Des. Codes Cryptogr. (2017) 84:359–372
DOI 10.1007/s10623-016-0271-y

Constructions of maximum distance separable symbol-pair codes using cyclic and constacyclic codes

Shuxing Li[1] · Gennian Ge[2,3]

Received: 13 January 2016 / Revised: 30 June 2016 / Accepted: 8 August 2016 /
Published online: 19 August 2016

Abstract Symbol-pair code is a new coding framework which is proposed to correct errors in the symbol-pair read channel. In particular, maximum distance separable (MDS) symbol-pair codes are a kind of symbol-pair codes with the best possible error-correction capability. Employing cyclic and constacyclic codes, we construct three new classes of MDS symbol-pair codes with minimum pair-distance five or six. Moreover, we find a necessary and sufficient condition which ensures a class of cyclic codes to be MDS symbol-pair codes. This condition is related to certain property of a special kind of linear fractional transformations. A detailed analysis on these linear fractional transformations leads to an algorithm, which produces many MDS symbol-pair codes with minimum pair-distance seven.

Keywords Algebraic construction · Constacyclic codes · Cyclic codes · Linear fractional transformations · MDS symbol-pair codes · Symbol-pair codes

Mathematics Subject Classification 68P20 · 94B15 · 94B60

1 Introduction

Motivated by high-density storage applications, a new coding framework named symbol-pair code was proposed in [1,2] to correct errors in the so-called symbol-pair read channel. Consider a scenario where we want to read data from certain storage medium. When the data is written in a very compact way and our data reader has relatively low resolution, instead

Communicated by C. Mitchell.

✉ Gennian Ge
gnge@zju.edu.cn

1 School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, Zhejiang, China

2 School of Mathematical Sciences, Capital Normal University, Beijing 100048, China

3 Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing 100048, China

of individual symbols, we can only receive overlapping pairs of symbols. Suppose the data symbols belong to an alphabet Σ. Then, what we receive are pairs of symbols belonging to a different alphabet $\Sigma \times \Sigma$. In order to recover the original data reliably, we need a new coding scheme which is able to correct errors in this symbol-pair read channel.

Cassuto and Blaum laid the foundation of symbol-pair codes in [1,2], which play the roles of error-correcting codes for the symbol-pair read channel. They presented several bounds and constructions, as well as a decoding algorithm for symbol-pair codes. The construction of symbol-pair codes are further studied in a series of papers, including algebraic constructions [3,5,7] and combinatorial constructions [5]. Moreover, an efficient decoding algorithm of cyclic symbol-pair codes is proposed in [8].

In [5], the authors derived a Singleton-type bound for symbol-pair codes. Consequently, the concept of maximum distance separable (MDS) symbol-pair codes is proposed. The construction of MDS symbol-pair codes is interesting because they have the best possible capability against errors in the symbol-pair read channel. In general, there are two ways to construct MDS symbol-pair codes. The first one is direct construction using linear codes with appropriate properties, such as MDS codes [5], as well as cyclic and constacyclic codes [7]. The second way is recursive construction employing the interleaving technique [4,5], the Eulerian graph [4,5,7] and other combinatorial configurations [4,5].

In particular, we focus on the construction of $(n, d_p)_q$ MDS symbol-pair code whose minimum pair-distance d_p is small. The known parameters of $(n, d_p)_q$ MDS symbol-pair codes with small d_p are the following ones:

(a) $q \geq 2, n \geq 2, d_p \in \{2, 3\}$ [5],
(b) $q \geq 2, n \geq 4, d_p = 4$ [5],
(c1) q is an even prime power, $n \leq q + 2, d_p = 5$ [5],
(c2) q is an odd prime, $5 \leq n \leq 2q + 3, d_p = 5$ [5],
(c3) q is a prime power, $n \mid q^2 - 1, n > q + 1, d_p = 5$ [7],
(c4) q is a prime power, $n = q^2 + q + 1, d_p = 5$ [7],
(c5) $q \equiv 1 \pmod 3$ is a prime power, $n = \frac{q^2+q+1}{3}, d_p = 5$ [7],
(d1) q is a prime power, $n = q^2 + 1, d_p = 6$ [7],
(d2) q is an odd prime power, $n = \frac{q^2+1}{2}, d_p = 6$ [7],
(e) q is an odd prime, $n = 8, d_p = 7$ [5].

In this paper, we follow the idea in [7] to construct MDS symbol-pair codes by employing cyclic and constacyclic codes. We use $v_p(n)$ to denote the largest integer a, such that $p^a \mid n$, where p is a prime. We obtain the following new classes of $(n, d_p)_q$ MDS symbol-pair codes with $d_p \in \{5, 6\}$.

(1) Let q be a prime power. Let n and r be two integers such that

$$r \mid q - 1,\ nr \mid q^3 - 1,\ nr \nmid q - 1,\ \left(\frac{q-1}{r}, n\right) = 1.$$

Then there exists an $(n, d_p)_q$ MDS symbol-pair code with $d_p = 5$.

(2) Let q be a prime power, Let n and r be two integers such that

$$nr \mid (q-1)(q^2+1),\ nr \nmid q^2 - 1,\ \left(\frac{q-1}{r}, n\right) = 1.$$

Then there exists an $(n, d_p)_q$ MDS symbol-pair code with $d_p = 6$.

(3) Let q be a prime power. Suppose $n \mid q^2 - 1$, n is odd or n is even and $v_2(n) < v_2(q^2 - 1)$, then there exists an $(n, d_p)_q$ MDS symbol-pair code with $d_p = 6$.

We remark that the class (1) (resp. class (2)) is an extension of the classes (c4) and (c5) (resp. classes (d1) and (d2)). More interestingly, for a class of cyclic codes, we find a necessary and sufficient condition which guarantees them to be MDS symbol-pair codes with minimum pair-distance $d_p = 7$. We observe that this condition is related to the property of a special kind of linear fractional transformations. Moreover, we present a detailed analysis of these linear fractional transformations, which leads to a precise characterization of this condition. Using this characterization, we obtain many examples of MDS symbol-pair codes with minimum pair-distance $d_p = 7$.

The rest of this paper is organized as follows. Section 2 gives a brief introduction to cyclic and constacyclic codes. Some preliminaries concerning symbol-pair codes and MDS symbol-pair codes are also presented. Employing cyclic and constacyclic codes, several constructions of MDS symbol-pair codes are presented in Section 3. Section 4 concludes the paper.

2 Preliminaries

2.1 Cyclic and constacyclic codes

Let q be a prime power, $\mathbb{F}_q$ be a finite field and $\omega \in \mathbb{F}_q^*$. An ω-constacyclic code $\mathcal{C}$ is a linear code which is invariant under the constacyclic shift. Namely, if

$$(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C},$$

then

$$(\omega c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}.$$

An ω-constacyclic code $\mathcal{C}$ of length n over $\mathbb{F}_q$ can be identified with an ideal of the principal ideal ring $\mathbb{F}_q[x]/(x^n - \omega)$. Thus, $\mathcal{C}$ can be generated by one element. There is a unique monic polynomial $g(x) \in \mathbb{F}_q[x]$ of minimum degree in $\mathcal{C}$, such that $g(x) \mid x^n - \omega$ and $\mathcal{C} = \langle g(x) \rangle$. This polynomial is called the *generator polynomial* of $\mathcal{C}$. Given the ring $\mathbb{F}_q[x]/(x^n - \omega)$ and a generator polynomial $g(x)$, an ω-constacyclic code $\mathcal{C} = \langle g(x) \rangle$ of length n is determined, which is a linear subspace of $\mathbb{F}_q^n$ with dimension $n - \deg(g(x))$. When $\omega = 1$, an ω-constacyclic code is simply a cyclic code.

Suppose $\omega \in \mathbb{F}_q^*$ is an element of order r and m is the smallest integer such that $nr \mid q^m - 1$. Then we can find an element $\delta \in \mathbb{F}_{q^m}^*$ of order nr, such that $\omega = \delta^n$. Therefore the roots of $x^n - \omega$ are of the form $\{\delta^{1+jr} \mid 0 \le j \le n-1\}$. Define $\Omega = \{1 + jr \mid 0 \le j \le n-1\}$. For $s \in \Omega$, the q-cyclotomic coset modulo nr containing s is defined to be $C_s = \{q^i s \pmod{nr} \mid 0 \le i \le m-1\}$. Since $g(x) \in \mathbb{F}_q[x]$ and $g(x) \mid x^n - \omega$, we have $g(x) = \prod_{s \in S} \prod_{j \in C_s} (x - \delta^j)$, where $S \subset \Omega$ is a subset of representatives of the q-cyclotomic cosets modulo nr.

For cyclic codes, we have the well-known BCH bound on the minimum distance. Similarly, we have the following BCH-type bound on the minimum distance of a constacyclic code, which is a slight generalization of [7, Theorem 3].

Proposition 1 *Let q be a prime power and n be a positive integer with $(n, q) = 1$. Let $\omega \in \mathbb{F}_q^*$ be an element of order r. Let m be the smallest positive integer such that $nr \mid q^m - 1$. Then there exists $\delta \in \mathbb{F}_{q^m}^*$, such that δ has order nr and $\omega = \delta^n$. Define $\xi = \delta^r$. Let $\mathcal{C} = \langle g(x) \rangle \subset \mathbb{F}_q[x]/(x^n - \omega)$ be an ω-constacyclic code with length n. Let l be an integer with $(l, n) = 1$ and d be an integer with $1 \le d \le n - 1$. Suppose each element of $\{\delta\xi^{li} \mid b \le i \le b + d - 1\}$*

is a root of the generator polynomial $g(x)$, where b is an arbitrary integer. Then the minimum distance of $\mathcal{C}$ is at least $d+1$.

Proof The condition $(n, q) = 1$ ensures that $g(x)$ has no repeated roots. Since each element belonging to $\{\delta\xi^{li} \mid b \le i \le b+d-1\}$ is a root of $g(x)$, the matrix

$$\begin{pmatrix} 1 & \delta\xi^{bl} & \dots & \delta^{n-1}\xi^{(n-1)bl} \\ 1 & \delta\xi^{(b+1)l} & \dots & \delta^{n-1}\xi^{(n-1)(b+1)l} \\ \vdots & \vdots & & \vdots \\ 1 & \delta\xi^{(b+d-1)l} & \dots & \delta^{n-1}\xi^{(n-1)(b+d-1)l} \end{pmatrix}$$

is a submatrix of the parity matrix of $\mathcal{C}$. Employing the condition $(l, n) = 1$ and the property of the Vandermonde matrix, we conclude that any submatrix of the above one with d columns must be nonsingular. Consequently, the minimum distance of $\mathcal{C}$ is at least $d+1$. □

2.2 Symbol-pair codes and MDS symbol-pair codes

Let Σ be an alphabet consisting of q elements. Given $\mathbf{u} = (u_0, u_1, \dots, u_{n-1}) \in \Sigma^n$, the *symbol-pair read vector* of $\mathbf{u}$ is defined to be

$$\pi(\mathbf{u}) = ((u_0, u_1), (u_1, u_2), \dots, (u_{n-2}, u_{n-1}), (u_{n-1}, u_0)) \in (\Sigma \times \Sigma)^n.$$

Let $\mathbf{u} = (u_0, u_1, \dots, u_{n-1}) \in \Sigma^n$ and $\mathbf{v} = (v_0, v_1, \dots, v_{n-1}) \in \Sigma^n$, the *pair-distance* between $\mathbf{u}$ and $\mathbf{v}$ is

$$d_P(\mathbf{u}, \mathbf{v}) = |\{0 \le i \le n-1 \mid (u_i, u_{i+1}) \ne (v_i, v_{i+1})\}|,$$

where the subscripts are regarded as integers modulo n. An $(n, M, d_p)_q$ symbol-pair code is a subset $\mathcal{C} \subset \Sigma^n$ with $|\mathcal{C}| = M$, such that $d_p = \min\{d_P(\mathbf{u}, \mathbf{v}) \mid \mathbf{u}, \mathbf{v} \in \mathcal{C}, \mathbf{u} \ne \mathbf{v}\}$. If Σ is a finite field $\mathbb{F}_q$, define the *pair-weight* of $\mathbf{u} \in \mathbb{F}_q^n$ to be

$$w_P(\mathbf{u}) = |\{0 \le i \le n-1 \mid (u_i, u_{i+1}) \ne (0, 0)\}|,$$

where the subscripts are regarded as integers modulo n. In particular, if the $(n, M, d_p)_q$ symbol-pair code $\mathcal{C}$ is a linear subspace of $\mathbb{F}_q^n$, then $d_p = \min\{w_P(\mathbf{u}) \mid \mathbf{u} \in \mathcal{C}, \mathbf{u} \ne (0, 0, \dots, 0)\}$.

Let $\mathbf{u} = (u_0, u_1, \dots, u_{n-1})$ be the original vector. Let

$$((u'_0, u''_1), (u'_1, u''_2), \dots, (u'_{n-2}, u''_{n-1}), (u'_{n-1}, u''_0)) \in (\Sigma \times \Sigma)^n$$

be the received vector via the symbol-pair read channel. Then the number of *pair errors* is defined to be

$$\left|\left\{0 \le i \le n-1 \mid (u_i, u_{i+1}) \ne (u'_i, u''_{i+1})\right\}\right|$$

where the subscripts are regarded as integers modulo n. Similar to the classical error-correcting codes, an $(n, M, d_p)_q$ symbol-pair code can correct up to $\lfloor \frac{d_p-1}{2} \rfloor$ pair errors [2, Proposition 3]. Hence, given q, n and M, we aim to construct symbol-pair codes with d_p as large as possible. To this end, we want to take advantage of the fruitful results concerning classical error-correcting codes. A first step is to understand the connection between symbol-pair codes and classical error-correcting codes.

The pair-distance was first introduced in [1,2], which has been shown to be a well-defined metric. Recall that the Hamming distance between $\mathbf{u} = (u_0, u_1, \dots, u_{n-1})$ and $\mathbf{v} = (v_0, v_1, \dots, v_{n-1})$ is defined to be

$$d_H(\mathbf{u}, \mathbf{v}) = |\{0 \le i \le n-1 \mid u_i \ne v_i\}|.$$

In order to build a connection between the pair-distance and the Hamming distance, we need the following definition.

Definition 2 Let S be a subset of $\{0, 1, \ldots, n-1\}$. Thus, the elements of S can be regarded as elements of $\mathbb{Z}_n$, the ring of integers modulo n. S can be partitioned into a union of subsets, such that each subset consists of elements of $\mathbb{Z}_n$, which are consecutive in the sense of modulo n. Clearly, the partition of S with smallest number of subsets is unique. Therefore, we define $L(S)$ to be the number of subsets in this unique partition.

The following proposition reveals the connection between the pair-distance and the Hamming distance.

Proposition 3 [2, Proposition 1 and Theorem 2] *Let* $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ *and* $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ *be two vectors of* Σ^n *with* $0 < d_H(\mathbf{u}, \mathbf{v}) < n$. *Define* $S = \{0 \le i \le n-1 \mid u_i \ne v_i\}$. *Then*

$$d_P(\mathbf{u}, \mathbf{v}) = d_H(\mathbf{u}, \mathbf{v}) + L(S).$$

Therefore, we have $L(S) = d_P(\mathbf{u}, \mathbf{v}) - d_H(\mathbf{u}, \mathbf{v}) \le n - d_H(\mathbf{u}, \mathbf{v})$. *Together with* $1 \le L(S) \le d_H(\mathbf{u}, \mathbf{v})$, *we have*

$$d_H(\mathbf{u}, \mathbf{v}) + 1 \le d_P(\mathbf{u}, \mathbf{v}) \le \min\{2d_H(\mathbf{u}, \mathbf{v}), n\}.$$

In addition,

$$d_P(\mathbf{u}, \mathbf{v}) = \begin{cases} 0 & if\ d_H(\mathbf{u}, \mathbf{v}) = 0, \\ n & if\ d_H(\mathbf{u}, \mathbf{v}) = n. \end{cases}$$

In particular, for linear symbol-pair codes, we have the following corollary concerning the relation between the Hamming weight and the pair-weight of a codeword.

Corollary 4 *Let* $\mathcal{C}$ *be an* $(n, M, d_p)_q$ *symbol-pair code, which is a linear subspace of* $\mathbb{F}_q^n$. *For any* $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, *define*

$$I(\mathbf{c}) = L(\{0 \le i \le n-1 \mid c_i \ne 0\}).$$

Suppose $0 < w_H(\mathbf{c}) < n$, *where* $w_H(\mathbf{c})$ *denotes the Hamming weight of* $\mathbf{c}$. *Then we have*

$$w_P(\mathbf{c}) = w_H(\mathbf{c}) + I(\mathbf{c}). \tag{1}$$

Therefore, we have $I(\mathbf{c}) = w_P(\mathbf{c}) - w_H(\mathbf{c}) \le n - w_H(\mathbf{c})$. *Together with* $1 \le I(\mathbf{c}) \le w_H(\mathbf{c})$, *we have*

$$w_H(\mathbf{c}) + 1 \le w_P(\mathbf{c}) \le \min\{2w_H(\mathbf{c}), n\}.$$

In particular, if the minimum Hamming distance of $\mathcal{C}$ *is* $d < n$, *then the minimum pair distance*

$$d + 1 \le d_p \le \min\{2d, n\}. \tag{2}$$

Similar to classical error-correcting codes, there are several bounds providing fundamental restrictions on the parameters of symbol-pair codes. One of them is the following Singleton-type bound.

Proposition 5 [5, Theorem 2.1] *Let* $q \ge 2$ *and* $2 \le d \le n$. *If* $\mathcal{C}$ *is an* $(n, M, d_p)_q$ *symbol-pair code, then* $M \le q^{n-d_p+2}$.

The symbol-pair code $\mathcal{C}$ achieving this Singleton-type bound is called an MDS symbol-pair code. We denote it by an $(n, d_p)_q$ MDS symbol-pair code. Below, we focus on the direct construction of MDS symbol-pair codes. In fact, classical MDS codes directly generate MDS symbol-pair codes.

Proposition 6 [5, Proposition 3.1] *If $\mathcal{C}$ is an MDS code, then $\mathcal{C}$ is an MDS symbol-pair code. Moreover, if $\mathcal{C}$ is an $[n, n-d+1, d]_q$ MDS code with $d < n$, then $\mathcal{C}$ is an $(n, d+1)_q$ MDS symbol-pair code.*

Together with the knowledge concerning classical MDS codes, the above proposition implies that we have known a systematic construction for $(n, d_p)_q$ MDS symbol-pair codes with q being a prime power and $2 \le d_p \le n \le q+1$. Below, we will focus on the construction of $(n, d_p)_q$ MDS symbol-pair codes with q being a prime power and $n > q+1$.

We observe that if $\mathcal{C}$ is a constacyclic code and is not MDS, then the lower bound in (2) can be improved.

Proposition 7 *Let $\mathcal{C}$ be an $[n, k, d]_q$ constacyclic code with generator polynomial $g(x)$ and $d \le n-k$. Let $c(x) \in \mathcal{C}$ be a codeword with Hamming weight $d' \le n-k$. Then we have $I(c(x)) \ge 2$ and $w_P(c(x)) \ge d'+2$. In particular, $\mathcal{C}$ is an $(n, q^k, d_p)_q$ symbol-pair code with $d_p \ge d+2$.*

Proof It suffices to show that $I(c(x)) \ge 2$, which implies $w_P(c(x)) \ge d'+2$ by (1). Otherwise, we must have $I(c(x)) = 1$. This implies the indices of nonzero entries in $c(x)$ form one consecutive subset. Without loss of generality, we can assume that $c(x) = \sum_{i=0}^{d'-1} c_i x^i$, where $c_i \in \mathbb{F}_q^*$ for each $0 \le i \le d'-1$. Note that $g(x) \mid c(x)$. This leads to a contradiction since $\deg(g(x)) = n-k \ge d' > \deg(c(x))$. Therefore, we have $w_P(c(x)) \ge d'+2$. In particular, since $\mathcal{C}$ is a linear code, the minimum pair-distance of $\mathcal{C}$ equals its minimum nonzero pair-weight. Since $d \le n-k$, we can easily see that $d_p \ge d+2$ by Corollary 4. □

This proposition is an essential ingredient for the constructions in [7] (see [7, Lemma 5]). In the following, we will employ cyclic and constacyclic codes to generate MDS symbol-pair codes.

3 New constructions of MDS symbol-pair codes

Let q be a prime power and n be a positive integer. In this section, we are going to construct $(n, d_p)_q$ MDS symbol-pair codes with $d_p \in \{5, 6, 7\}$.

First, we consider the construction of MDS symbol-pair codes with $d_p = 5$, which extends the results of [7, Theorem 16] and [7, Theorem 19].

Theorem 8 *Let q be a prime power. Let n and r be two positive integers such that*

$$r \mid q-1,\ nr \mid q^3-1,\ nr \nmid q-1,\ (\frac{q-1}{r}, n) = 1.$$

Then there exists an $(n, 5)_q$ MDS symbol-pair code.

Proof Let $\omega \in \mathbb{F}_q^*$ be an element of order r. Let $\delta \in \mathbb{F}_{q^3}^*$ be an element of order nr, such that $\delta^n = \omega$. Since $nr \nmid q-1$, we have $\delta \in \mathbb{F}_{q^3}^* \backslash \mathbb{F}_q$, and the polynomial $g(x) = (x-\delta)(x-\delta^q)(x-\delta^{q^2}) \in \mathbb{F}_q[x]$ divides $x^n - \omega$. Let $\mathcal{C}$ be the ω-constacyclic code $\langle g(x) \rangle \subset \mathbb{F}_q[x]/(x^n-\omega)$. Employing Proposition 1 with $l = \frac{q-1}{r}$, we have the minimum distance of $\mathcal{C}$ is at least three.

In addition, by the Singleton bound, $\mathcal{C}$ is an $[n, n-3, d]_q$ code with $3 \le d \le 4$. A direct application of Propositions 6 and 7 shows that $\mathcal{C}$ is an $(n, 5)_q$ MDS symbol-pair code. □

Remark 9 By [6, Corollary 7.4.4], when $n > 2(q-1)$, the code $\mathcal{C}$ in the above theorem must have minimum distance 3. In addition, when $n = q^2+q+1$, $\mathcal{C}$ is simply the Hamming code with minimum distance 3. In this case, $\mathcal{C}$ also achieves the pair-sphere packing bound [2, Theorem 19].

Next, we provide two constructions of MDS symbol-pair codes with $d_p = 6$. The first one extends the results of [7, Theorem 12] and [7, Theorem 13].

Theorem 10 *Let q be a prime power. Let n and r be two integers such that*

$$r \mid q-1,\ nr \mid (q-1)(q^2+1),\ nr \nmid q^2-1,\ \left(\frac{q-1}{r}, n\right) = 1.$$

Then there exists an $(n, 6)_q$ MDS symbol-pair code.

Proof Let $\omega \in \mathbb{F}_q^*$ be an element of order r. Let $\delta \in \mathbb{F}_{q^4}^*$ be an element of order nr, such that $\delta^n = \omega$. Since $nr \nmid q^2-1$, we have $\delta \in \mathbb{F}_{q^4}^* \backslash \mathbb{F}_{q^2}$, and the polynomial $g(x) = (x-\delta)(x-\delta^q)(x-\delta^{q^2})(x-\delta^{q^3}) \in \mathbb{F}_q[x]$ divides $x^n - \omega$. Let $\mathcal{C}$ be the ω-constacyclic code $\langle g(x) \rangle \subset \mathbb{F}_q[x]/(x^n - \omega)$. Employing Proposition 1 with $l = \frac{q-1}{r}$, we have that the minimum distance of $\mathcal{C}$ is at least three. In addition, by the Singleton bound, $\mathcal{C}$ is an $[n, n-4, d]_q$ code with $3 \le d \le 5$. Below, we are going to show that $d \ne 3$.

Assume the minimum distance of $\mathcal{C}$ is three. Without loss of generality, we have a codeword $1 + a_i x^i + a_j x^j$, where $1 \le i, j \le n-1$, $i \ne j$ and $a_i, a_j \in \mathbb{F}_q^*$. Thus, we have $1 + a_i\delta^i + a_j\delta^j = 0$. Since $nr \mid (q-1)(q^2+1)$, we get

$$(1 + a_i\delta^i)^{(q-1)(q^2+1)} = (-a_j\delta^j)^{(q-1)(q^2+1)} = 1,$$

which implies that $(1 + a_i\delta^i)^{q(q^2+1)} = (1 + a_i\delta^i)^{(q^2+1)}$. A direct computation leads to $\delta^{qi} + \delta^{q^3 i} + a_i\delta^{(q^3+q)i} = \delta^i + \delta^{q^2 i} + a_i\delta^{(q^2+1)i}$. Since $q^3 + q \equiv q^2 + 1 \pmod{nr}$, we have $\delta^{q^3+q} = \delta^{q^2+1}$ and $\delta^{q^3-1} = \delta^{q^2-q}$. Consequently, we have $\delta^{(q-1)i} + \delta^{(q^3-1)i} = 1 + \delta^{(q^2-1)i}$. Noting that $\delta^{q^3-1} = \delta^{q^2-q}$, we have $\delta^{(q-1)i} + \delta^{(q^2-q)i} = 1 + \delta^{(q^2-1)i}$, which implies

$$(\delta^{(q-1)i} - 1)(\delta^{(q^2-q)i} - 1) = 0.$$

This forces that $nr \mid (q-1)i$ for some $1 \le i \le n-1$. However, since $\left(\frac{q-1}{r}, n\right) = 1$, this is impossible.

Hence, the minimum distance of $\mathcal{C}$ is either four or five. It is easily followed from Propositions 6 and 7 that $\mathcal{C}$ is an $(n, 6)_q$ MDS symbol-pair code. □

When $n \mid q^2 - 1$, we have the following construction of $(n, 6)_q$ MDS symbol-pair codes.

Theorem 11 *Let q be a prime power and n be an integer with $n > q+1$ and $n \mid q^2-1$. Then*

(1) *There exists an $(n, 6)_q$ MDS symbol-pair code when n is odd.*
(2) *There exists an $(\frac{n}{2}, 6)_q$ MDS symbol-pair code when n is even.*

Proof (1) Let $\delta \in \mathbb{F}_{q^2}^* \backslash \mathbb{F}_q$ be an element of order n with n being odd. The polynomial $g(x) = (x - \delta^{-q})(x - \delta^{-1})(x - \delta)(x - \delta^q) \in \mathbb{F}_q[x]$ divides $x^n - 1$. Let $\mathcal{C}_1$ be the cyclic code $\langle g(x) \rangle \subset \mathbb{F}_q[x]/(x^n - 1)$. Note that δ^{-1} and δ are two roots of $g(x)$ and $(2, n) = 1$. Employing Proposition 1 with $r = 1, l = 2, b = -1$ and $d = 2$, we can see that δ^{-1} and δ are two consecutive roots and the minimum distance of $\mathcal{C}_1$ is at least three. Together with the Singleton bound, $\mathcal{C}_1$ is an $[n, n-4, d]_q$ code with $3 \le d \le 5$. When $4 \le d \le 5$, it is easily followed from Propositions 6 and 7 that $\mathcal{C}_1$ is an $(n, 6)_q$ MDS symbol-pair code. When $d = 3$, by Propositions 6 and 7, any codeword whose weight is greater than three has pair-weight at least six. Thus, by (1), it suffices to show that for each codeword $c(x) \in \mathcal{C}$ with $w_H(c(x)) = 3$, we have $I(c(x)) \ge 3$. To this end, we are going to show that there is no codeword of the form $1 + a_1 x + a_i x^i$, where $2 \le i \le n-1$ and $a_1, a_i \in \mathbb{F}_q^*$. Below, we will split our discussion into two cases.

Firstly, assume there is a codeword $1 + a_1 x + a_2 x^2$, where $a_1, a_2 \in \mathbb{F}_q^*$. Then we have the following system

$$\begin{cases} 1 + a_1\delta + a_2\delta^2 = 0, \\ 1 + a_1\delta^{-1} + a_2\delta^{-2} = 0. \end{cases}$$

By solving this system, one can see that $a_1 = -(\delta + \frac{1}{\delta})$. Therefore, we have $\delta + \frac{1}{\delta} \in \mathbb{F}_q^*$. Thus, $(\delta + \frac{1}{\delta})^q = \delta + \frac{1}{\delta}$, which implies that $(\delta^{q+1} - 1)(\delta^{q-1} - 1) = 0$. Then, we have either $\delta^{q+1} = 1$ or $\delta^{q-1} = 1$. Namely, we have either $n \mid q+1$ or $n \mid q-1$. This is impossible because $n > q + 1$.

Secondly, assume there is a codeword $1 + a_1 x + a_i x^i$, where $3 \le i \le n-2$ and $a_1, a_i \in \mathbb{F}_q^*$. Then we have the following system

$$\begin{cases} 1 + a_1\delta + a_i\delta^i = 0, \\ 1 + a_1\delta^{-1} + a_i\delta^{-i} = 0. \end{cases}$$

By solving the system, one can see that $a_1 = -\frac{\delta^{2i}-1}{\delta^{2i-1}-\delta}$ and $a_i = \frac{\delta^{i+1}-\delta^{i-1}}{\delta^{2i-1}-\delta}$. Therefore, we have $\frac{\delta^{2i}-1}{\delta^{2i-1}-\delta}, \frac{\delta^{i+1}-\delta^{i-1}}{\delta^{2i-1}-\delta} \in \mathbb{F}_q^*$. Since

$$\frac{\delta^{2i} - 1}{\delta^{2i-1} - \delta} + \frac{\delta^{i+1} - \delta^{i-1}}{\delta^{2i-1} - \delta} = \frac{\delta^{i+1} - 1}{\delta^i - \delta} \in \mathbb{F}_q^*,$$

and

$$\frac{\delta^{2i} - 1}{\delta^{2i-1} - \delta} - \frac{\delta^{i+1} - \delta^{i-1}}{\delta^{2i-1} - \delta} = \frac{\delta^{i+1} + 1}{\delta^i + \delta} \in \mathbb{F}_q,$$

we have

$$\frac{\delta^i - \delta}{\delta^{i+1} - 1} + \frac{\delta^{i+1} + 1}{\delta^i + \delta} = \frac{(\delta^{2i} - 1)(\delta^2 + 1)}{(\delta^i + \delta)(\delta^{i+1} - 1)} \in \mathbb{F}_q^*.$$

Note that $\frac{\delta^{2i}-1}{\delta^{2i-1}-\delta} \in \mathbb{F}_q^*$ and $\frac{\delta^{i+1}-1}{\delta^i-\delta} \in \mathbb{F}_q^*$. Together with the above equation, we have

$$\frac{(\delta^{2i-1} - \delta)(\delta^2 + 1)}{(\delta^i + \delta)(\delta^i - \delta)} = \delta + \frac{1}{\delta} \in \mathbb{F}_q^*.$$

However, as shown in the above, $\delta + \frac{1}{\delta} \in \mathbb{F}_q^*$ is impossible.

(2) Let $\delta \in \mathbb{F}_{q^2}^{*}\backslash\mathbb{F}_q$ be an element of order n with n being even. Since $\delta^{\frac{n}{2}} = -1$, the polynomial $g(x) = (x-\delta^{-q})(x-\delta^{-1})(x-\delta)(x-\delta^{q}) \in \mathbb{F}_q[x]$ divides $x^{\frac{n}{2}}+1$. Let $\mathcal{C}_2$ be the (-1)-constacyclic code $\langle g(x)\rangle \subset \mathbb{F}_q[x]/(x^{\frac{n}{2}}+1)$. Note that δ^{-1} and δ are two roots of $g(x)$. Employing Proposition 1 with $r=2$, $l=1$, $b=-1$ and $d=2$, we can see that δ^{-1} and δ are two consecutive roots and the minimum distance of $\mathcal{C}_2$ is at least three. Together with the Singleton bound, $\mathcal{C}_2$ is an $[\frac{n}{2}, \frac{n}{2}-4, d]_q$ code with $3 \le d \le 5$. The remaining part is similar to the proof of (1) and we omit it here. □

Remark 12 For $n \mid q^2-1$, $(n,6)_q$ MDS symbol-pair codes are constructed in Theorem 11, when n is odd or n is even and $v_2(n) < v_2(q^2-1)$. If n is even and $v_2(n) = v_2(q^2-1)$, the construction in Theorem 11 generates codes with minimum distance two, which are not MDS symbol-pair codes.

Remark 13 By [6, Corollary 7.4.4], the code $\mathcal{C}_1$ (resp. $\mathcal{C}_2$) in the above theorem has minimum distance $3 \le d \le 4$ when $n > 2(q-1)$ (resp. $n > 4(q-1)$). Moreover, the codes $\mathcal{C}_1$ and $\mathcal{C}_2$ do have minimum distance 3 in some cases. For instance, when $3 \mid n$, $\mathcal{C}_1$ contains a codeword $1+x^{\frac{n}{3}}+x^{\frac{2n}{3}}$ with weight three and $\mathcal{C}_2$ contains a codeword $1-x^{\frac{n}{6}}+x^{\frac{n}{3}}$ with weight three.

In the following theorem, we will show that under certain condition, MDS symbol-pair codes with minimum pair-distance $d_p = 7$ can be generated from certain cyclic codes.

Theorem 14 *Let q be a prime power and n be a positive integer with $n \mid q^2-1$ and $n > q+1$. Let $\delta \in \mathbb{F}_{q^2}^{*}\backslash\mathbb{F}_q$ be an element of order n. Let $\mathcal{C} \subset \mathbb{F}_q[x]/(x^n-1)$ be an $[n, n-5, d]_q$ cyclic code having generator polynomial $g(x) = (x-\delta^{-q})(x-\delta^{-1})(x-1)(x-\delta)(x-\delta^{q}) \in \mathbb{F}_q[x]$. Then*

(1) *When $5 \le d \le 6$, $\mathcal{C}$ is an $(n,7)_q$ MDS symbol-pair code.*
(2) *When $d=4$ and n is odd, $\mathcal{C}$ is an $(n,7)_q$ MDS symbol-pair code if and only if for each $3 \le i \le n-3$, $\frac{\delta^{i+1}-1}{\delta^{i}-\delta} \notin \mathbb{F}_q^{*}$.*

Proof By the BCH bound and the Singleton bound, the minimum distance $4 \le d \le 6$. We only prove (2) since the proof of (1) is easy. When $d=4$, by Propositions 6 and 7, any codeword whose weight is greater than four has pair-weight at least seven. Thus, by (1), it suffices to show that for each codeword $c(x) \in \mathcal{C}$ with $w_H(c(x)) = 4$, we have $I(c(x)) \ge 3$. Below, we are going to study the necessary and sufficient condition which ensures this restriction on codewords of weight four.

Suppose there is a codeword $c(x)$ of weight four, such that $I(c(x)) = 1$. Then without loss of generality, we can assume that $c(x) = 1+a_1x+a_2x^2+a_3x^3$, where $a_1, a_2, a_3 \in \mathbb{F}_q^{*}$. Consequently, the following system holds:

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

By solving this system, we have $a_2 = 1+\delta+\frac{1}{\delta}$. However, $\delta+\frac{1}{\delta} \in \mathbb{F}_q$ implies that $(\delta^{q+1}-1)(\delta^{q-1}-1)=0$. This leads to a contradiction since $n > q+1$.

Suppose there is a codeword $c(x)$ of weight four, such that $I(c(x)) = 2$. Then without loss of generality, we have the following two cases

(i) There is a codeword $c(x) = 1+a_1x+a_2x^2+a_ix^i$, where $3 \le i \le n-2$ and $a_1, a_2, a_i \in \mathbb{F}_q^{*}$.

(ii) There is a codeword $c(x) = 1 + a_1 x + a_i x^i + a_{i+1} x^{i+1}$, where $3 \le i \le n-3$ and $a_1, a_i, a_{i+1} \in \mathbb{F}_q^*$.

For Case (i), we must have the following system:

$$\begin{cases} 1 + a_1 + a_2 + a_i = 0, \\ 1 + a_1\delta + a_2\delta^2 + a_i\delta^i = 0, \\ 1 + a_1\delta^{-1} + a_2\delta^{-2} + a_i\delta^{-i} = 0. \end{cases}$$

By solving this system, we have

$$\frac{a_1}{a_2} = -\frac{\delta^{i-2} - \delta}{\delta^{i-1} - 1} - 1, \quad a_2 = \frac{\delta^i - 1}{\delta^{i-1} - \delta},$$

which implies

$$\frac{\delta^{i-2} - \delta}{\delta^{i-1} - 1} \in \mathbb{F}_q \setminus \{-1\}, \quad \frac{\delta^i - 1}{\delta^{i-1} - \delta} \in \mathbb{F}_q^*.$$

Thus,

$$\frac{\delta^{i-1} - 1}{\delta^{i-2} - \delta} - \frac{\delta^i - 1}{\delta^{i-1} - \delta} = \frac{\delta^{i-2}(\delta + 1)(\delta - 1)^2}{(\delta^{i-1} - \delta)(\delta^{i-2} - \delta)} \in \mathbb{F}_q^*,$$
$$\frac{\delta^{i-1} - \delta}{\delta^i - 1} - \frac{\delta^{i-2} - \delta}{\delta^{i-1} - 1} = \frac{\delta^{i-1}(\delta - 1)^2}{(\delta^i - 1)(\delta^{i-1} - 1)} \in \mathbb{F}_q^*.$$

By comparing the right hand side of the above two equations, we have $1 + \frac{1}{\delta} \in \mathbb{F}_q^*$, which is impossible.

For Case (ii), we must have the following system:

$$\begin{cases} 1 + a_1 + a_i + a_{i+1} = 0, \\ 1 + a_1\delta + a_i\delta^i + a_{i+1}\delta^{i+1} = 0, \\ 1 + a_1\delta^{-1} + a_i\delta^{-i} + a_{i+1}\delta^{-(i+1)} = 0. \end{cases}$$

If n is even, the above system holds if $i = \frac{n}{2}$, $a_1 = a_{\frac{n}{2}+1} = -1$ and $a_{\frac{n}{2}} = 1$. Hence, the condition of n being odd is necessary. By solving the above system, we have

$$a_1 = -\frac{\delta^{i+1} - 1}{\delta^i - \delta}, \quad a_i = \frac{\delta^{i+1} - 1}{\delta^i - \delta}, \quad a_{i+1} = -1.$$

Thus, the above system does not hold, if and only if for each $3 \le i \le n-3$, $\frac{\delta^{i+1}-1}{\delta^i - \delta} \notin \mathbb{F}_q^*$. Therefore, we complete the proof. $\square$

Given an integer $3 \le i \le n-3$, $\frac{\delta^{i+1}-1}{\delta^i-\delta} = \theta \in \mathbb{F}_q^*$ is equivalent to $\delta^i = \frac{1-\theta\delta}{-\theta+\delta}$ for $\theta \in \mathbb{F}_q^*$. Thus, the necessary and sufficient condition in 2) of Theorem 14 is related to the property of the linear fractional transformation $\frac{1-\theta\delta}{-\theta+\delta}$ with respect to δ, where $\theta \in \mathbb{F}_q^*$. This provides a motivation to study this special type of linear fractional transformation. Using the result derived in the Appendix, we have the following theorem which gives a more precise characterization of the necessary and sufficient condition.

Theorem 15 *Let q be a prime power and n be an integer with $n \mid q^2 - 1$ and $n > q + 1$. Let $\delta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ be an element of order n. Let $x^2 - bx - c$ be the monic minimal polynomial of δ over $\mathbb{F}_q$. For an integer $i \ge 2$, define*

$$a_0^{(i)} = \sum_{j=0}^{\lfloor \frac{i-2}{2} \rfloor} \binom{i-2-j}{j} b^{i-2-2j} c^{j+1}, \quad a_1^{(i)} = \sum_{j=0}^{\lfloor \frac{i-1}{2} \rfloor} \binom{i-1-j}{j} b^{i-1-2j} c^{j}. \tag{3}$$

Let $\mathcal{C} \subset \mathbb{F}_q[x]/(x^n-1)$ be an $[n, n-5, d]_q$ cyclic code having generator polynomial $g(x) = (x-\delta^{-q})(x-\delta^{-1})(x-1)(x-\delta)(x-\delta^q)$. Then $\mathcal{C}$ is an $[n, n-5, d]_q$ code with $4 \le d \le 6$. When $5 \le d \le 6$, $\mathcal{C}$ is an $(n, 7)_q$ MDS symbol-pair code. When $d = 4$ and n is odd, $\mathcal{C}$ is an $(n, 7)_q$ MDS symbol-pair code if and only if for each $3 \le i \le n-3$, one of the following holds:

(1) $a_1^{(i)} = 0$,

or when $a_1^{(i)} \neq 0$,

(2) *if* $a_1^{(i)} = 1$, *then* $a_0^{(i)} \neq -b$ *or* $c = 1$,

(3) *if* $a_0^{(i)} = 0$, *then* $a_1^{(i)} \neq \frac{1}{c}$ *or* $b = 0$,

(4) *if* $a_0^{(i)} \neq 0$ *and* $a_1^{(i)} \neq 1$, *then* $a_1^{(i)} c = 1$ *or* $\frac{a_1^{(i)} b + a_0^{(i)}}{a_1^{(i)} - 1} \neq \frac{a_1^{(i)} c - 1}{a_0^{(i)}}$.

Proof The conclusion is a direct application of Theorem 14 and Corollary 18. □

Remark 16 By the sphere packing bound, when $n(n-1) \ge \frac{2q^5}{(q-1)^2}$, the code $\mathcal{C}$ in the above theorem has minimum distance $d = 4$.

The above theorem and remark suggest an algorithm which aim to construct $(n, 7)_q$ MDS symbol-pair codes with $n \mid q^2 - 1$, $n(n-1) \ge \frac{2q^5}{(q-1)^2}$ and n being odd. We run a numerical experiment for all pairs

$$\{(q, n) \mid q \text{ prime power}, q \le 100, n \mid q^2 - 1, n \text{ odd}, n > q + 1\}.$$

For these instances, the corresponding $[n, n-5, d]_q$ code $\mathcal{C}$ in Theorem 15 always has $d = 4$. The code $\mathcal{C}$ is an $(n, 7)_q$ MDS symbol-pair code whenever q is odd, except for $(q, n) \in \{(59, 435), (67, 561), (83, 861)\}$. Moreover, the experimental result suggests that $\mathcal{C}$ is not an MDS symbol-pair code when q is even. However, it seems not easy to prove that q being odd is a necessary condition for $\mathcal{C}$ being an $(n, 7)_q$ MDS symbol-pair code.

4 Conclusion

Following the idea in [7], we use cyclic and constacyclic codes to construct MDS symbol-pair codes with minimum pair-distance $d_p \in \{5, 6, 7\}$ in this paper. Our constructions extend the results in [7]. Moreover, we derive a necessary and sufficient condition which ensures a class of cyclic code to be MDS symbol-pair codes. This condition is related to the property of a special kind of linear fractional transformations. We study these linear fractional transformations in detail and propose a more precise characterization of the necessary and sufficient condition. This characterization leads to an algorithm aiming to construct MDS symbol-pair codes with minimum pair-distance $d_p = 7$. We believe that a deeper understanding on this characterization may bring new classes of MDS symbol-pair codes.

We observe that most of the known constructions of $(n, d_p)_q$ MDS symbol-pair codes focus on the case where d_p is small. In this case, if we use an $[n, k, d]_q$ linear code to construct a symbol-pair code, then the difference $d_p - d$ is necessarily small. Thus, it is relatively easy to show that the required minimum pair-distance is achieved. It is an interesting research problem to consider the constructions of MDS symbol-pair codes with large minimum pair-distances.

Acknowledgements The authors wish to thank the anonymous reviewers for their comments which are very helpful to improve the paper. The first author would like to express his gratitude to Prof. Maosheng Xiong, Hong Kong University of Science and Technology, for the enlightening discussions on this topic. The research of G. Ge is supported by the National Natural Science Foundation of China under Grant Nos. 11431003 and 61571310.

Appendix

Let q be a prime power. For $u, v, w, z \in \mathbb{F}_q$ and $\delta \in \mathbb{F}_{q^2}$, define a linear fractional transformation from $\mathbb{F}_{q^2}$ to $\mathbb{F}_{q^2}$ by

$$f_{u,v,w,z}(\delta) = \frac{u + v\delta}{w + z\delta},$$

where $w + z\delta \neq 0$ and $uz - vw \neq 0$. We further assume that $z \neq 0$, since otherwise, $f_{u,v,w,z}$ degenerates into a linear function. Below, we will study this special kind of linear fractional transformation. In particular, suppose $\delta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$, we will present a necessary and sufficient condition such that

$$\delta^i = \frac{u + v\delta}{w + z\delta}$$

for some integer i. This condition provides a criterion to determine whether the linear fractional transformation $f_{u,v,w,z}$ maps δ to an element belonging to the multiplicative cyclic group generated by δ.

Proposition 17 *Let $\delta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Let $x^2 - bx - c$ be the monic minimal polynomial of δ over $\mathbb{F}_q$. For an integer $i \geq 2$, define*

$$a_0^{(i)} = \sum_{j=0}^{\lfloor \frac{i-2}{2} \rfloor} \binom{i-2-j}{j} b^{i-2-2j} c^{j+1}, \quad a_1^{(i)} = \sum_{j=0}^{\lfloor \frac{i-1}{2} \rfloor} \binom{i-1-j}{j} b^{i-1-2j} c^j. \tag{4}$$

Then for $i \geq 0$, $\delta^i = \frac{u+v\delta}{w+z\delta}$ if and only if one of the following holds:

(1) *If $i = 0$, then $u = w$, $v = z$.*
(2) *If $i = 1$, then $b = \frac{v-w}{z}$ and $c = \frac{u}{z}$.*
(3) *If $i \geq 2$, then*

$$a_1^{(i)} \neq 0, \quad b = -\frac{a_0^{(i)}}{a_1^{(i)}} + \frac{v}{z a_1^{(i)}} - \frac{w}{z}, \quad c = -\frac{w a_0^{(i)}}{z a_1^{(i)}} + \frac{u}{z a_1^{(i)}}.$$

Proof (1) and (2) are trivial. We only consider (3) below. Since $\delta^i = \frac{u+v\delta}{w+z\delta}$ and $z \neq 0$, we have $\delta^{i+1} + \frac{w}{z}\delta^i - \frac{v}{z}\delta - \frac{u}{z} = 0$. Therefore, δ is a root of the polynomial $x^{i+1} + \frac{w}{z}x^i - \frac{v}{z}x - \frac{u}{z}$ and

$$x^{i+1} + \frac{w}{z}x^i - \frac{v}{z}x - \frac{u}{z} \equiv 0 \pmod{x^2 - bx - c}.$$

For an integer $i \geq 0$, we define a polynomial $T_i(x) = x^{i+1} + \frac{w}{z}x^i$. For any $i \geq 2$, we have the following recurrence relation:

$$\begin{aligned}
T_i(x) &\equiv x^{i+1} + \frac{w}{z}x^i \\
&\equiv bx^i + cx^{i-1} + \frac{w}{z}(bx^{i-1} + cx^{i-2}) \\
&\equiv b(x^i + \frac{w}{z}x^{i-1}) + c(x^{i-1} + \frac{w}{z}x^{i-2}) \\
&\equiv bT_{i-1}(x) + cT_{i-2}(x) \pmod{x^2 - bx - c}.
\end{aligned}$$

By employing this recurrence relation repeatedly, we have

$$\begin{aligned}
T_i(x) &\equiv d_2^{(i)}T_2(x) + d_1^{(i)}T_1(x) \\
&\equiv e_1^{(i)}T_1(x) + e_0^{(i)}T_0(x) \pmod{x^2 - bx - c},
\end{aligned}$$

where $d_1^{(i)}, d_2^{(i)}, e_0^{(i)}, e_1^{(i)} \in \mathbb{F}_q$. Now, we aim to determine $e_0^{(i)}$ and $e_1^{(i)}$ explicitly. The recurrence relation implies that $T_0(x)$ necessarily originates from $T_2(x)$ by subtracting a proper multiple of $x^2 - bx - c$. Since $T_2(x) \equiv bT_1(x) + cT_0(x) \pmod{x^2 - bx - c}$, we have $e_0^{(i)} = cd_2^{(i)}$. Apparently, $d_2^{(i)}$ is a summation of monomials regarding of b and c. More precisely, suppose $i-2$ can be expressed as an ordered sum containing $i-2-2j$ ones and j twos. Then this ordered sum corresponds to a monomial $b^{i-2-2j}c^j$ in the summation of $d_2^{(i)}$. Recall that there are $\binom{i-2-j}{j}$ ways to decompose $i-2$ into distinct ordered sums containing $i-2-2j$ ones and j twos. Therefore, we have

$$d_2^{(i)} = \sum_{j=0}^{\lfloor \frac{i-2}{2} \rfloor} \binom{i-2-j}{j} b^{i-2-2j}c^j,$$

and

$$e_0^{(i)} = cd_2^{(i)} = \sum_{j=0}^{\lfloor \frac{i-2}{2} \rfloor} \binom{i-2-j}{j} b^{i-2-2j}c^{j+1} = a_0^{(i)}.$$

Similarly, by analyzing the decomposition of $i-1$ into ordered sums consisting of ones and twos, we have

$$e_1^{(i)} = \sum_{j=0}^{\lfloor \frac{i-1}{2} \rfloor} \binom{i-1-j}{j} b^{i-1-2j}c^j = a_1^{(i)}.$$

Consequently,

$$\begin{aligned}
x^{i+1} + \frac{w}{z}x^i - \frac{v}{z}x - \frac{u}{z} &\equiv T_i(x) - \frac{v}{z}x - \frac{u}{z} \\
&\equiv a_1^{(i)}T_1(x) + a_0^{(i)}T_0(x) - \frac{v}{z}x - \frac{u}{z} \\
&\equiv a_1^{(i)}x^2 + (a_0^{(i)} + \frac{wa_1^{(i)}}{z} - \frac{v}{z})x + \frac{wa_0^{(i)}}{z} - \frac{u}{z} \\
&\equiv 0 \pmod{x^2 - bx - c}.
\end{aligned}$$

Hence, we must have $a_1^{(i)} \neq 0$ and $x^2 + (\frac{a_0^{(i)}}{a_1^{(i)}} + \frac{w}{z} - \frac{v}{za_1^{(i)}})x + \frac{wa_0^{(i)}}{za_1^{(i)}} - \frac{u}{za_1^{(i)}} = x^2 - bx - c$. The conclusion follows by comparing the coefficients. □

Particularly, given $\delta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ and an integer $i \geq 2$, we have the following easy criterion to determine if $\delta^i = \frac{1-\theta\delta}{-\theta+\delta}$ for some $\theta \in \mathbb{F}_q^*$.

Corollary 18 *Let $\delta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Let $x^2 - bx - c$ be the monic minimal polynomial of δ over $\mathbb{F}_q$. For an integer $i \geq 2$, $\delta^i = \frac{1-\theta\delta}{-\theta+\delta}$ for some $\theta \in \mathbb{F}_q^*$ if and only if $a_1^{(i)} \neq 0$ and one of the following condition holds*

1) If $a_1^{(i)} = 1$, then $a_0^{(i)} = -b$ and $c \neq 1$,
2) If $a_0^{(i)} = 0$, then $a_1^{(i)} = \frac{1}{c}$ and $b \neq 0$,
3) If $a_0^{(i)} \neq 0$ and $a_1^{(i)} \neq 1$, then $a_1^{(i)}c \neq 1$ and $\frac{a_1^{(i)}b+a_0^{(i)}}{a_1^{(i)}-1} = \frac{a_1^{(i)}c-1}{a_0^{(i)}}$.

where $a_0^{(i)}$ and $a_1^{(i)}$ are defined in (4). Moreover, let $\mathbb{F}_r$ be a subfield of $\mathbb{F}_q$. If $b, c \in \mathbb{F}_r$, then $\delta^i = \frac{1-\theta\delta}{-\theta+\delta}$ for some $i \geq 2$ only if $\theta \in \mathbb{F}_r$.

Proof By setting $u = z = -1$ and $v = w = \theta$ in Proposition 17, we have $\delta^i = \frac{1-\theta\delta}{-\theta+\delta}$ for some $\theta \in \mathbb{F}_q^*$ if and only if

$$b = \frac{(a_1^{(i)} - 1)\theta - a_0^{(i)}}{a_1^{(i)}}, \quad c = \frac{a_0^{(i)}\theta + 1}{a_1^{(i)}}.$$

If $a_0^{(i)} = 0$ and $a_1^{(i)} = 1$, then we have $b = 0$ and $c = 1$, which is impossible since $x^2 - 1$ is reducible over $\mathbb{F}_q$. If either $a_1^{(i)} = 1$ or $a_0^{(i)} = 0$, then the Condition 1) or the Condition 2) holds. If $a_0^{(i)} \neq 0$ and $a_1^{(i)} \neq 1$, the Condition 3) is derived from the expressions of b and c. Suppose b and c belong to a subfield $\mathbb{F}_r$, then $a_0^{(i)}, a_1^{(i)} \in \mathbb{F}_r$ by definition. Since we have either $a_0^{(i)} \neq 0$ or $a_1^{(i)} \neq 1$, it is easy to see that $\theta \in \mathbb{F}_r$. □

References

1. Cassuto, Y., Blaum, M.: Codes for symbol-pair read channels. In: Proceedings of the International Symposium on Information Theory, 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 the International Symposium on Information Theory, pp. 2348–2352 (2011)
4. Chee, Y.M., Kiah, H.M., Wang, C.: Maximum distance separable symbol-pair codes. In: Proceedings of the International Symposium on Information Theory, pp. 2886–2890 (2012)
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. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
7. Kai, X., Zhu, S., Li, P.: A construction of new MDS symbol-pair codes. IEEE Trans. Inf. Theory **61**(11), 5828–5834 (2015)
8. Yaakobi, E., Bruck, J., Siegel, P.H.: Decoding of cyclic codes over symbol-pair read channels. In: Proceedings of the International Symposium on Information Theory, pp. 2891–2895 (2012)