

A construction of optimal locally recoverable codes

Xiaoru Li · Ziling Heng

Received: date / Accepted: date

Abstract Locally recoverable codes are widely used in distributed and cloud storage systems. The objective of this paper is to present a construction of near MDS codes with oval polynomials and then determine the locality of the codes. It turns out that the near MDS codes and their duals are both distance-optimal and dimension-optimal locally recoverable codes. The lengths of the locally recoverable codes are different from known ones in the literature.

Keywords Linear code · near MDS code · locally recoverable codes

Mathematics Subject Classification (2010) 94B05 · 94A05

1 Introduction

Let \mathbb{F}_q be the finite field with q elements, where q is a power of a prime p . Let $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$.

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ with \mathcal{C} a non-empty set. Then \mathcal{C} is said to be an $[n, k, d]$ linear code over \mathbb{F}_q if it is a k -dimensional linear subspace over \mathbb{F}_q , where d denotes its minimal distance. Define the dual of an $[n, k, d]$ linear code \mathcal{C} by

$$\mathcal{C}^\perp = \{ \mathbf{u} \in \mathbb{F}_q^n : \langle \mathbf{u}, \mathbf{c} \rangle = 0 \forall \mathbf{c} \in \mathcal{C} \},$$

where $\langle \mathbf{u}, \mathbf{c} \rangle$ denotes the Euclidean inner product of \mathbf{u} and \mathbf{c} . It is obvious that \mathcal{C}^\perp is an $[n, n - k]$ linear code. Denote by A_i the number of codewords of weight i in an $[n, k]$ linear code \mathcal{C} for $0 \leq i \leq n$. The polynomial $A(z) = 1 + A_1z + A_2z^2 + \cdots + A_nz^n$ is referred to as the *weight*

X. Li and Z.Heng are with the School of Science, Chang'an University, Xi'an, 710064, China. E-mail: lixiaoru@163.com, zilingheng@chd.edu.cn

Z. Heng's research was supported in part by the National Natural Science Foundation of China under Grant 11901049, in part by the Young Talent Fund of University Association for Science and Technology in Shaanxi, China, under Grant 20200505 and in part by the Fundamental Research Funds for the Central Universities, CHD, under Grant 300102122202.

enumerator of \mathcal{C} . The weight enumerator is an interesting research project as it not only contains the error detection and error correction capabilities of the code, but also is useful for calculating the error probability of error detection. In recent years, the weight enumerators of linear codes were widely studied in the literature [2, 3, 8, 10, 11, 19, 20].

Linear codes achieving or nearly achieving the Singleton bound are important in both theory and practice. Linear codes of parameters $[n, k, n - k + 1]$ are called MDS (maximum distance separable) codes. An $[n, k, n - k]$ linear code is said to be almost maximum distance separable (AMDS for short). A linear code is referred to as a near maximum distance separable (near MDS or NMDS for short) code provided that both this code and its dual are AMDS. Constructions of MDS, AMDS and NMDS as well as their applications were investigated in [2–4, 9, 16–22].

Locally recoverable codes (LRCs for short) are widely used in distributed data storage systems. A LRC with locality r is a block code such that any symbol in the encoding is a function of r other symbols. In this letter, we only consider linear LRCs. Denote by $[n] = \{0, 1, \dots, n - 1\}$ with n a positive integer. For an $[n, k, d]$ linear code \mathcal{C} over \mathbb{F}_q , let the coordinates of the codewords in \mathcal{C} be indexed by the elements in $[n]$. For any $i \in [n]$, if there always exist a subset $R_i \subseteq [n] \setminus i$ with $|R_i| = r$ and a function $f_i(x_1, x_2, \dots, x_r)$ over \mathbb{F}_q^r such that $c_i = f_i(\mathbf{c}_{R_i})$ for any $\mathbf{c} = (c_0, \dots, c_{n-1}) \in \mathcal{C}$, then \mathcal{C} is referred to as an $(n, k, d, q; r)$ -LRC, where \mathbf{c}_{R_i} is the projection of \mathbf{c} at R_i and the set R_i is called the repair set of c_i . There exist some tradeoffs between the parameters of LRCs. For any $(n, k, d, q; r)$ -LRC, the Singleton-like bound (see [1]) is given by

$$d \leq n - k - \left\lceil \frac{k}{r} \right\rceil + 2. \quad (1)$$

LRCs are said to be distance-optimal if they achieve this bound. For any $(n, k, d, q; r)$ -LRC, the Cadambe-Mazumdar bound (see [6]) is given as

$$k \leq \min_{t \in \mathbb{Z}^+} [rt + k_{opt}^{(q)}(n - t(r + 1), d)], \quad (2)$$

where $k_{opt}^{(q)}(n, d)$ denotes the largest possible dimension of a linear code of length n , minimum distance d over \mathbb{F}_q , \mathbb{Z}^+ denotes the set of all positive integers. LRCs are called dimension-optimal if they achieve the Cadambe-Mazumdar bound. Constructing distance-optimal or dimension-optimal LRCs is an interesting research topic. In [7] and [18], AMDS and NMDS codes were used to derive optimal or nearly optimal locally recoverable codes. Hence it is interesting to construct new AMDS or NMDS codes with desired locality.

In [20], several families of NMDS codes with some special matrixes were constructed. The objective of this paper is to present a construction of NMDS codes with larger lengths than those in [20] and then determine the locality of the codes. It turns out that the NMDS codes and their duals are both distance-optimal and dimension-optimal LRCs.

The rest of this paper is organized as follows. In Section 2, we present some preliminaries on NMDS codes and oval polynomials. In Section 3, we construct a family of $[q + 5, 3, q + 2]$ NMDS codes with $q = 2^m$. In Section 4, the localities of the NMDS codes and their duals are determined. In Section 4, we conclude this paper and give some remarks.

2 Preliminaries

Let $(1, A_1, \dots, A_n)$ and $(1, A_1^\perp, \dots, A_n^\perp)$ respectively denote the weight distributions of a linear code \mathcal{C} and its dual \mathcal{C}^\perp with length n . The weight distributions of an NMDS code and its dual satisfy the following recurrence relations.

Lemma 1 ([4]) *Let \mathcal{C} be an $[n, k]$ NMDS code over \mathbb{F}_q . Then*

$$A_{k+s}^\perp = \binom{n}{k+s} \sum_{j=0}^{s-1} (-1)^j \binom{k+s}{j} (q^{s-j} - 1) + (-1)^s \binom{n-k}{s} A_k^\perp$$

for $s \in \{1, 2, \dots, n-k\}$; and

$$A_{n-k+s} = \binom{n}{k-s} \sum_{j=0}^{s-1} (-1)^j \binom{n-k+s}{j} (q^{s-j} - 1) + (-1)^s \binom{k}{s} A_{n-k}$$

for $s \in \{1, 2, \dots, k\}$.

The following theorem shows an interesting property of NMDS codes.

Lemma 2 ([5]) *Let \mathcal{C} be an NMDS code and $\text{suppt}(\mathbf{c}) = \{1 \leq i \leq n : c_i \neq 0\}$ denote the support of $\mathbf{c} = (c_1, \dots, c_n) \in \mathcal{C}$. Then for any minimum weight codeword \mathbf{c} in \mathcal{C} , there exists, up to a multiple, a unique minimum weight codeword \mathbf{c}^\perp in \mathcal{C}^\perp satisfying $\text{suppt}(\mathbf{c}) \cap \text{suppt}(\mathbf{c}^\perp) = \emptyset$. Besides, \mathcal{C} and \mathcal{C}^\perp have the same number of minimum weight codewords.*

Next we list the definition and some properties of oval polynomial used in this letter.

Definition 1 [13] *Let $q = 2^m$ with $m \geq 2$. If $f \in \mathbb{F}_q[x]$ is a polynomial satisfying*

1. f is a permutation polynomial of \mathbb{F}_q with $\deg(f) < q$ and $f(0) = 0, f(1) = 1$;
2. for each $a \in \mathbb{F}_q$, $g_a(x) := (f(x+a) + f(a))x^{q-2}$ is also a permutation polynomial of \mathbb{F}_q ,

then f is called an oval polynomial.

To construct near MDS codes over \mathbb{F}_q in the paper, we need concrete oval polynomials over \mathbb{F}_q . Some known infinite families of oval polynomials are listed in the following.

Theorem 1 [15, Table 1] *Let $m \geq 2$ be an integer. The following are oval polynomials of \mathbb{F}_q , where $q = 2^m$.*

- The translation polynomial $f(x) = x^{2^h}$, where $\gcd(h, m) = 1$.
- The Segre polynomial $f(x) = x^6$, where m is odd.
- The Glynn oval polynomial $f(x) = x^{3 \times 2^{(m+1)/2} + 4}$, where m is odd.
- The Glynn oval polynomial $f(x) = x^{2^{(m+1)/2} + 2^{(m+1)/4}}$ for $m \equiv 3 \pmod{4}$.
- The Glynn oval polynomial $f(x) = x^{2^{(m+1)/2} + 2^{(3m+1)/4}}$ for $m \equiv 1 \pmod{4}$.
- The Cherowitzo oval polynomial $f(x) = x^{2^e} + x^{2^e+2} + x^{3 \times 2^e+4}$, where $e = (m+1)/2$ and m is odd.
- The Payne oval polynomial $f(x) = x^{\frac{2^{m-1}+2}{3}} + x^{2^{m-1}} + x^{\frac{3 \times 2^{m-1}-2}{3}}$, where m is odd.
- The Subiaco polynomial

$$f_a(x) = ((a^2(x^4 + x) + a^2(1 + a + a^2)(x^3 + x^2))(x^4 + a^2x^2 + 1)^{2^{m-2}} + x^{2^{m-1}}),$$

where $\text{Tr}_{q/2}(1/a) = 1$ and $a \notin \mathbb{F}_4$ if $m \equiv 2 \pmod{4}$.

- The Adelaide oval polynomial

$$f(x) = \frac{T(\beta^m)(x+1)}{T(\beta)} + \frac{T((\beta x + \beta^q)^m)}{T(\beta)(x + T(\beta)x^{2^{m-1}} + 1)^{m-1}} + x^{2^{m-1}},$$

where $m \geq 4$ is even, $\beta \in \mathbb{F}_{q^2} \setminus \{1\}$ with $\beta^{q+1} = 1$, $m \equiv \pm(q-1)/3 \pmod{q+1}$, and $T(x) = x + x^q$.

Lemma 3 [14] Let $q = 2^m$ with $m \geq 2$. Then a polynomial f with $f(0) = 0$ over \mathbb{F}_q is an oval polynomial if and only if $f_u := f(x) + ux$ is 2-to-1 for each $u \in \mathbb{F}_q^*$.

Lemma 4 [20] Let $q = 2^m$ with $m \geq 2$. Then f is an oval polynomial over \mathbb{F}_q if and only if the following two conditions hold:

1. f is a permutation polynomial of \mathbb{F}_q ;
- 2.

$$\frac{f(x) + f(y)}{x + y} \neq \frac{f(x) + f(z)}{x + z}$$

for all pairwise different elements x, y, z in \mathbb{F}_q .

Lemma 5 [20] Let $q = 2^m$ with $m \geq 3$ being odd and $f(x)$ be an oval polynomial over \mathbb{F}_q whose coefficients are in \mathbb{F}_2 . Then $f(x) + x + 1 = 0$ has no solution in \mathbb{F}_q .

3 A Construction of NMDS codes

In this section, let $q = 2^m$ where m is an odd integer with $m \geq 3$. For convenience, let $\dim(\mathcal{C})$ and $d(\mathcal{C})$ respectively denote the dimension and minimal distance of a linear code \mathcal{C} . Let f be an oval polynomial over \mathbb{F}_q . Let $\alpha_0 = 0, \alpha_1 = 1, \dots, \alpha_{q-1}$ be all elements of \mathbb{F}_q . Define

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 & 0 & 0 & 1 & 0 & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{q-1} & 0 & 1 & 0 & 1 & 1 \\ f(\alpha_0) & f(\alpha_1) & \cdots & f(\alpha_{q-1}) & 1 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Then G is a 3 by $q + 5$ matrix over \mathbb{F}_q . Let G generate a linear code \mathcal{C} over \mathbb{F}_q . The parameters and weight enumerator of \mathcal{C} are determined in the following theorem.

Theorem 2 *Let m be an odd integer with $m \geq 3$, and let f be an oval polynomial over \mathbb{F}_q . Then \mathcal{C} is a $[q + 5, 3, q + 2]$ NMDS code over \mathbb{F}_q with weight enumerator*

$$A(z) = 1 + \frac{(q-1)(3q+8)}{2}z^{q+2} + \frac{(q-2)(q-1)(q+2)}{2}z^{q+3} + \frac{3(q^2-3q+2)}{2}z^{q+4} + \frac{(q-1)(q-2)^2}{2}z^{q+5}.$$

Proof It is easy to deduce that $\dim(\mathcal{C}) = 3$ as the first, $q+1$ -th and $q+2$ -th columns of the generator matrix G are linearly independent. We then prove that \mathcal{C}^\perp has parameters $[q+5, q+2, 3]$. Obviously, $\dim(\mathcal{C}^\perp) = (q+5) - 3 = q+2$. Since each column of G is nonzero and any two columns of G are linearly independent over \mathbb{F}_q , we have $d(\mathcal{C}^\perp) > 2$. Note that the $q+1$ -th, $q+2$ -th, $q+4$ -th columns of G are linearly dependent. Then $d(\mathcal{C}^\perp) = 3$.

To calculate the total number of codewords of weight 3 in \mathcal{C}^\perp , we consider the following cases.

Case 1.1: Let x, y, z be three pairwise different elements in \mathbb{F}_q . Consider the submatrix

$$M_{1,1} = \begin{bmatrix} 1 & 1 & 1 \\ x & y & z \\ f(x) & f(y) & f(z) \end{bmatrix}.$$

Then $|M_{1,1}| = (x+y)(f(x)+f(z)) + (x+z)(f(x)+f(y)) \neq 0$ by Lemma 4. Hence, \mathcal{C}^\perp has no codeword of weight 3 whose nonzero coordinates are at the first q locations.

Case 1.2: Let x, y be two different elements in \mathbb{F}_q . Consider the submatrix

$$M_{1,2} = \begin{bmatrix} 1 & 1 & 0 \\ x & y & 0 \\ f(x) & f(y) & 1 \end{bmatrix}.$$

Then $|M_{1,2}| = y + x \neq 0$ as $x \neq y$. Hence, \mathcal{C}^\perp has no codeword of weight 3 whose first two nonzero coordinates are at the first q locations and the rest is at the $q+1$ -th location.

Case 1.3: Let x, y be two different elements in \mathbb{F}_q . Consider the submatrix

$$M_{1,3} = \begin{bmatrix} 1 & 1 & 0 \\ x & y & 1 \\ f(x) & f(y) & 0 \end{bmatrix}.$$

Since f is a permutation polynomial and $x \neq y$, then $|M_{1,3}| = f(y) + f(x) \neq 0$. Hence, \mathcal{C}^\perp has no codeword of weight 3 whose first two nonzero coordinates are at the first q locations and the rest is at the $q+2$ -th location.

Case 1.4: Let x, y be two different elements in \mathbb{F}_q . Consider the submatrix

$$M_{1,4} = \begin{bmatrix} 1 & 1 & 1 \\ x & y & 0 \\ f(x) & f(y) & 1 \end{bmatrix}.$$

Then $|M_{1,4}| = (f(y) + 1)x + (f(x) + 1)y$. If $(x, y) = (0, 1)$ or $(1, 0)$, then $|M_{1,4}| \neq 0$ and \mathcal{C} has no codeword of weight 3 whose coordinates are at the first, second and $q + 3$ -th locations. Now we count the number of different pairs (x, y) such that $|M_{1,4}| = 0$, where $x, y \in \mathbb{F}_q \setminus \{0, 1\}$. For any $x \in \mathbb{F}_q \setminus \{0, 1\}$, $|M_{1,4}| = 0$ if and only if

$$\frac{f(x) + 1}{x} = \frac{f(y) + 1}{y}.$$

Let $a := \frac{f(x)+1}{x}$. Then $a \neq 0$ and $a \neq 1$ by Lemma 5. Since $f(z) + az$ is 2-to-1 by Lemma 3, there exists a unique element $y \in \mathbb{F}_q \setminus \{0, 1\}$ such that $f(x) + ax = 1 = f(y) + ay$. For this pair (x, y) , $|M_{1,4}| = 0$ and vice versa. Hence, the number of distinct $(x, y) \in \mathbb{F}_q \setminus \{0, 1\}$ such that $|M_{1,4}| = 0$ equals $(q - 2)/2$. As a result, the number of codewords of weight 3 in \mathcal{C}^\perp whose first two nonzero coordinates are at the first q locations (except the first two locations) and the rest is at the $q + 3$ -th location is equal to $(q - 2)(q - 1)/2$.

Case 1.5: Let x, y be two distinct elements in \mathbb{F}_q . Consider the submatrix

$$M_{1,5} = \begin{bmatrix} 1 & 1 & 0 \\ x & y & 1 \\ f(x) & f(y) & 1 \end{bmatrix}.$$

Then $|M_{1,5}| = f(x) + f(y) + x + y$. $|M_{1,5}| = 0$ is equal to $f(x) + x = f(y) + y$. Note that $f(z) + z$ is 2-to-1 by Lemma 3. If we fix $x \in \mathbb{F}_q$, there exists a unique element $y \in \mathbb{F}_q$ such that $f(x) + x = a = f(y) + y$, where $a \in \mathbb{F}_q$. For this pair (x, y) , $|M_{1,5}| = 0$ and vice versa. Then the number of (x, y) in \mathbb{F}_q such that $|M_{1,5}| = 0$ equals $q/2$. In conclusion, the number of codewords of weight 3 in \mathcal{C}^\perp whose first two nonzero coordinates are at the first q locations and the rest is at the $q + 4$ -th location is equal to $q(q - 1)/2$.

Case 1.6: Let x, y be two different elements in \mathbb{F}_q . Consider the submatrix

$$M_{1,6} = \begin{bmatrix} 1 & 1 & 1 \\ x & y & 1 \\ f(x) & f(y) & 0 \end{bmatrix}.$$

Then $|M_{1,6}| = (x + 1)f(y) + (y + 1)f(x)$. For any $y \in \mathbb{F}_q \setminus \{0, 1\}$, let $a := f(y)/(y + 1)$ which implies $f(y) + ay = a$. Then $a \neq 0$ and $a \neq 1$ by Lemma 5. By Lemma 3, $f(z) + az$ is 2-to-1. Then there exists a unique element $x \in \mathbb{F}_q \setminus \{0, 1\}$ such that $f(x) + ax = a$. For this pair (x, y) , $|M_{1,6}| = 0$ and vice versa. Hence, the number of (x, y) in $\mathbb{F}_q \setminus \{0, 1\}$ satisfying $|M_{1,6}| = 0$ equals $(q - 2)/2$.

Consequently, the number of codewords of weight 3 in \mathcal{C}^\perp whose first two nonzero coordinates are at the first q locations (except the first two locations) and the rest is at the $q + 5$ -th location is equal to $(q - 2)(q - 1)/2$.

Case 1.7: Let x be an element in \mathbb{F}_q . Consider the following three submatrixes as

$$M_{1,7} = \begin{bmatrix} 1 & 0 & 0 \\ x & 0 & 1 \\ f(x) & 1 & 0 \end{bmatrix}, \quad M_{1,8} = \begin{bmatrix} 1 & 0 & 0 \\ x & 0 & 1 \\ f(x) & 1 & 1 \end{bmatrix},$$

$$M_{1,9} = \begin{bmatrix} 1 & 0 & 0 \\ x & 1 & 1 \\ f(x) & 0 & 1 \end{bmatrix}.$$

Then we have $|M_{1,7}| = |M_{1,8}| = |M_{1,9}| = 1$. Hence, \mathcal{C}^\perp has no codeword of weight 3 whose first nonzero coordinate is at the first q locations and the others are at the u -th and v -th locations, where $(u, v) = (q + 1, q + 2)$ or $(q + 1, q + 4)$ or $(q + 2, q + 4)$.

Case 1.8: Let x be an element in \mathbb{F}_q . Consider the submatrix

$$M_{1,10} = \begin{bmatrix} 1 & 0 & 1 \\ x & 0 & 0 \\ f(x) & 1 & 1 \end{bmatrix}.$$

Then $|M_{1,10}| = x$. $|M_{1,10}| = 0$ if and only if $x = 0$. Consequently, the number of codewords of weight 3 in \mathcal{C}^\perp whose nonzero coordinates are at the first, $q + 1$ -th and $q + 3$ -th locations is equal to $q - 1$.

Case 1.9: Let x be an element in \mathbb{F}_q . Consider the submatrix

$$M_{1,11} = \begin{bmatrix} 1 & 0 & 1 \\ x & 0 & 1 \\ f(x) & 1 & 0 \end{bmatrix}.$$

Then $|M_{1,11}| = x + 1$. $|M_{1,11}| = 0$ if and only if $x = 1$. Consequently, the number of codewords of weight 3 in \mathcal{C}^\perp whose nonzero coordinates are at the second, $q + 1$ -th and $q + 5$ -th locations equals $q - 1$.

Case 1.10: Let x be an element in \mathbb{F}_q . Consider the submatrix

$$M_{1,12} = \begin{bmatrix} 1 & 0 & 1 \\ x & 1 & 0 \\ f(x) & 0 & 1 \end{bmatrix}.$$

Then $|M_{1,12}| = f(x) + 1$. Since f is a permutation polynomial of \mathbb{F}_q with $f(0) = 0$, $f(1) = 1$, then $|M_{1,12}| = 0$ if and only if $x = 1$. Consequently, the number of codewords of weight 3 in \mathcal{C}^\perp whose nonzero coordinates are at the second, $q + 2$ -th and $q + 3$ -th locations equals $q - 1$.

Case 1.11: Let x be an element in \mathbb{F}_q . Consider the submatrix

$$M_{1,13} = \begin{bmatrix} 1 & 0 & 1 \\ x & 1 & 1 \\ f(x) & 0 & 0 \end{bmatrix}.$$

Then $|M_{1,13}| = f(x)$. Since f is a permutation polynomial of \mathbb{F}_q with $f(0) = 0$, $f(1) = 1$, then $|M_{1,13}| = 0$ if and only if $x = 0$. Consequently, the number of codewords of weight 3 in \mathcal{C}^\perp whose nonzero coordinates are at the first, $q + 1$ -th and $q + 5$ -th locations is equal to $q - 1$.

Case 1.12: Let x be an element in \mathbb{F}_q . Consider the following three submatrixes as

$$M_{1,14} = \begin{bmatrix} 1 & 1 & 0 \\ x & 0 & 1 \\ f(x) & 1 & 1 \end{bmatrix}, M_{1,15} = \begin{bmatrix} 1 & 1 & 1 \\ x & 0 & 1 \\ f(x) & 1 & 0 \end{bmatrix},$$

$$M_{1,16} = \begin{bmatrix} 1 & 1 & 0 \\ x & 1 & 1 \\ f(x) & 0 & 1 \end{bmatrix}.$$

Then we have $|M_{1,14}| = |M_{1,15}| = |M_{1,16}| = f(x) + x + 1$. By Lemma 5, $f(x) + x + 1 \neq 0$ for $x \in \mathbb{F}_q$. Hence, \mathcal{C}^\perp has no codeword of weight 3 whose first nonzero coordinate is at the first q locations and the others are at the t_1 -th and t_2 -th locations, where $(t_1, t_2) = (q + 3, q + 4)$ or $(q + 3, q + 5)$ or $(q + 4, q + 5)$.

Case 1.13: Let the nonzero coordinates of the codewords with weight 3 in \mathcal{C}^\perp be at three of the last five locations. Then there are ten subcases. Here, we only discuss two subcases of them as the others can be discussed in a similar way. Consider the following two submatrixes as

$$M_{1,17} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}, M_{1,18} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

The ranks of these submatrixes are all 2. Hence, the number of codewords of weight 3 in \mathcal{C}^\perp whose nonzero coordinates are at the $q + 1$ -th, $q + 2$ -th and $q + 4$ -th locations is equal to $q - 1$ and the number of codewords of weight 3 in \mathcal{C}^\perp whose nonzero coordinates are at the last three locations is equal to $q - 1$. For other subcases, the corresponding number of codewords of weight 3 in \mathcal{C}^\perp is 0.

Thanks to the discussions in the above cases, we deduce that $A_3^\perp = \frac{(q-1)(3q+8)}{2}$.

We finally prove that $d(\mathcal{C}) = q+2$. Assume that $d(\mathcal{C}) \leq q+1 = q+5-4$. Let $\mathbf{c} = a\mathbf{g}_1 + b\mathbf{g}_2 + c\mathbf{g}_3$ be a codeword with the minimum weight in \mathcal{C} , where \mathbf{g}_1 , \mathbf{g}_2 and \mathbf{g}_3 respectively represent the first, second and third rows of G . Then at least four coordinates are zero in \mathbf{c} .

Case 2.1: Assume that four of the last five coordinates in \mathbf{c} are zero. Here we suppose the $q+1$ -th, $q+2$ -th, $q+3$ -th, $q+4$ -th coordinates in \mathbf{c} are zero. Then we have

$$\begin{cases} c = 0, \\ b = 0, \\ a + c = 0, \\ b + c = 0. \end{cases}$$

Then $a = b = c = 0$ and $\mathbf{c} = 0$, which contradicts to the fact that \mathbf{c} is a minimum weight codeword in \mathcal{C} . For other subcases, we can similarly obtain this contradiction.

Case 2.2: Assume that three of the last five coordinates in \mathbf{c} are zero. Here we suppose the $q+1$ -th, $q+2$ -th, $q+3$ -th coordinates in \mathbf{c} are zero. Then there exists an element x in \mathbb{F}_q such that

$$\begin{cases} a + bx + cf(x) = 0, \\ c = 0, \\ b = 0, \\ a + c = 0. \end{cases}$$

Then $a = b = c = 0$ and $\mathbf{c} = 0$. This is contrary to the fact that \mathbf{c} is a minimum weight codeword in \mathcal{C} . For other subcases, we can similarly obtain this contradiction.

Case 2.3: Assume that two of the last five coordinates in \mathbf{c} are zero. Here we suppose the $q+1$ -th, $q+2$ -th of the last five coordinates in \mathbf{c} are zero. Then there exist two different elements x and y in \mathbb{F}_q such that

$$\begin{cases} a + bx + cf(x) = 0, \\ a + by + cf(y) = 0, \\ c = 0, \\ b = 0. \end{cases}$$

Then $a = b = c = 0$ and $\mathbf{c} = 0$. This is contrary to the fact that \mathbf{c} is a minimum weight codeword in \mathcal{C} . For other subcases, we can similarly obtain this contradiction.

Case 2.4: Assume that at most one of the last four coordinates in \mathbf{c} is zero. Let x, y, z be three pairwise different elements in \mathbb{F}_q such that

$$\begin{cases} a + bx + cf(x) = 0, \\ a + by + cf(y) = 0, \\ a + bz + cf(z) = 0. \end{cases}$$

By Lemma 4, we can deduce that the rank of the coefficient matrix for this system of equations is 3. Hence, $a = b = c = 0$ and $\mathbf{c} = 0$, which is contrary to the fact that \mathbf{c} is a minimum weight codeword in \mathcal{C} .

Summarizing the above discussions, $d(\mathcal{C}) \geq q + 2$. By the Singleton bound, $d(\mathcal{C}) \leq q + 3$. If $d(\mathcal{C}) = q + 3$, then \mathcal{C} is a $[q + 5, 3, q + 3]$ MDS code whose dual is also an MDS code, which contradicts to the fact that \mathcal{C}^\perp is AMDS. Then $d(\mathcal{C}) = q + 2$, and \mathcal{C} is a $[q + 5, 3, q + 2]$ NMDS code. By Lemma 2, $A_{q+2} = A_3^\perp = \frac{(q-1)(3q+8)}{2}$. Then the weight enumerator of \mathcal{C} follows from Lemma 1.

Example 1 Let $m = 3$ and $f(x) = x^4$. Then the code \mathcal{C} over \mathbb{F}_q has parameters $[13, 3, 10]$ and weight enumerator $A(z) = 1 + 112z^{10} + 210z^{11} + 63z^{12} + 126z^{13}$.

With the first seven families of oval polynomials documented in Theorem 1, we have derived seven infinite families of near MDS codes over $\mathbb{F}(q)$ with parameters $[q + 5, 3, q + 2]$ via Theorem 2. This construction may not work for the Subiaco and Adelaide oval polynomials in general.

4 Optimal locally recoverable codes

In this section, we prove that the NMDS code in Theorem 2 and its dual are both distance-optimal and dimension-optimal LRCs.

For an $[n, k, d]$ linear code \mathcal{C} , denote by $\mathcal{B}_d(\mathcal{C})$ the set of the supports of all codewords with weight d in \mathcal{C} . Denote by $d^\perp = d(\mathcal{C}^\perp)$. Besides, the coordinates of the codewords are indexed with $(0, 1, \dots, n - 1)$.

Lemma 6 ([18]) *Let \mathcal{C} be a linear code with length n and $d(\mathcal{C}) > 1$. Then the minimum linear locality of \mathcal{C} equals $d^\perp - 1$ if and only if*

$$\bigcup_{\mathcal{S} \in \mathcal{B}_{d^\perp}(\mathcal{C}^\perp)} \mathcal{S} = [n].$$

Lemma 7 ([18]) *Let \mathcal{C} be an NMDS code with $d(\mathcal{C}) > 1$, then the minimum linear locality of \mathcal{C} is either $d(\mathcal{C}^\perp) - 1$ or $d(\mathcal{C}^\perp)$.*

Lemma 8 ([18]) *Let \mathcal{C} be an NMDS code. If*

$$\bigcap_{\mathcal{S} \in \mathcal{B}_{d^\perp}(\mathcal{C}^\perp)} \mathcal{S} = \emptyset,$$

then the minimum linear locality of \mathcal{C}^\perp is equal to $d(\mathcal{C}) - 1$.

Theorem 3 *The NMDS code \mathcal{C} in Theorem 2 is a*

$$(q + 5, 3, q + 2, q; 2) - \text{LRC}$$

and \mathcal{C}^\perp is a

$$(q + 5, q + 2, 3, q; q + 1) - \text{LRC}.$$

In addition, \mathcal{C} and \mathcal{C}^\perp are both distance-optimal and dimension-optimal LRCs.

Proof By the proof of Theorem 2, it is easy to deduce that

$$\bigcup_{\mathcal{S} \in \mathcal{B}_3(\mathcal{C}^\perp)} \mathcal{S} = [q + 5]$$

and

$$\bigcap_{\mathcal{S} \in \mathcal{B}_3(\mathcal{C}^\perp)} \mathcal{S} = \emptyset.$$

Then by Lemma 6, the minimum linear locality of \mathcal{C} is $d(\mathcal{C}^\perp) - 1 = 2$. By Theorem 8, the minimum linear locality of \mathcal{C}^\perp is $d(\mathcal{C}) - 1 = q$. Now we prove \mathcal{C} is an optimal LRC. Putting the parameters of the $(q + 5, 3, q + 2, q; 2)$ -LRC into the right-hand side of the Singleton-like bound in (1), we have

$$n - k - \left\lceil \frac{k}{r} \right\rceil + 2 = q + 5 - 3 - \left\lceil \frac{3}{2} \right\rceil + 2 = q + 2.$$

Hence \mathcal{C} is a distance-optimal LRC. Putting $t = 1$ and the parameters of the $(q + 5, 3, q + 2, q; 2)$ -LRC into the right-hand side of the Cadambe-Mazumdar bound in (2), we have

$$k \leq r + k_{opt}^{(q)}(n - (r + 1), d) = 2 + k_{opt}^{(q)}(q + 2, q + 2) = 3,$$

where $k_{opt}^{(q)}(q + 2, q + 2) = 1$ by the classical Singleton bound. Thus, \mathcal{C} is a dimension-optimal LRC. Similarly, we can prove \mathcal{C}^\perp is both distance-optimal and dimension-optimal.

5 Concluding remarks

With the special generator matrix G and an oval polynomial $f(x)$, we presented a construction of $[q + 5, 3, q + 2]$ NMDS code \mathcal{C} in Theorem 2 for $q = 2^m$ and odd m . Then we derived seven infinite families of $[q + 5, 3, q + 2]$ NMDS codes with the first seven families of oval polynomials documented in Theorem 1. The NMDS codes \mathcal{C} and \mathcal{C}^\perp were proved to be both distance-optimal and dimension-optimal LRCs in Theorem 3.

In [12], a class of optimal locally repairable codes of distances 3 and 4 with unbounded length was constructed. We remark that the optimal locally repairable codes in this paper are not contained in [12] as they have different lengths. Finally, we point out that the NMDS codes in this paper have larger lengths than those in [20].

References

1. V. Cadambe, A. Mazumdar, An upper bound on the size of locally recoverable codes, Proc. IEEE Int. Symp. Network Coding (2013) 1–5.
2. C. Ding, Designs from linear codes, World Scientific, Singapore, 2019.
3. C. Ding, C. Tang, Infinite families of near MDS codes holding t -designs, IEEE Trans. Inform. Theory 66 (9) (2020) 5419–5428.
4. S. Dodunekov, I. Landgev, On near-MDS codes, J. Geometry 54 (1995) 30–43.
5. A. Faldum, W. Willems, Codes of small defect, Des. Codes Cryptogr. 10 (1997) 341–350.
6. P. Gopalan, C. Huang, H. Simitci, S. Yekhanin, On the locality of codeword symbols, IEEE Trans. Inform. Theory 58 (11) (2012) 6925–6934.
7. X. Geng, M. Yang, J. Zhang, Z. Zhou, A class of almost MDS codes, Finite Fields Appl. 79 (2022) 101996.
8. Z. Heng, C. Ding, Z. Zhou, Minimal linear codes over finite fields, Finite Fields Appl. 54 (2018) 176–196.
9. D. Huang, Q. Yue, Y. Niu, X. Li, MDS or NMDS self-dual codes from twisted generalized Reed-Solomon codes, Designs Codes Cryptogr. 89 (9) (2021) 2195–2209.
10. C. Li, Q. Yue, F. Li, Weight distributions of cyclic codes with respect to pairwise coprime order elements, Finite Fields Appl. 28 (2014) 94–114.
11. C. Li, P. Wu and F. Liu, On two classes of primitive BCH Codes and some related codes, IEEE Trans. Inform. Theory 65 (6) (2019) 3830–3840.
12. Y. Luo, C. Xing, Y. Chen, Optimal locally repairable codes of distance 3 and 4 via cyclic codes, IEEE Trans. Inform. Theory 65 (2) (2018) 1048–1053.
13. R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
14. A. Maschietti, Difference sets and hyperovals, Des. Codes Cryptogr. 14(1) (1998) 89–98.
15. S. Mesnager, Bent vectorial functions and linear codes from o-polynomials, Des. Codes Cryptogr. 77 (2015) 99–116.
16. X. Shi, Q. Yue, Y. Wu, New quantum MDS codes with large minimum distance and short length from generalized Reed-Solomon codes, Dis. Math. 342 (7) (2019) 1989–2001.
17. X. Shi, Q. Yue, Y. Chang, Some quantum MDS codes with large minimum distance from generalized Reed-Solomon codes, Cryptogr. Commun. 10 (2018) 1165–1182.
18. P. Tan, C. Fan, C. Ding, Z. Zhou, The minimum linear locality of linear codes, arXiv: 2102.00597, 2021.
19. C. Tang, C. Ding, An infinite family of linear codes supporting 4-designs, IEEE Trans. Inform. Theory 67 (1) (2020) 244–254.
20. Q. Wang, Z. Heng, Near MDS codes from oval polynomials, Discrete Math. 344 (4) (2021) 112277.
21. Y. Wu, Twisted Reed-Solomon codes with one-dimensional hull, IEEE Commun. Letters 25(2) (2021)383-386.
22. Y. Wu, J. Y. Hyun, Y. Lee, New LCD MDS codes of non-Reed-Solomon type, IEEE Trans. Inform. Theory 67 (8) (2021) 5069–5078.