beta + 1) = 5j + 4. \end{cases} \tag{22}$$

This leads to $(5i + 2)^2 = 5j + 4$. Since it can be verified that $p \nmid (5i + 2)$, it follows from $c^{(2)}(1) = 0$ that

$$\beta^2 = (5i + 2)(5i + 3). \tag{23}$$

Then (21) and $c^{(1)}(1) = 0$ indicates that

$$(5i + 2)\,\beta^2 + \beta - (5j + 3) = 0. \tag{24}$$

Let $t = 5i + 2$. Then one has $\beta + 1 = t\beta^3$ and $\beta^2 = t(t + 1)$ due to the first equality of (22) and (23). It follows from (24) that

$$t^2(t + 1) + \beta - (t^2 - 1) = 0$$

which implies $\beta + 1 = -t^3$. Combining with $\beta + 1 = t\beta^3$, we have $\beta^3 = -t^2$. Since β is a primitive 5-th root of unity, one can derive

$$\begin{aligned} 0 &= \beta^4 + \beta^3 + \beta^2 + \beta + 1 \\ &= (\beta + 1)\left(\beta^3 + 1\right) + \beta^2 \\ &= -t^3\left(-t^2 + 1\right) + t(t + 1) \\ &= t(t + 1)\left(t^3 - t^2 + 1\right). \end{aligned}$$

It follows from $t(t + 1) = \beta^2 \neq 0$ that $t^3 - t^2 + 1 = 0$. Then we obtain

$$\beta = -t^3 - 1 = -t^2 = \beta^3$$

which yields $\beta^2 - 1 = 0$, a contradiction.

(3) For the subcase $c(x) = 1 + a_1 x + a_2 x^{5i+3} + a_3 x^{5j+4}$ with $0 \le i < j \le p-2$ and $a_1, a_2, a_3 \in \mathbb{F}_p^*$, it follows from $c(1) = c(\beta) = c\left(\beta^2\right) = 0$ and Lemma 6 that

$$a_1 = \frac{\beta^2}{\beta+1}, \quad a_2 = -\frac{1}{\beta+1}, \quad a_3 = -\beta. \tag{25}$$

Since $c^{(1)}(1) = c^{(1)}\left(\beta^2\right) = 0$, one can immediately get

$$\begin{cases} (5i+3)\left(\beta^4 - 1\right) a_2 + (5j+4)(\beta - 1) a_3 = 0, \\ a_1(\beta - 1) = (5i+3)\left(\beta^4 - \beta\right) a_2. \end{cases}$$

Together with (25), one can conclude that

$$\begin{cases} (5i+3)\left(\beta^2 + 1\right) + (5j+4)\beta = 0, \\ (5i+3)\left(\beta^2 + \beta + 1\right) + \beta = 0. \end{cases}$$

which indicates

$$\begin{cases} (5i+3)\,\beta^2 + (5j+4)\beta + 5i + 3 = 0, \\ (5i+3)\,\beta^2 + (5i+4)\beta + 5i + 3 = 0. \end{cases}$$

It follows that $5(i-j) = 0$, a contradiction.

Case III $(w_H(c(x)),\ w_p(c(x))) = (5,\ 7)$. In this case, we can assume that $c(x)$ is of the form

$$(\mathbf{a},\ \mathbf{0},\ \mathbf{b},\ \mathbf{0})$$

where $\mathbf{a}$, $\mathbf{b}$ are row vectors with all entries of $\mathbf{a}$, $\mathbf{b}$ being nonzero. Then its certain cyclic shift must have the form

$$(\star,\ \star,\ \star,\ \star,\ \mathbf{0},\ \star,\ \mathbf{0})$$

or

$$(\star,\ \star,\ \star,\ \mathbf{0},\ \star,\ \star,\ \mathbf{0})\,.$$

- For $(\star,\ \star,\ \star,\ \star,\ \mathbf{0},\ \star,\ \mathbf{0})$, there are five subcases to be considered:
  (1) Consider the subcase $c(x) = 1 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^{5i}$ with $1 \le i \le p-1$ and $a_1, a_2, a_3, a_4 \in \mathbb{F}_p^*$. It can be verified that

$$\begin{cases} 1 + a_1 + a_2 + a_3 + a_4 = 0, \\ 1 + a_1\beta + a_2\beta^2 + a_3\beta^3 + a_4 = 0, \\ 1 + a_1\beta^2 + a_2\beta^4 + a_3\beta + a_4 = 0 \end{cases}$$

  since $c(1) = c(\beta) = c\left(\beta^2\right) = 0$. Then one can derive that $p \nmid (a_4 + 1)$. By Lemma 6, one can obtain

$$a_1 = -\frac{\beta^2+\beta+1}{\beta^2}(a_4+1), a_2 = \frac{\beta^2+\beta+1}{\beta^3}(a_4+1), a_3 = -\frac{1}{\beta^3}(a_4+1). \tag{26}$$

  It follows from $c^{(1)}(1) = c^{(1)}\left(\beta^2\right) = 0$ that

$$\begin{cases} a_1 + 2a_2 + 3a_3 + 5i\,a_4 = 0, \\ a_1 + 2a_2\beta^2 + 3a_3\beta^4 + 5i\,a_4\beta^3 = 0 \end{cases}$$

  which indicates

$$\left(\beta^3 - 1\right) a_1 + 2\left(\beta^3 - \beta^2\right) a_2 + 3\left(\beta^3 - \beta^4\right) a_3 = 0.$$

Combining with (26), one can derive that

$$-\left(\beta^3-1\right)\beta\left(\beta^2+\beta+1\right)+2\beta^2\left(\beta-1\right)\left(\beta^2+\beta+1\right)+3\beta^3\left(\beta-1\right)=0.$$

Since β is a primitive 5-th root of unity, by expanding the above equality, one can get $\beta^2+3\beta+1=0$. This is contradictory with the inequality (3) in Lemma 6.
(2) Consider the subcase $c(x)=1+a_1\,x+a_2\,x^2+a_3\,x^3+a_4\,x^{5i+1}$ with $1\le i\le p-1$ and $a_1,\ a_2,\ a_3,\ a_4\in\mathbb{F}_p^*$. It follows from $c\left(1\right)=c\left(\beta\right)=c\left(\beta^2\right)=0$ and Lemma 6 that

$$a_1+a_4=-\frac{\beta^2+\beta+1}{\beta^2},\quad a_2=\frac{\beta^2+\beta+1}{\beta^3},\quad a_3=-\frac{1}{\beta^3}. \tag{27}$$

Then $c^{(1)}\left(1\right)=c^{(1)}\left(\beta^2\right)=0$ induces that

$$\begin{cases} a_1+2\,a_2+3\,a_3+(5i+1)\,a_4=0,\\ a_1+2\,a_2\,\beta^2+3\,a_3\,\beta^4+(5i+1)\,a_4=0.\end{cases}$$

This leads to

$$2\left(\beta^2-1\right)a_2+3\left(\beta^4-1\right)a_3=0.$$

Together with (27), one can immediately get $(\beta-1)^2=0$, which is impossible.
(3) Consider the subcase $c(x)=1+a_1\,x+a_2\,x^2+a_3\,x^3+a_4\,x^{5i+2}$ with $1\le i\le p-1$ and $a_1,\ a_2,\ a_3,\ a_4\in\mathbb{F}_p^*$. The fact $c\left(1\right)=c\left(\beta\right)=c\left(\beta^2\right)=0$ and Lemma 6 induces

$$a_1=-\frac{\beta^2+\beta+1}{\beta^2},\quad a_2+a_4=\frac{\beta^2+\beta+1}{\beta^3},\quad a_3=-\frac{1}{\beta^3}. \tag{28}$$

It follows from $c^{(1)}\left(1\right)=c^{(1)}\left(\beta^2\right)=0$ that

$$\begin{cases} a_1+2\,a_2+3\,a_3+(5i+2)\,a_4=0,\\ a_1+2\,a_2\,\beta^2+3\,a_3\,\beta^4+(5i+2)\,a_4\,\beta^2=0\end{cases}$$

which implies

$$\left(\beta^2-1\right)a_1+3\left(\beta^2-\beta^4\right)a_3=0.$$

By substituting (28) into the above equality, we have $(\beta-1)^2=0$, a contradiction.
(4) Consider the subcase $c(x)=1+a_1\,x+a_2\,x^2+a_3\,x^3+a_4\,x^{5i+3}$ with $1\le i\le p-1$ and $a_1,\ a_2,\ a_3,\ a_4\in\mathbb{F}_p^*$. By $c\left(1\right)=c\left(\beta\right)=c\left(\beta^2\right)=0$ and Lemma 6, one has

$$a_1=-\frac{\beta^2+\beta+1}{\beta^2},\quad a_2=\frac{\beta^2+\beta+1}{\beta^3},\quad a_3+a_4=-\frac{1}{\beta^3}. \tag{29}$$

It follows from $c^{(1)}\left(1\right)=c^{(1)}\left(\beta^2\right)=0$ that

$$\begin{cases} a_1+2\,a_2+3\,a_3+(5i+3)\,a_4=0,\\[2ex] a_1+2\,a_2\,\beta^2+3\,a_3\,\beta^4+(5i+3)\,a_4\,\beta^4=0.\end{cases}$$

This yields

$$\left(\beta^4-1\right)a_1+2\left(\beta^4-\beta^2\right)a_2=0.$$

Combining with (29), one can derive that $(\beta-1)^2=0$, which is impossible.
(5) Consider the subcase $c(x)=1+a_1\,x+a_2\,x^2+a_3\,x^3+a_4\,x^{5i+4}$ with $1\le i\le p-2$ and $a_1,\ a_2,\ a_3,\ a_4\in\mathbb{F}_p^*$. It can be verified that

$$\begin{cases} 1+a_1+a_2+a_3+a_4=0, \\ 1+a_1\,\beta+a_2\,\beta^2+a_3\,\beta^3+a_4\,\beta^4=0, \\ 1+a_1\,\beta^2+a_2\,\beta^4+a_3\,\beta+a_4\,\beta^3=0 \end{cases}$$

since $c\,(1)=c\,(\beta)=c\left(\beta^2\right)=0$. Then one can obtain that

$$\begin{cases} a_1=-\beta^3\,a_4+\beta^2+\beta, \\ a_2=-\left(\beta^4+1\right)a_4-\beta-1, \\ a_3=-\left(\beta^2+\beta+1\right)a_4-\beta^2. \end{cases} \tag{30}$$

It follows from $c^{(1)}\,(1)=c^{(1)}\left(\beta^2\right)=0$ that

$$\begin{cases} a_1+2\,a_2+3\,a_3+(5i+4)\,a_4=0, \\ a_1+2\,a_2\,\beta^2+3\,a_3\,\beta^4+(5i+4)\,a_4\,\beta=0 \end{cases}$$

which implies

$$(\beta-1)\,a_1+2\left(\beta-\beta^2\right)a_2+3\left(\beta-\beta^4\right)a_3=0.$$

This is equivalent to

$$a_1-2\,\beta\,a_2-3\,\beta\left(\beta^2+\beta+1\right)a_3=0.$$

Together with (30), one can immediately have

$$(-\beta^3+2\beta(\beta^4+1)+3\,\beta(\beta^2+\beta+1)^2)a_4+\beta^2+\beta+2\,\beta(\beta+1)+3\,\beta^3(\beta^2+\beta+1)=0.$$

Then we get that

$$-\beta^3+2\beta\left(\beta^4+1\right)+3\,\beta\left(\beta^2+\beta+1\right)^2=0$$

due to $\beta^4+\beta^3+\beta^2+\beta+1=0$ and $a_4\in\mathbb{F}_p^*$. By a straightforward computation, one has $\beta^2+3\beta+1=0$. This contradicts with the inequality (3) in Lemma 6.

- For $(\star,\ \star,\ \star,\ \mathbf{0},\ \star,\ \star,\ \mathbf{0})$, there are also five subcases to be considered:
(1) Consider the subcase $c(x)=1+a_1\,x+a_2\,x^2+a_3\,x^{5i}+a_4\,x^{5i+1}$ with $1\le i\le p-1$ and $a_1,\ a_2,\ a_3,\ a_4\in\mathbb{F}_p^*$. It follows from $c\,(1)=c\,(\beta)=c\left(\beta^2\right)=0$ that

$$\begin{cases} 1+a_1+a_2+a_3+a_4=0, \\ 1+a_1\,\beta+a_2\,\beta^2+a_3+a_4\,\beta=0, \\ 1+a_1\,\beta^2+a_2\,\beta^4+a_3+a_4\,\beta^2=0 \end{cases}$$

which implies

$$\begin{cases} (a_1+a_4)\,(\beta-1)+a_2\left(\beta^2-1\right)=0, \\ (a_1+a_4)\left(\beta^2-\beta\right)+a_2\left(\beta^4-\beta^2\right)=0. \end{cases}$$

This indicates that $\beta\left(\beta^2-1\right)a_2=\left(\beta^4-\beta^2\right)a_2$. Hence $\beta=1$, a contradiction.
(2) Consider the subcase $c(x)=1+a_1\,x+a_2\,x^2+a_3\,x^{5i+1}+a_4\,x^{5i+2}$ with $1\le i\le p-1$ and $a_1,\ a_2,\ a_3,\ a_4\in\mathbb{F}_p^*$. It can be verified that

$$\begin{cases} 1+a_1+a_2+a_3+a_4=0, \\ 1+a_1\,\beta+a_2\,\beta^2+a_3\,\beta+a_4\,\beta^2=0, \\ 1+a_1\,\beta^2+a_2\,\beta^4+a_3\,\beta^2+a_4\,\beta^4=0 \end{cases}$$

since $c\,(1)=c\,(\beta)=c\left(\beta^2\right)=0$. Then one can derive that

$$\begin{cases} (a_2+a_4)\left(\beta^2-\beta\right)=\beta-1, \\ (a_2+a_4)\left(\beta^4-\beta^3\right)=\beta-1. \end{cases}$$

It follows that $\beta^3 = \beta$, which is impossible.
(3) Consider the subcase $c(x) = 1 + a_1 x + a_2 x^2 + a_3 x^{5i+2} + a_4 x^{5i+3}$ with $1 \le i \le p-1$ and $a_1, a_2, a_3, a_4 \in \mathbb{F}_p^*$. The fact $c(1) = c(\beta) = c\left(\beta^2\right) = 0$ and Lemma 6 induces that

$$a_1 = -\frac{\beta^2 + \beta + 1}{\beta^2}, \quad a_2 + a_3 = \frac{\beta^2 + \beta + 1}{\beta^3}, \quad a_4 = -\frac{1}{\beta^3}. \tag{31}$$

It follows from $c^{(1)}(1) = c^{(1)}\left(\beta^2\right) = 0$ that

$$\begin{cases} a_1 + 2 a_2 + (5i+2) a_3 + (5i+3) a_4 = 0, \\ a_1 + 2 a_2 \beta^2 + (5i+2) a_3 \beta^2 + (5i+3) a_4 \beta^4 = 0. \end{cases}$$

This yields

$$\left(\beta^2 - 1\right) a_1 + (5i+3)\left(\beta^2 - \beta^4\right) a_4 = 0.$$

By substituting (31), one can deduce that

$$\beta^2 - (5i+2)\beta + 1 = 0.$$

Let $t = 5i + 2$. Then $\beta^2 = t\beta - 1$ and

$$\beta^4 + \beta^3 + \beta^2 + \beta + 1 = (t\beta - 1)(t^2 + t - 1) = 0.$$

It follows that $t^2 + t = 1$. By $c^{(2)}(1) = 0$ and (31), we get

$$5i\,(t+1)\, a_3 = (t+2)\,\beta + 1.$$

The fact $c^{(1)}(1) = 0$ indicates $5i\, a_3 = (2-t)(\beta+1)$. Hence

$$(t+2)\beta + 1 = (t+1)(2-t)(\beta+1).$$

This leads to $t^2\beta - 2t = 0$ due to $t^2 + t = 1$. It follows from $t \ne 0$ that $t\beta = 2$ and $\beta^2 = t\beta - 1 = 1$, a contradiction.
(4) Consider the subcase $c(x) = 1 + a_1 x + a_2 x^2 + a_3 x^{5i+3} + a_4 x^{5i+4}$ with $1 \le i \le p-2$ and $a_1, a_2, a_3, a_4 \in \mathbb{F}_p^*$. It can be checked that

$$\begin{cases} 1 + a_1 + a_2 + a_3 + a_4 = 0, \\ 1 + a_1 \beta + a_2 \beta^2 + a_3 \beta^3 + a_4 \beta^4 = 0, \\ 1 + a_1 \beta^2 + a_2 \beta^4 + a_3 \beta + a_4 \beta^3 = 0 \end{cases}$$

since $c(1) = c(\beta) = c\left(\beta^2\right) = 0$. Then one can derive that

$$\begin{cases} a_1 = -\beta^3 a_4 + \beta^2 + \beta, \\ a_2 = -\left(\beta^4 + 1\right) a_4 - \beta - 1, \\ a_3 = -\left(\beta^2 + \beta + 1\right) a_4 - \beta^2. \end{cases} \tag{32}$$

Let $t = 5i + 2$. By $c^{(1)}(1) = c^{(1)}\left(\beta^2\right) = 0$ and (32), we have

$$\begin{cases} t\beta^2 + \beta + 2 = \left((t-1)\beta^4 + t\beta^3 + t\right) a_4, \\ 2\beta^2 + \beta + t = \left(t\beta^2 + (t-1)\beta + t\right) a_4. \end{cases} \tag{33}$$

Then

$$(t\beta^2 + \beta + 2)\left(t\beta^2 + (t-1)\beta + t\right) = (2\beta^2 + \beta + t)\left((t-1)\beta^4 + t\beta^3 + t\right)$$

which implies

$$(t^2 + t - 1)(\beta^2 - 1) = 0.$$

Thus $t^2+t=1$. It follows from $c^{(2)}(1)=0$ that $2\,a_2+a_3+(2t+3)\,a_4=0$. Together with (32), one can immediately get

$$\left(-\beta^4+\beta^3+2t+1\right)a_4=\beta^2+2\beta+2.$$

Combining with the second equality in (33), we can obtain

$$\left(-\beta^4+\beta^3+2t+1\right)\left(2\beta^2+\beta+t\right)=\left(\beta^2+2\beta+2\right)\left(t\beta^2+(t-1)\beta+t\right).$$

By expanding the above equality, one can deduce

$$\left(\beta^2-1\right)t+3\beta^2+2=0$$

which yields $t=\frac{3\beta^2+2}{1-\beta^2}$. The fact $t^2+t-1=0$ induces

$$\left(\frac{3\beta^2+2}{1-\beta^2}\right)^2+\frac{3\beta^2+2}{1-\beta^2}-1=0$$

which is equivalent to

$$\left(3\beta^2+2\right)^2+\left(3\beta^2+2\right)\left(1-\beta^2\right)-\left(1-\beta^2\right)^2=0.$$

It follows that

$$\beta^4+3\,\beta^2+1=0$$

which indicates

$$2\,\beta^2-\beta^3-\beta=0$$

due to $\beta^4+\beta^3+\beta^2+\beta+1=0$. Hence $\beta(\beta-1)^2=0$, which is impossible.

(5) Consider the subcase $c(x)=1+a_1\,x+a_2\,x^2+a_3\,x^{5i+4}+a_4\,x^{5i+5}$ with $0\le i\le p-2$ and $a_1,\ a_2,\ a_3,\ a_4\in\mathbb{F}_p^*$. It follows from $c(1)=c(\beta)=c\left(\beta^2\right)=0$ that $p\nmid(a_4+1)$ and

$$a_1=-\frac{1}{\beta}\,(a_4+1)\,,\quad a_2=-\frac{\beta}{\beta+1}\,(a_4+1)\,,\quad a_3=\frac{1}{\beta(\beta+1)}\,(a_4+1) \tag{34}$$

due to Lemma 6. The fact $c^{(1)}(1)=c^{(1)}\left(\beta^2\right)=0$ leads to

$$\begin{cases} a_1+2\,a_2+(5i+4)\,a_3+(5i+5)\,a_4=0,\\ a_1+2\,a_2\,\beta^2+(5i+4)\,a_3\,\beta+(5i+5)\,a_4\,\beta^3=0\end{cases}$$

which implies

$$\begin{cases} \left(\beta^3-1\right)a_1+2\left(\beta^3-\beta^2\right)a_2+(5i+4)\left(\beta^3-\beta\right)a_3=0,\\ 2\,(\beta+1)\,a_2+(5i+4)\,a_3+(5i+5)\left(\beta^2+\beta+1\right)a_4=0.\end{cases}$$

By substituting (34), one can obtain that

$$\beta^4+(5i+3)\,\beta^3-(5i+3)\,\beta-1=0 \tag{35}$$

and

$$\left(-2\beta^2\,(\beta+1)+5i+4\right)(a_4+1)+(5i+5)\,\beta\,(\beta+1)\left(\beta^2+\beta+1\right)a_4=0. \tag{36}$$

Let $t=5i+3$. It follows from (35) that

$$\beta^4-1+t\left(\beta^3-\beta\right)=\left(\beta^2-1\right)\left(\beta^2+1+t\,\beta\right)=0$$

which yields $\beta^2 = -t\beta - 1$. Then we have

$$0 = \beta^4 + \beta^3 + \beta^2 + \beta + 1 = -\left(t^2 - t - 1\right)\beta^2$$

which indicates $t^2 = t + 1$ due to $\beta^2 \neq 0$. It can be verified that

$$\begin{aligned}
&-2\beta^2(\beta+1) + 5i + 4 + (5i+5)\beta(\beta+1)\left(\beta^2+\beta+1\right) \\
&= -2\beta^3 - 2\beta^2 + t + 1 - (t+2)\left(\beta^4 + \beta + 2\right) \\
&= -2t(\beta+1) + 2(t\beta+1) + (t+2)(\beta+t) - (t+2)\beta - t - 3 = 0.
\end{aligned}$$

Hence (36) and $a_4 \in \mathbb{F}_p^*$ induces

$$0 = -2\beta^2(\beta+1) + 5i + 4 = 3 - t$$

which means that $t = 3$ and $\beta^2 = -3\beta - 1$, a contradiction with the inequality (3) in Lemma 6.

As a consequence, $\mathcal{C}$ is an MDS $(5p,\ 8)_p$ symbol-pair code. The desired result follows.

□

References

1. Cassuto Y., Blaum M.: Codes for symbol-pair read channels. In: Proceedings of IEEE International Symposium Information Theory (ISIT), pp. 988–992 (2010).
2. Cassuto Y., Blaum M.: Codes for symbol-pair read channels. IEEE Trans. Inf. Theory **57**(12), 8011–8020 (2011).
3. Cassuto Y., Litsyn S.: Symbol-pair codes: algebraic constructions and asymptotic bounds. In: Proceedings of IEEE International Symposium Information Theory (ISIT), pp. 2348–2352 (2011).
4. 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).
5. 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).
6. 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).
7. Chen B., Lin L., Liu H.: Constacyclic symbol-pair codes: lower bounds and optimal constructions. IEEE Trans. Inf. Theory **63**(12), 7661–7666 (2017).
8. Ding B., Ge G., Zhang J., Zhang T., Zhang Y.: New constructions of MDS symbol-pair codes. Des. Codes Cryptogr. **86**(4), 841–859 (2018).
9. Ding B., Zhang T., Ge G.: Maximum distance separable codes for b-symbol read channels. Finite Fields Appl. **49**(1), 180–197 (2018).
10. Dinh H.Q., Nguyen B.T., Singh A.K., Sriboonchitta S.: Hamming and symbol-pair distances of repeated-root constacyclic codes of prime power lengths over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. IEEE Commun. Letters **22**(12), 2400–2403 (2018).
11. 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).
12. Dinh H.Q., Nguyen B.T., Sriboonchitta S.: MDS symbol-pair cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$. IEEE Trans. Inf. Theory **66**(1), 240–262 (2020).
13. Dinh H.Q., Wang X., Liu H., Sriboonchitta S.: On the symbol-pair distances of repeated-root constacyclic codes of length $2p^s$. Discret Math. **342**(11), 3062–3078 (2019).
14. Elishco O., Gabrys R., Yaakobi E.: Bounds and constructions of codes over symbol-pair read channels. IEEE Trans. Inf. Theory **66**(3), 1385–1395 (2020).
15. Horii S., Matsushima T., Hirasawa S.: Linear programming decoding of binary linear codes for symbol-pair read channels. In: Proceedings of IEEE International Symposium Information Theory (ISIT), pp. 1944–1948 (2016).
16. Huffman W.C., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge, U.K. (2003).

17. Kai X., Zhu S., Li P.: A construction of new MDS symbol-pair codes. IEEE Trans. Inf. Theory **61**(11), 5828–5834 (2015).
18. 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).
19. 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).
20. Liu S., Xing C., Yuan C.: List decodability of symbol-pair codes. IEEE Trans. Inf. Theory **65**(8), 4815–4821 (2019).
21. Ma J., Luo J.: MDS symbol-pair codes from repeated-root cyclic codes. Des. Codes Cryptogr. **90**(1), 121–137 (2022).
22. Ma J., Luo J.: On symbol-pair weight distribution of MDS codes and simplex codes over finite fields. Cryptogr. Commun. **13**(1), 101–115 (2021).
23. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North. Holland, Amsterdam (1977).
24. Massey J.L., Costello D.J., Justesen J.: Polynomial weights and code constructions. IEEE Trans. Inf. Theory **IT-19**(1), 101–110 (1973).
25. Morii M., Hirotomo M., Takita M.: Error-trapping decoding for cyclic codes over symbol-pair read channels. In: Proceedings of IEEE International Symposium Information Theory (ISIT), pp. 681–685 (2016).
26. Sun Z., Zhu S., Wang L.: The symbol-pair distance distribution of a class of repeated-root cyclic codes over $\mathbb{F}_{p^m}$. Cryptogr. Commun. **10**(4), 643–653 (2018).
27. Takita M., Hirotomo M., Morii M.: Syndrome decoding of symbol-pair codes. IEICE Trans. A **98**(12), 2423–2428 (2015).
28. Yaakobi E., Bruck J., Siegel P. H.: Decoding of cyclic codes over symbol-pair read channels. In: Proceedings of IEEE International Symposium Information Theory (ISIT), pp. 2891–2895 (2012).