Quantum Information Processing (2020) 19:65
https://doi.org/10.1007/s11128-019-2561-6

Entanglement-assisted quantum MDS codes from cyclic codes

Liqi Wang[1] · Shixin Zhu[1] · Zhonghua Sun[1]

Received: 15 June 2019 / Accepted: 23 December 2019 / Published online: 2 January 2020

Abstract
Entanglement-assisted quantum error-correcting codes are a generalization of standard stabilizer quantum error-correcting codes, which can be possibly constructed from any classical codes by relaxing the duality condition and utilizing pre-shared entanglement between the sender and the receiver. In this paper, we construct seven new families of entanglement-assisted quantum maximum-distance-separable codes from cyclic codes by exploiting less pre-shared entangled states. Most of these codes are new in the sense that their parameters are not covered by the codes available in the literature.

Keywords Entanglement-assisted quantum error-correcting codes · Cyclic codes · Cyclotomic cosets

Mathematics Subject Classification 94B15 · 94B65

1 Introduction

Quantum error-correcting (QEC) codes were introduced to reduce decoherence during quantum communications and quantum computations. The stabilizer formalism makes QEC codes that can be constructed from classical codes with certain self-orthogonality (dual-containing) properties. However, the need for such dual-containing forms an obstacle in the development of quantum coding theory. In Brun et al. [1,12], a more general framework named entanglement-assisted stabilizer formalism was introduced and it increases the communication capacity. The related codes are called

✉ Zhonghua Sun
sunzhonghuas@163.com

Liqi Wang
liqiwangg@163.com

Shixin Zhu
zhushixin@hfut.edu.cn

1 School of Mathematics, Hefei University of Technology, Hefei 230601, Anhui, China

entanglement-assisted quantum error-correcting (EAQEC) codes which can be possibly constructed from any classical codes by relaxing the duality condition and utilizing pre-shared entanglement between the sender and the receiver. After that, many scholars have constructed lots of EAQEC codes with good parameters. (see, for example, [6,10,11,16,17,35,36] and the relevant references therein).

Let q be a prime power. A q-ary EAQEC code, denoted by $[[n, k, d; c]]_q$, encodes k information qudits into n channel qudits with the help of c pairs of maximally entangled states and can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors, where d is the minimum distance of the code. Actually, if $c = 0$, it is the standard $[[n, k, d]]_q$ quantum codes. Moreover, if $c = n - k$, it is called a maximal-entanglement EAQEC code.

Similar to quantum Singleton bound, there is also a so-called entanglement-assisted (EA) quantum Singleton bound for EAQEC codes.

Theorem 1 (EA quantum Singleton bound) [1,7,15] *For any* $[[n, k, d; c]]_q$ *EAQEC code with* $d \leqslant \frac{n+2}{2}$, *its parameters satisfy*

$$n + c - k \geqslant 2(d - 1),$$

where $0 \leqslant c \leqslant n - 1$.

An EAQEC code achieving this bound is called an EAQMDS code. If $c = 0$, it is the quantum Singleton bound. As we said before, EAQEC codes can be constructed from classical codes without dual-containing condition, but it is still hard to do so, since it is not an easy task to determine the number of shared pairs in the construction of EAQEC codes. Scholars have proposed several methods to solve this problem, and many EAQEC codes with good parameters have been constructed.

Maximal-entanglement EAQEC codes with small lengths constructed from quaternary zero radical codes were presented in [25]. Qian and Zhang [31] constructed maximal-entanglement EAQEC codes from arbitrary binary linear codes and proved that asymptotically good EAQEC codes exist in binary case. Very recently, Liu et al. [22] generalized [31] to linear codes with k-Galois product and they also constructed some EAQEC codes from matrix-product codes in [21]. Recently, a relationship between the number of maximally shared qudits required to construct an EAQEC code from a classical code and hull of the classical code was obtained in [8], in which EAQEC codes with flexible parameters were also constructed. Meanwhile, codes based on linear codes with complementary duals were also used to construct EAQEC codes in [9] and [32], respectively. In addition, EAQMDS codes were constructed from Reed–Solomon and generalized Reed–Solomon codes in [18,28,29].

Lu et al. [24] utilized the decomposition of the defining set of codes which was introduced in [20], to construct EAQEC codes from BCH codes. Recently, Lu et al. [26] and Chen et al. [2] proposed the concept of decomposition of the defining set of constacyclic codes, which makes the shared qudits c that can be easily determined, and they also constructed some new EAQMDS codes. Since then, many EAQMDS codes have been constructed from constacyclic codes (including cyclic codes and negacyclic codes). Among the obtained results, the lengths of these EAQMDS codes divide $q^2 + 1$ (see, for example, $q^2 + 1$ in [2,27,33,34]; $\frac{q^2+1}{2}$ in [2]; $\frac{q^2+1}{5}$ in [3,13,26];

$\frac{q^2+1}{10}$ in [13,27], etc.), and q^2-1 (see, for example, [2,19,23,26,27,34]). Very recently, Chen et al. [4] also used negacyclic BCH codes to construct EAQEC codes.

In this paper, through the analysis of the intersection of the defining set D of cyclic codes and $-qD$, we obtain several new families of EAQMDS codes of lengths that divide q^2+1 with q being an odd prime power as follows:

(1) $[[\frac{q^2+1}{2}, \frac{q^2+1}{2}-2d+6, d; 4]]_q$, where $q+2 \le d \le 2q-1$ is odd.
(2) $[[\frac{q^2+1}{5}, \frac{q^2+1}{5}-2d+3, d; 1]]_q$, where $q \equiv 3 \pmod{10}$, $q > 3$, $2 \le d \le \frac{4q-2}{5}$ is even.
(3) $[[\frac{q^2+1}{5}, \frac{q^2+1}{5}-2d+7, d; 5]]_q$, where $q \equiv 3 \pmod{10}$, $q > 3$, $\frac{4q+8}{5} \le d \le \frac{6q+2}{5}$ is even.
(4) $[[\frac{q^2+1}{5}, \frac{q^2+1}{5}-2d+3, d; 1]]_q$, where $q \equiv 7 \pmod{10}$, $2 \le d \le \frac{4q+2}{5}$ is even.
(5) $[[\frac{q^2+1}{5}, \frac{q^2+1}{5}-2d+7, d; 5]]_q$, where $q \equiv 7 \pmod{10}$, $\frac{4q+12}{5} \le d \le \frac{6q-2}{5}$ is even.
(6) $[[\frac{q^2+1}{10}, \frac{q^2+1}{10}-2d+6, d; 4]]_q$, where $q \equiv 3 \pmod{10}$, $q > 3$, $\frac{2q+9}{5} \le d \le \frac{4q+3}{5}$ is odd.
(7) $[[\frac{q^2+1}{10}, \frac{q^2+1}{10}-2d+6, d; 4]]_q$, where $q \equiv 7 \pmod{10}$, $\frac{2q+11}{5} \le d \le \frac{4q-3}{5}$ is odd.

The paper is organized as follows. In Sect. 2, some notations and basic results of cyclic codes and EAQEC codes are presented. In Sect. 3, some new families of EAQMDS codes with small pre-shared entangled states are constructed from cyclic codes. The conclusion is given in Sect. 4.

2 Preliminaries

Let q be a prime power and $\mathbb{F}_{q^2}$ be the Galois field with q^2 elements. A q^2-ary linear code $\mathscr{C}$ of length n with dimension k, denoted by $[n,k]_{q^2}$, is a linear subspace of $\mathbb{F}_{q^2}^n$ with dimension k. The number of nonzero components of $\mathbf{c} \in \mathscr{C}$ is said to be the weight $\mathrm{wt}(\mathbf{c})$ of the codeword $\mathbf{c}$. The minimum nonzero weight of all codewords in $\mathscr{C}$ is said to be the minimum distance of $\mathscr{C}$, denoted by $d(\mathscr{C})$. An $[n,k]_{q^2}$ linear code with minimum distance d is denoted by $[n,k,d]_{q^2}$.

Given two vectors $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$, and $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_{q^2}^n$, their Hermitian inner product is defined as

$$\langle \mathbf{x}, \mathbf{y} \rangle := x_0 y_0^q + x_1 y_1^q + \cdots + x_{n-1} y_{n-1}^q.$$

The vectors $\mathbf{x}$ and $\mathbf{y}$ are called orthogonal with respect to the Hermitian inner product if $\langle \mathbf{x}, \mathbf{y} \rangle = 0$. For a q^2-ary linear code $\mathscr{C}$ of length n, the Hermitian dual code of $\mathscr{C}$ is defined as

$$\mathscr{C}^{\perp_H} := \{\mathbf{x} \in \mathbb{F}_{q^2}^n : \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{y} \in \mathscr{C}\}.$$

It is clear that $\mathscr{C}^{\perp_H}$ is a q^2-ary linear code with dimension $n - \dim(\mathscr{C})$.

A q^2-ary linear code $\mathscr{C}$ of length n is called cyclic if it is invariant under the cyclic shift of $\mathbb{F}_{q^2}^n$: $(c_0, c_1, \ldots, c_{n-1}) \rightarrow (c_{n-1}, c_0, \ldots, c_{n-2})$. Each codeword $\mathbf{c} =$

$(c_0, c_1, \ldots, c_{n-1})$ is customarily identified with its polynomial representation $c(x) := c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, and the code $\mathscr{C}$ is in turn identified with the set of all polynomial representations of its codewords. Then in the ring $\mathscr{R} := \mathbb{F}_{q^2}[x]/(x^n - 1)$, $xc(x)$ corresponds to a cyclic shift of $c(x)$. It is well known that a q^2-ary linear code $\mathscr{C}$ of length n is cyclic if and only if $\mathscr{C}$ is an ideal of the quotient ring $\mathscr{R}$. Moreover, $\mathscr{R}$ is a principal ideal ring, whose ideals are generated by monic factors of $x^n - 1$, i.e., $\mathscr{C} = (f(x))$ and $f(x)|(x^n - 1)$.

Suppose that $\gcd(n, q) = 1$. Let i be an integer with $0 \le i \le n - 1$. The q^2-cyclotomic coset of i modulo n is defined by $C_i := \{iq^{2l} \pmod{n} : 0 \le l \le l_i - 1\}$, where l_i is the smallest positive integer such that $iq^{2l_i} \equiv i \pmod{n}$. The smallest number in C_i is called the coset leader of C_i.

Let $\mathscr{C}$ be a q^2-ary cyclic code of length n with generator polynomial $g(x)$, then the set $D = \{0 \leqslant i \leqslant n - 1 : g(\alpha^i) = 0\}$ is called the defining set of $\mathscr{C}$, where α is a primitive n-th root of unity in some extension field of $\mathbb{F}_{q^2}$. Obviously, the defining set D is a union of some q^2-cyclotomic cosets and $\dim(\mathscr{C}) = n - |D|$, where $|D|$ denotes the cardinality of the set D. The minimum distance of $\mathscr{C}$ has the following well-known bound.

Theorem 2 (BCH bound) [30] *Let δ be an integer in the range $2 \leqslant \delta \leqslant n$. Assume that C is a cyclic code of length n with defining set D. If D consists of $\delta - 1$ consecutive elements, then $d(\mathscr{C}) \ge \delta$.*

As we said before, scholars had proposed several methods to construct EAQMDS codes. Among these methods, the most frequently used one is to decompose the defining set of the codes based on [2,26] et al. Similar to this method, we have the following result.

Theorem 3 *Let $\mathscr{C}$ be a q^2-ary cyclic code of length n with defining set D. Suppose $\mathscr{D} = D \cap (-qD)$, where $-qD = \{-qz \pmod{n} : z \in D\}$. If $\mathscr{C}$ has parameters $[n, n - |D|, d]_{q^2}$, then there exists an EAQEC code with parameters $[[n, n - 2|D| + |\mathscr{D}|, d; |\mathscr{D}|]]_q$.*

3 Constructions of entanglement-assisted quantum MDS codes

In this section, we will construct some new EAQMDS codes with lengths that divide $q^2 + 1$. We first give a useful lemma in the following which will play an important role in our construction.

Lemma 1 [14] *Let $n \mid (q^2+1)$ and $s = \lfloor \frac{n}{2} \rfloor$. If n is odd, then the q^2-cyclotomic cosets modulo n containing integers from 0 to n are: $C_0 = \{0\}$, $C_i = \{i, -i\} = \{i, n - i\}$, where $1 \leqslant i \leqslant s$. If n is even, then the q^2-cyclotomic cosets modulo n containing integers from 0 to n are: $C_0 = \{0\}$, $C_s = \{s\}$ and $C_i = \{i, -i\} = \{i, n - i\}$, where $1 \leqslant i \leqslant s - 1$.*

3.1 Entanglement-assisted quantum MDS codes of length $\frac{q^2+1}{2}$

Throughout this subsection, let q be an odd prime power, $n = \frac{q^2+1}{2}$ and $s = \frac{n-1}{2}$. From Lemma 1, the q^2-cyclotomic cosets modulo n are: $C_0 = \{0\}$ and for every i with $0 \le i \le s-1$,

$$C_{s-i} = \{s-i, s+1+i\}. \tag{1}$$

For every t with $0 \le t \le s-1$, let $\mathscr{C}_{I,t}$ be the q^2-ary cyclic code of length n with defining set

$$D_{I,t} = \bigcup_{i=0}^{t} C_{s-i}. \tag{2}$$

We have the following basic property for the defining set $D_{I,t}$.

Lemma 2 *Let $D_{I,t}$ be defined as above. If $\frac{q-1}{2} \le t \le q-2$, then $|D_{I,t} \cap (-qD_{I,t})| = 4$.*

Proof Clearly, for every q^2-cyclotomic coset C, $-qC$ is also a q^2-cyclotomic coset modulo n. Consequently, $D_{I,t} \cap (-qD_{I,t})$ is either an empty set or a union of some q^2-cyclotomic cosets. Next, by analyzing the q^2-cyclotomic coset modulo n represented by $-qC_{s-i}$, for $0 \le i \le t$, we will determine $D_{I,t} \cap (-qD_{I,t})$. Thereby, the desired result follows.

For every i with $0 \le i \le s-1$, from (1), there is a unique a_i with $0 \le a_i \le s-1$ such that $-qC_{s-i} = C_{s-a_i}$. Now, we determine a_i for $0 \le i \le t$. Since $s = \frac{n-1}{2}$ and q is odd,

$$-q(s-i) \equiv s + \frac{q+1}{2} + qi \pmod{n}, \tag{3}$$

for each i in the range $0 \le i \le s-1$. It follows from (1) and (3) that

$$a_i \equiv \frac{q-1}{2} + qi \pmod{n}, \tag{4}$$

or

$$a_i \equiv -\left(\frac{q+1}{2} + qi\right) \pmod{n}. \tag{5}$$

Notice that $\frac{q+1}{2} \le \frac{q+1}{2} + qi \le 2n - \frac{3q+1}{2}$ for $0 \le i \le q-2$, so we have the following four cases.

- Case 1: $i \in \Gamma_1 := \{i : \frac{q+1}{2} \le \frac{q+1}{2} + qi \le s\}$. From (4), $a_i = \frac{q-1}{2} + qi$. Hence,

$$-qC_{s-i} = C_{s-\frac{q-1}{2}-qi}.$$

  From (2), $(-qC_{s-i}) \cap D_{I,t} \ne \emptyset$ if and only if $0 \le \frac{q-1}{2} + qi \le t \le q-2$. Since i is an integer, there is only an $i = 0$ such that $(-qC_{s-i}) \cap D_{I,t} \ne \emptyset$ for $i \in \Gamma_1$. Hence,

$$(\cup_{i\in\Gamma_1}(-qC_{s-i})) \cap D_{I,t} = C_{s-\frac{q-1}{2}}.$$

- Case 2: $i \in \Gamma_2 := \{i : s+1 \le \frac{q+1}{2} + qi \le n\}$. We claim $\frac{q+1}{2} + qi \ne s+1$. Otherwise,
$$\frac{n-q}{2} = s+1-\frac{q+1}{2} \equiv 0 \pmod{q}.$$
It implies that $n \equiv 0 \pmod{q}$ since q is odd, which contradicts to the fact that $\gcd(n,q)=1$. It follows from (5) that
$$a_i = n - \frac{q+1}{2} - qi = q\left(\frac{q-1}{2} - i\right).$$
From (2), $(-qC_{s-i}) \cap D_{I,t} \ne \emptyset$ if and only if $0 \le a_i \le t \le q-2$. Since i is an integer, there is only an $i = \frac{q-1}{2}$ such that $(-qC_{s-i}) \cap D_{I,t} \ne \emptyset$ for $i \in \Gamma_2$. In this case, $a_i = 0$. Therefore,
$$(\cup_{i\in\Gamma_2}(-qC_{s-i})) \cap D_{I,t} = C_s.$$
- Case 3: $i \in \Gamma_3 := \{i : n+1 \le \frac{q+1}{2} + qi \le n+s\}$. It follows from (4) that
$$a_i = \frac{q+1}{2} + qi - n - 1 = q\left(i - \frac{q-1}{2}\right) - 1.$$
From (2), $(-qC_{s-i}) \cap D_{I,t} \ne \emptyset$ if and only if $0 \le a_i \le t \le q-2$. Since i is an integer, there is no $i \in \Gamma_3$ such that $0 \le a_i \le q-2$. That is to say, $\cup_{i\in\Gamma_3}(-qC_{s-i}) \cap D_{I,t} = \emptyset$.
- Case 4: $i \in \Gamma_4 := \{i : n+s+1 \le \frac{q+1}{2} + qi \le 2n - \frac{3q+1}{2}\}$. Clearly, if $\Gamma_4 \ne \emptyset$, we have $q > 3$. Now, assume that $q > 3$. We claim $\frac{q+1}{2} + qi \ne n+s+1$ for $i \in \Gamma_4$. Otherwise,
$$\frac{q^2+3}{4} = \frac{n+1}{2} = s+1 = qi + \frac{q+1}{2} - n = q(i - \frac{q-1}{2}),$$
which implies that $3 \equiv 0 \pmod{q}$ since q is odd. This contradicts to the fact that $q > 3$. It follows from (5) that
$$\frac{3q+1}{2} \le a_i = 2n - \frac{q+1}{2} - qi = q(q-i) - \frac{q-1}{2}.$$
From (2), $(-qC_{s-i}) \cap D_{I,t} \ne \emptyset$ if and only if $\frac{3q+1}{2} \le a_i \le t \le q-2$. Since i is an integer, there is no $i \in \Gamma_4$ such that $\frac{3q+1}{2} \le a_i \le q-2$. Then,
$$(\cup_{i\in\Gamma_4}(-qC_{s-i})) \cap D_{I,t} = \emptyset.$$

In conclusion, we have $D_{I,t} \cap (-qD_{I,t}) = C_s \cup C_{s-\frac{q-1}{2}}$. The result follows □

Theorem 4 *Let q be an odd prime power. For each odd integer d with $q+2 \le d \le 2q-1$, there exists an EAQMDS code with parameters $[[\frac{q^2+1}{2}, \frac{q^2+1}{2} - 2d + 6, d; 4]]_q$.*

Table 1 New entanglement-assisted quantum MDS codes of length $\frac{q^2+1}{2}$

q	Parameters $[[n,k,d;c]]_q$	d
7	$[[25, 31-2d, d; 4]]_7$	$9 \leqslant d \leqslant 13$ is odd
9	$[[41, 27-2d, d; 4]]_9$	$11 \leqslant d \leqslant 17$ is odd
11	$[[61, 67-2d, d; 4]]_{11}$	$13 \leqslant d \leqslant 21$ is odd
13	$[[85, 91-2d, d; 4]]_{13}$	$15 \leqslant d \leqslant 25$ is odd
17	$[[145, 151-2d, d; 4]]_{17}$	$19 \leqslant d \leqslant 33$ is odd
19	$[[181, 187-2d, d; 4]]_{19}$	$21 \leqslant d \leqslant 37$ is odd
23	$[[265, 271-2d, d; 4]]_{23}$	$25 \leqslant d \leqslant 45$ is odd
25	$[[313, 319-2d, d; 4]]_{25}$	$27 \leqslant d \leqslant 49$ is odd

Table 2 Entanglement-assisted quantum MDS codes of length $\frac{q^2+1}{2}$

q	Parameters $[[n,k,d;c]]_q$	d	References
Odd	$[[\frac{q^2+1}{2}, \frac{q^2+1}{2}-2d+3, d; 1]]_q$	$2 \leqslant d \leqslant q+1$ is even	[5]
Odd	$[[\frac{q^2+1}{2}, \frac{q^2+1}{2}-2d+7, d; 5]]_q$	$q+5 \leqslant d \leqslant 2q$ is even	[2]
Odd	$[[\frac{q^2+1}{2}, \frac{q^2+1}{2}-2d+6, d; 4]]_q$	$q+2 \leqslant d \leqslant 2q-1$ is odd	New

Proof For each odd integer d with $q+2 \leq d \leq 2q-1$, let $t = \frac{d-3}{2}$, then $\frac{q-1}{2} \leq t \leq q-2$. Consider the q^2-ary cyclic code $\mathscr{C}_{I,t}$ of length $n = \frac{q^2+1}{2}$ with defining set $D_{I,t}$. It follows from (1) and (2) that $|D_{I,t}| = 2t+2 = d-1$. Hence, $\dim(\mathscr{C}_{I,t}) = n - |D_{I,t}| = n-d+1$. By the definition of $D_{I,t}$ (see (2)), the defining set $D_{I,t}$ consists of $d-1$ consecutive integers

$$\left\{s - \frac{d-3}{2}, s - \frac{d-5}{2}, \cdots, s-1, s, s+1, \cdots, s + \frac{d-3}{2}, s + \frac{d-1}{2}\right\}.$$

Then by Theorem 2, the minimum distance of $\mathscr{C}_{I,t}$ is at least d. Thus, $\mathscr{C}_{I,t}$ is a cyclic code with parameters $[n, n-d+1, \geqslant d]_{q^2}$. From Lemma 2, $|D_{I,t} \cap (-qD_{I,t})| = 4$. Combining Theorem 3 with EA quantum Singleton bound, there is an EAQMDS code with parameters

$$[[n, n-2d+6, d; 4]]_q.$$

The result follows. □

Example 1 We list some new EAQMDS codes of length $\frac{q^2+1}{2}$ obtained from Theorem 4 in Table 1.

Remark 1 EAQMDS codes of length $\frac{q^2+1}{2}$ with $c = 1$ and $c = 5$ had been constructed in [2] and [5] using cyclic codes and negacyclic codes, respectively. We list them in Table 2.

3.2 Entanglement-assisted quantum MDS codes of length $\frac{q^2+1}{5}$

Throughout this subsection, let q be an odd prime power with $q \equiv \pm 3 \pmod{10}$ and $q > 3$. Let $n = \frac{q^2+1}{5}$, then n is even. From Lemma 1, the q^2-cyclotomic cosets modulo n are: $C_0 = \{0\}$, $C_{\frac{n}{2}} = \{\frac{n}{2}\}$, and for $1 \leq i \leq \frac{n}{2} - 1$,

$$C_i = \{i, n-i\}. \tag{6}$$

For each t with $0 \leq t \leq \frac{n}{2} - 1$, let $\mathscr{C}_{II,t}$ be the q^2-ary cyclic code of length n with defining set

$$D_{II,t} = \bigcup_{i=0}^{t} C_i. \tag{7}$$

We have the following basic property for the defining set $D_{II,t}$.

Lemma 3 *Let $D_{II,t}$ be defined as above. If $0 \leq t \leq \lfloor \frac{3q-4}{5} \rfloor$, then*

$$|D_{II,t} \cap (-qD_{II,t})| = \begin{cases} 1 & \text{if } 0 \leq t \leq \lfloor \frac{2q-4}{5} \rfloor, \\ 5 & \text{if } \lfloor \frac{2q+1}{5} \rfloor \leq t \leq \lfloor \frac{3q-4}{5} \rfloor. \end{cases}$$

Proof Let $t_0 = \lfloor \frac{3q-4}{5} \rfloor$. We now prove

$$D_{II,t_0} \cap (-qD_{II,t_0}) = C_0 \cup C_{\lceil \frac{q-2}{5} \rceil} \cup C_{\lfloor \frac{2q+1}{5} \rfloor}$$

and $-qC_{\lceil \frac{q-2}{5} \rceil} = C_{\lfloor \frac{2q+1}{5} \rfloor}$. The main idea is to analyze the q^2-cyclotomic coset modulo n represented by $-qC_i$ for $0 \leq i \leq t_0$. Clearly, $-qC_0 = C_0$. For every i in the range $1 \leq i \leq t_0$,

$$-q(n-i) \equiv qi \pmod{n}. \tag{8}$$

Let a_i be an integer with $1 \leq a_i \leq \frac{n}{2}$ such that $-qC_i = C_{a_i}$. From (6) and (8), we have

$$a_i \equiv qi \pmod{n}, \tag{9}$$

or

$$a_i \equiv -qi \pmod{n}. \tag{10}$$

Notice that $0 < qi \leq qt_0 < 3n$ for $1 \leq i \leq t_0$, we now analyze a_i in the following six cases.

- Case 1: $i \in \Gamma_1 := \{i : 1 \leq qi \leq \frac{n}{2}\}$. From (9), $a_i = qi$, i.e., $-qC_i = C_{qi}$. From (7), $(-qC_i) \cap D_{II,t_0} \neq \emptyset$ if and only if $1 \leq qi \leq t_0$. Since i is an integer and $t_0 < q$, then
$$(\cup_{i \in \Gamma_1}(-qC_i)) \cap D_{II,t_0} = \emptyset.$$
- Case 2: $i \in \Gamma_2 := \{i : \frac{n}{2} + 1 \leq qi \leq n\}$. Since $\gcd(n, q) = 1$, $qi \neq n$. It follows from (10) that $a_i = n - qi$, i.e., $-qC_i = C_{n-qi}$. From (7), $(-qC_i) \cap D_{II,t_0} \neq \emptyset$

if and only if $1 \le n - qi \le t_0$. Since i is an integer, $1 \le n - qi \le t_0$ is equivalent to

$$\left\lceil \frac{q-2}{5} \right\rceil = \left\lceil \frac{n-t_0}{q} \right\rceil \le i \le \left\lfloor \frac{n-1}{q} \right\rfloor = \left\lfloor \frac{q-2}{5} \right\rfloor.$$

Hence, if $q \equiv -3 \pmod{10}$, there is only an $i = \frac{q-2}{5}$ such that $(-qC_i) \cap D_{II,t_0} \neq \emptyset$ for $i \in \Gamma_2$. In this case, $a_i = n - qi = \frac{2q+1}{5}$, and

$$(\cup_{i \in \Gamma_2}(-qC_i)) \cap D_{II,t_0} = C_{\frac{2q+1}{5}}.$$

If $q \equiv 3 \pmod{10}$, $(\cup_{i \in \Gamma_2}(-qC_i)) \cap D_{II,t_0} = \emptyset$.

- Case 3: $i \in \Gamma_3 := \{i : n+1 \le qi \le \frac{3n}{2}\}$. From (9), $a_i = qi - n$, i.e., $-qC_i = C_{qi-n}$. It follows from (7) that $(-qC_i) \cap D_{II,t_0} \neq \emptyset$ if and only if $1 \le qi - n \le t_0$. Note that i is an integer, $1 \le qi - n \le t_0$ is equivalent to

$$\left\lceil \frac{q+2}{5} \right\rceil = \left\lceil \frac{n+1}{q} \right\rceil \le i \le \left\lfloor \frac{n+t_0}{q} \right\rfloor = \left\lfloor \frac{q+2}{5} \right\rfloor.$$

Hence, if $q \equiv 3 \pmod{10}$, there is only an $i = \frac{q+2}{5}$ such that $(-qC_i) \cap D_{II,t_0} \neq \emptyset$ for $i \in \Gamma_3$. In this case, $a_i = qi - n = \frac{2q-1}{5}$, and

$$(\cup_{i \in \Gamma_3}(-qC_i)) \cap D_{II,t_0} = C_{\frac{2q-1}{5}}.$$

If $q \equiv -3 \pmod{10}$, we have $(\cup_{i \in \Gamma_3}(-qC_i)) \cap D_{II,t_0} = \emptyset$.

- Case 4: $i \in \Gamma_4 := \{i : \frac{3n}{2} + 1 \le qi \le 2n\}$. Since q is an odd prime power and $\gcd(n, q) = 1$, one can get $qi \neq 2n$. Hence, $1 \le 2n - qi \le \frac{n}{2} - 1$. From (10), $a_i = 2n - qi$, i.e., $-qC_i = C_{2n-qi}$. It follows from (7) that $(-qC_i) \cap D_{II,t_0} \neq \emptyset$ if and only if $1 \le 2n - qi \le t_0$. Since i is an integer, $1 \le 2n - qi \le t_0$ is equivalent to

$$\left\lceil \frac{2q-1}{5} \right\rceil = \left\lceil \frac{2n-t_0}{q} \right\rceil \le i \le \left\lfloor \frac{2n-1}{q} \right\rfloor = \left\lfloor \frac{2q-1}{5} \right\rfloor.$$

Hence, if $q \equiv 3 \pmod{10}$, there is only an $i = \frac{2q-1}{5}$ such that $(-qC_i) \cap D_{II,t_0} \neq \emptyset$, for $i \in \Gamma_4$. In this case, $a_i = 2n - qi = \frac{q+2}{5}$, and

$$(\cup_{i \in \Gamma_4}(-qC_i)) \cap D_{II,t_0} = C_{\frac{q+2}{5}}.$$

If $q \equiv -3 \pmod{10}$, we have $(\cup_{i \in \Gamma_4}(-qC_i)) \cap D_{II,t_0} = \emptyset$.

- Case 5: $i \in \Gamma_5 := \{i : 2n+1 \le qi \le \frac{5n}{2}\}$. Similar to Case 4, one can get $qi \neq \frac{5n}{2}$. It implies that $1 \le qi - 2n \le \frac{n}{2} - 1$. From (9), $a_i = qi - 2n$, i.e., $-qC_i = C_{qi-2n}$. From (7), $(-qC_i) \cap D_{II,t_0} \neq \emptyset$ if and only if $1 \le qi - 2n \le t_0$. Since i is an integer, $1 \le qi - 2n \le t_0$ is equivalent to

$$\left\lceil \frac{2q+1}{5} \right\rceil = \left\lceil \frac{2n+1}{q} \right\rceil \le i \le \left\lfloor \frac{2n+t_0}{q} \right\rfloor = \left\lfloor \frac{2q+1}{5} \right\rfloor.$$

Therefore, if $q \equiv -3 \pmod{10}$, there is only an $i = \frac{2q+1}{5}$ such that $(-qC_i) \cap D_{II,t_0} \neq \emptyset$, for $i \in \Gamma_5$. In this case, $a_i = qi - 2n = \frac{q-2}{5}$, and

$$(\cup_{i\in\Gamma_5}(-qC_i)) \cap D_{II,t_0} = C_{\frac{q-2}{5}}.$$

If $q \equiv 3 \pmod{10}$, we have $(\cup_{i\in\Gamma_5}(-qC_i)) \cap D_{II,t_0} = \emptyset$.

- Case 6: $i \in \Gamma_6 := \{i : \frac{5n}{2} + 1 \leq qi \leq qt_0\}$. Obviously, $1 < 3n - qt_0 \leq 3n - qi \leq \frac{n}{2} - 1$. From (10), $a_i = 3n - qi$, i.e., $-qC_i = C_{3n-qi}$. From (7), $(-qC_i) \cap D_{II,t_0} \neq \emptyset$ if and only if $3n - qt_0 \leq 3n - qi \leq t_0$. Since i is an integer, $3n - qt_0 \leq 3n - qi \leq t_0$ is equivalent to

$$\left\lceil \frac{3q-1}{5} \right\rceil = \left\lceil \frac{3n-t_0}{q} \right\rceil \leq i \leq t_0 = \left\lfloor \frac{3q-4}{5} \right\rfloor$$

Therefore, $(\cup_{i\in\Gamma_6}(-qC_i)) \cap D_{II,t_0} = \emptyset$.

In conclusion, we have $D_{II,t_0} \cap (-qD_{II,t_0}) = C_0 \cup C_{\lceil\frac{q-2}{5}\rceil} \cup C_{\lfloor\frac{2q+1}{5}\rfloor}$. The result follows. □

Theorem 5 *Let q be an odd prime power with $q \equiv \pm 3 \pmod{10}$ and $q > 3$. For each even integer d with $2 \leq d \leq 2\lfloor\frac{2q+1}{5}\rfloor$, there exists an EAQMDS code with parameters*

$$\left[\left[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 3, d; 1\right]\right]_q.$$

For each even integer d with $2\lfloor\frac{2q+6}{5}\rfloor \leq d \leq 2\lfloor\frac{3q+1}{5}\rfloor$, there exists an EAQMDS code with parameters

$$\left[\left[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 7, d; 5\right]\right]_q.$$

Proof For each even integer d with $2 \leq d \leq 2\lfloor\frac{3q+1}{5}\rfloor$, let $t = \frac{d-2}{2}$, then $0 \leq t \leq \lfloor\frac{3q-4}{5}\rfloor$. Now consider the q^2-ary cyclic code $\mathscr{C}_{II,t}$ of length $n = \frac{q^2+1}{5}$ with defining set $D_{II,t}$. From (7), $|D_{I,t}| = 2t+1 = d-1$. Hence, $\dim(\mathscr{C}_{II,t}) = n - |D_{II,t}| = n-d+1$. According to the definition of $D_{II,t}$, it consists of $d-1$ consecutive integers

$$\left\{-\frac{d-2}{2}, \cdots, -1, 0, 1, \cdots, \frac{d-2}{2}\right\}.$$

Then by Theorem 2, $d(\mathscr{C}_{II,t}) \geqslant d$. Therefore, $\mathscr{C}_{II,t}$ is a cyclic code with parameters $[n, n-d+1, \geqslant d]_{q^2}$. From Lemma 3,

$$|D_{II,t} \cap (-qD_{II,t})| = \begin{cases} 1 & \text{if } 0 \leq t \leq \lfloor\frac{2q-4}{5}\rfloor, \\ 5 & \text{if } \lfloor\frac{2q+1}{5}\rfloor \leq t \leq \lfloor\frac{3q-4}{5}\rfloor. \end{cases}$$

Table 3 New entanglement-assisted quantum MDS codes of length $\frac{q^2+1}{5}$

q	Parameters $[[n, k, d; c]]_q$	d
13	$[[34, 37-2d, d; 1]]_{13}$	$2 \leqslant d \leqslant 10$ is even
	$[[34, 41-2d, d; 5]]_{13}$	$12 \leqslant d \leqslant 16$ is even
17	$[[58, 61-2d, d; 1]]_{17}$	$2 \leqslant d \leqslant 14$ is even
	$[[58, 65-2d, d; 5]]_{17}$	$16 \leqslant d \leqslant 20$ is even
37	$[[274, 277-2d, d; 1]]_{37}$	$2 \leqslant d \leqslant 30$ is even
	$[[274, 281-2d, d; 5]]_{37}$	$32 \leqslant d \leqslant 44$ is even
53	$[[562, 565-2d, d; 1]]_{53}$	$2 \leqslant d \leqslant 42$ is even
	$[[562, 569-2d, d; 5]]_{53}$	$44 \leqslant d \leqslant 64$ is even
57	$[[650, 653-2d, d; 1]]_{57}$	$2 \leqslant d \leqslant 46$ is even
	$[[650, 657-2d, d; 5]]_{57}$	$48 \leqslant d \leqslant 68$ is even

Combining Theorem 3 with the EA quantum Singleton bound, there is an EAQMDS code with parameters

$$\left[\left[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 3, d; 1\right]\right]_q,$$

for even d with $2 \leq d \leq 2\lfloor\frac{2q+1}{5}\rfloor$; and

$$\left[\left[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 7, d; 5\right]\right]_q,$$

for even d with $2\lfloor\frac{2q+6}{5}\rfloor \leq d \leq 2\lfloor\frac{3q+1}{5}\rfloor$. The result follows. □

Example 2 We list some new EAQMDS codes of length $\frac{q^2+1}{5}$ obtained from Theorem 5 in Table 3.

Remark 2 EAQMDS codes of length $\frac{q^2+1}{5}$ with $c = 1$ and $c = 5$ had been constructed in [26] from negacyclic codes, where $q = 10m + 3$, $q = 10m + 7$ and m is an even integer. However, in this paper, we construct EAQMDS codes of length $\frac{q^2+1}{5}$ with $c = 1$ and $c = 5$ under the case $q = 10m + 3$, $q = 10m + 7$ and m is any positive integer. Hence, our results are more general. It is easy to see that our results coincide with theirs under the case m is even. But when m is odd, our results are new. EAQMDS codes of such length with other cases also had been studied (see Table 4).

3.3 Entanglement-assisted quantum MDS codes of length $\frac{q^2+1}{10}$

Throughout this subsection, let q be an odd prime power with $q \equiv \pm 3 \pmod{10}$ and $q > 3$. Let $n = \frac{q^2+1}{10}$ and $s = \frac{n-1}{2}$. From Lemma 1, the q^2-cyclotomic cosets modulo n are: $C_0 = \{0\}$,

$$C_{s-i} = \{s - i, s + 1 + i\}, \tag{11}$$

Table 4 Entanglement-assisted quantum MDS codes of length $\frac{q^2+1}{5}$

q	Parameters $[[n,k,d;c]]_q$	d	References
$10m+2$	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+6,d;4]]_q$	$\frac{3q+9}{5}\leqslant d\leqslant q+1$ is odd	[3,13]
$10m+8$	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+6,d;4]]_q$	$\frac{3q+11}{5}\leqslant d\leqslant q+1$ is odd	[3,13]
$20m+3$	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+6,d;4]]_q$	$12m+4\leqslant d\leqslant 20m+4$ is even	[3]
$20m+7$	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+6,d;4]]_q$	$12m+6\leqslant d\leqslant 20m+8$ is even	[3]
$10m+3$	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+6,d;4]]_q$	$4m+3\leqslant d\leqslant 6m+1$ is odd	[26]
m odd		$6m+4\leqslant d\leqslant 10m+4$ is even	
m even	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+3,d;1]]_q$	$2\leqslant d\leqslant 8m+2$ is even	
	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+6,d;4]]_q$	$4m+3\leqslant d\leqslant 6m+1$ is odd	
	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+7,d;5]]_q$	$8m+4\leqslant d\leqslant 12m+4$ is even	
$10m+7$	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+6,d;4]]_q$	$8m+7\leqslant d\leqslant 14m+11$ is odd	[26]
m odd		$6m+6\leqslant d\leqslant 10m+8$ is even	
m even	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+3,d;1]]_q$	$2\leqslant d\leqslant 8m+6$ is even	
	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+6,d;4]]_q$	$8m+7\leqslant d\leqslant 14m+11$ is odd	
	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+7,d;5]]_q$	$8m+8\leqslant d\leqslant 12m+8$ is even	
$10m+3$	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+3,d;1]]_q$	$2\leqslant d\leqslant 8m+2$ is even	New
m odd	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+7,d;5]]_q$	$8m+4\leqslant d\leqslant 12m+4$ is even	
$10m+7$	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+3,d;1]]_q$	$2\leqslant d\leqslant 8m+6$ is even	New
m odd	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+7,d;5]]_q$	$8m+8\leqslant d\leqslant 12m+8$ is even	

for $1\le i\le s-1$. For every t with $0\le t\le s-1$, let $\mathscr{C}_{III,t}$ be the q^2-ary cyclic code of length n with defining set

$$D_{III,t}=\bigcup_{i=0}^{t} C_{s-i}. \tag{12}$$

We have the following basic property for the defining set $D_{III,t}$.

Lemma 4 *Let $D_{III,t}$ be defined as above. If $\lceil\frac{q-3}{5}\rceil\le t\le\lfloor\frac{2q-6}{5}\rfloor$, then*

$$|D_{III,t}\cap(-qD_{III,t})|=4.$$

Proof Let $t_0=\lfloor\frac{2q-6}{5}\rfloor$. It is clear that we only have to prove that

$$D_{III,t_0}\cap(-qD_{III,t_0})=C_{s-\lfloor\frac{q-3}{10}\rfloor}\cup C_{s-\lceil\frac{q-3}{5}\rceil}.$$

The main idea is similar to Lemma 3, that is, to analyze the q^2-cyclotomic coset modulo n represented by $-qC_{s-i}$ for $0\le i\le t_0$. From (11), there is a unique integer

a_i with $0 \le a_i \le s-1$ such that $-qC_{s-i} = C_{s-a_i}$. For every i with $0 \le i \le t_0$, it is easy to check that

$$-q(s-i) \equiv s + \frac{q+1}{2} + qi \pmod{n}. \tag{13}$$

From (11), we have

$$a_i \equiv \frac{q-1}{2} + qi \pmod{n}, \tag{14}$$

or

$$a_i \equiv -(\frac{q+1}{2} + qi) \pmod{n}. \tag{15}$$

Note that $\frac{q+1}{2} \le \frac{q+1}{2} + qi \le \frac{q+1}{2} + qt_0 < 4n$, for $0 \le i \le t_0$. We now analyze $D_{III,t_0} \cap (-qD_{III,t_0})$ in the following eight cases.

- Case 1: $i \in \Gamma_1 := \{i : \frac{q+1}{2} \le \frac{q+1}{2} + qi \le s\}$. From (14), $a_i = \frac{q-1}{2} + qi$, i.e., $-qC_{s-i} = C_{s-\frac{q-1}{2}-qi}$. From (12), $(-qC_{s-i}) \cap D_{III,t_0} \neq \emptyset$ if and only if $0 \le \frac{q-1}{2} + qi \le t_0$. Since i is an integer and $0 < t_0 < \frac{q-1}{2}$, we have $(\cup_{i\in\Gamma_1}(-qC_{s-i})) \cap D_{III,t_0} = \emptyset$.
- Case 2: $i \in \Gamma_2 := \{i : s+1 \le \frac{q+1}{2} + qi \le n\}$. Similar to Case 2 in the proof of Lemma 2, $\frac{q+1}{2} + qi \neq s+1$. From (15), $a_i = n - \frac{q+1}{2} - qi$. Thereby, from (12), $(-qC_{s-i}) \cap D_{III,t_0} \neq \emptyset$ if and only if $0 \le a_i \le t_0$. Since i is an integer, $0 \le a_i \le t_0$ is equivalent to

$$\left\lceil \frac{q-7}{10} \right\rceil = \left\lceil \frac{2n-q-1-2t_0}{2q} \right\rceil \le i \le \left\lfloor \frac{q^2-5q-4}{10q} \right\rfloor = \left\lfloor \frac{q-7}{10} \right\rfloor.$$

  Therefore, if $q \equiv -3 \pmod{10}$, there is only an $i = \frac{q-7}{10}$ such that $0 \le a_i \le t_0$ for $i \in \Gamma_2$. In this case, $a_i = n - \frac{q+1}{2} - qi = \frac{q-2}{5}$. Hence,

$$(\cup_{i\in\Gamma_2}(-qC_{s-i})) \cap D_{III,t_0} = C_{s-\frac{q-2}{5}}.$$

  If $q \equiv 3 \pmod{10}$, there is no $i \in \Gamma_2$ such that $0 \le a_i \le t_0$. Hence,

$$\cup_{i\in\Gamma_2}(-qC_{s-i}) \cap D_{III,t_0} = \emptyset.$$

- Case 3: $i \in \Gamma_3 := \{i : n+1 \le \frac{q+1}{2} + qi \le n+s\}$. From (14), $a_i = \frac{q-1}{2} + qi - n$. It follows from (12) that $(-qC_{s-i}) \cap D_{III,t_0} \neq \emptyset$ if and only if $0 \le a_i \le t_0$. Since i is an integer, $0 \le a_i \le t_0$ is equivalent to

$$\left\lceil \frac{q-3}{10} \right\rceil = \left\lceil \frac{2n-q+1}{2q} \right\rceil \le i \le \left\lfloor \frac{2n-q+1+2t_0}{2q} \right\rfloor = \left\lfloor \frac{q-3}{10} \right\rfloor.$$

  Hence, if $q \equiv 3 \pmod{10}$, there is only an $i = \frac{q-3}{10}$ such that $(-qC_{s-i}) \cap D_{III,t_0} \neq \emptyset$ for $i \in \Gamma_3$. Therefore,

$$(\cup_{i\in\Gamma_3}(-qC_{s-i})) \cap D_{III,t_0} = C_{s-\frac{q-3}{5}}.$$

If $q \equiv -3 \pmod{10}$, $\cup_{i\in\Gamma_3}(-qC_{s-i}) \cap D_{III,t_0} = \emptyset$.

- Case 4: $i \in \Gamma_4 := \{i : n+s+1 \le \frac{q+1}{2} + qi \le 2n\}$. Similar to Case 4 in the proof of Lemma 2, we have $\frac{q+1}{2} + qi \ne n+s+1$. It follows from (15) that $a_i = 2n - \frac{q+1}{2} - qi$. From (12), $(-qC_{s-i}) \cap D_{III,t_0} \ne \emptyset$ if and only if $0 \le a_i \le t_0$. Since i is an integer, $0 \le a_i \le t_0$ is equivalent to $\lceil \frac{q-3}{5} \rceil \le i \le \lfloor \frac{q-3}{5} \rfloor$. Hence, if $q \equiv 3 \pmod{10}$, there is only an $i = \frac{q-3}{5}$ such that $(-qC_{s-i}) \cap D_{III,t_0} \ne \emptyset$ for $i \in \Gamma_4$, i.e.,
$$(\cup_{i\in\Gamma_4}(-qC_{s-i})) \cap D_{III,t_0} = C_{s-\frac{q-3}{10}}.$$
Otherwise, if $q \equiv -3 \pmod{10}$, we have $\cup_{i\in\Gamma_4}(-qC_{s-i}) \cap D_{III,t_0} = \emptyset$.
- Case 5: $i \in \Gamma_5 := \{i : 2n+1 \le \frac{q+1}{2} + qi \le 2n+s\}$. From (14), $a_i = \frac{q-1}{2} + qi - 2n$. From (12), $(-qC_{s-i}) \cap D_{III,t_0} \ne \emptyset$ if and only if $0 \le a_i \le t_0$. Since i is an integer, $0 \le a_i \le t_0$ is equivalent to $\lceil \frac{q-2}{5} \rceil \le i \le \lfloor \frac{q-2}{5} \rfloor$. Hence, if $q \equiv -3 \pmod{10}$, there is only an $i = \frac{q-2}{5}$ such that $(-qC_{s-i}) \cap D_{III,t_0} \ne \emptyset$ for $i \in \Gamma_5$. Thereby,
$$(\cup_{i\in\Gamma_5}(-qC_{s-i})) \cap D_{III,t_0} = C_{s-\frac{q-7}{10}}.$$
Otherwise, if $q \equiv 3 \pmod{10}$, we have $\cup_{i\in\Gamma_5}(-qC_{s-i}) \cap D_{III,t_0} = \emptyset$.
- Case 6: $i \in \Gamma_6 := \{i : 2n+s+1 \le \frac{q+1}{2} + qi \le 3n\}$. We claim $\frac{q+1}{2} + qi \ne 2n+s+1$. Otherwise, $q+1+2qi = 5n+1$. It implies that $5n \equiv 0 \pmod{q}$, which contradicts to the fact that $\gcd(5n, q) = 1$. From (15), $a_i = 3n - \frac{q+1}{2} - qi$. It follows from (12) that $(-qC_{s-i}) \cap D_{III,t_0} \ne \emptyset$ if and only if $0 \le a_i \le t_0$. Since i is an integer, $0 \le a_i \le t_0$ is equivalent to $\lceil \frac{3q-1}{10} \rceil \le i \le \lfloor \frac{3q-9}{10} \rfloor$. Therefore,
$$(\cup_{i\in\Gamma_6}(-qC_{s-i})) \cap D_{III,t_0} = \emptyset.$$
- Case 7: $i \in \Gamma_7 := \{i : 3n+1 \le \frac{q+1}{2} + qi \le 3n+s\}$. From (14), $a_i = \frac{q-1}{2} + qi - 3n$. It follows from (12) that $(-qC_{s-i}) \cap D_{III,t_0} \ne \emptyset$ if and only if $0 \le a_i \le t_0$. Since i is an integer, $0 \le a_i \le t_0$ is equivalent to $\lceil \frac{3q-1}{10} \rceil \le i \le \lfloor \frac{3q-9}{10} \rfloor$. Hence,
$$(\cup_{i\in\Gamma_7}(-qC_{s-i})) \cap D_{III,t} = \emptyset.$$
- Case 8: $i \in \Gamma_8 := \{i : 3n+s+1 \le \frac{q+1}{2} + qi \le \frac{q+1}{2} + qt_0\}$. We claim $\frac{q+1}{2} + qi \ne 3n+s+1$. Otherwise, $q+1+2qi = 7n+1$. It implies that $7n \equiv 0 \pmod{q}$. Note that $\gcd(n, q) = 1$, we have $q = 7$. However, if $q = 7$, we have $\Gamma_8 = \emptyset$. It follows from (15) that $a_i = 4n - \frac{q+1}{2} - qi$. From (12), $(-qC_{s-i}) \cap D_{III,t_0} \ne \emptyset$ if and only if $0 \le a_i \le t_0$, that is, $\lceil \frac{2q-4}{5} \rceil \le i \le \lfloor \frac{2q-4}{5} \rfloor$. Notice that $i \le \lfloor \frac{2q-6}{5} \rfloor$, we have $(\cup_{i\in\Gamma_8}(-qC_{s-i})) \cap D_{III,t_0} = \emptyset$.

According to all the cases above, we have $D_{III,t_0} \cap (-qD_{III,t_0}) = C_{s-\lfloor \frac{q-3}{10} \rfloor} \cup C_{s-\lceil \frac{q-3}{5} \rceil}$. The result follows. □

Table 5 New entanglement-assisted quantum MDS codes of length $\frac{q^2+1}{10}$

q	Parameters $[[n, k, d; c]]_q$	d
13	$[[17, 23-2d, d; 4]]_{13}$	$7 \leqslant d \leqslant 11$ is odd
17	$[[29, 35-2d, d; 4]]_{17}$	$9 \leqslant d \leqslant 13$ is odd
23	$[[53, 59-2d, d; 4]]_{23}$	$11 \leqslant d \leqslant 19$ is odd
27	$[[73, 79-2d, d; 4]]_{27}$	$13 \leqslant d \leqslant 21$ is odd
37	$[[137, 143-2d, d; 4]]_{37}$	$17 \leqslant d \leqslant 29$ is odd
43	$[[185, 191-2d, d; 4]]_{43}$	$19 \leqslant d \leqslant 35$ is odd
47	$[[221, 227-2d, d; 4]]_{47}$	$21 \leqslant d \leqslant 37$ is odd

Theorem 6 *Let q be an odd prime power with $q \equiv \pm 3 \pmod{10}$ and $q > 3$. For each odd integer d with $2\lceil \frac{q+2}{5} \rceil + 1 \le d \le 2\lfloor \frac{2q-1}{5} \rfloor + 1$, there is an EAQMDS code with parameters*

$$\left[\left[\frac{q^2+1}{10}, \frac{q^2+1}{10} - 2d + 6, d; 4\right]\right]_q.$$

Proof For each odd integer d with $2\lceil \frac{q+2}{5} \rceil + 1 \le d \le 2\lfloor \frac{2q-1}{5} \rfloor + 1$, let $t = \frac{d-3}{2}$, then $\lceil \frac{q-3}{5} \rceil \le t \le \lfloor \frac{2q-6}{5} \rfloor$. Consider the q^2-ary cyclic code $\mathscr{C}_{III,t}$ of length $n = \frac{q^2+1}{10}$ with defining set $D_{III,t}$. From (12), $|D_{III,t}| = 2(t+1) = d-1$. Hence, $\dim(\mathscr{C}_{III,t}) = n - |D_{III,t}| = n - d + 1$. Clearly, the defining set $D_{III,t}$ consists of $d-1$ consecutive integers $\{s - \frac{d-3}{2}, \cdots, s-1, s, s+1, \cdots, s + \frac{d-1}{2}\}$. Then by Theorem 2, $d(\mathscr{C}_{III,t}) \geqslant d$. Therefore, $\mathscr{C}_{III,t}$ is a cyclic code with parameters $[n, n-d+1, \geqslant d]_{q^2}$. From Lemma 4, $c = |D_{III,t} \cap (-qD_{III,t})| = 4$. Combining Theorem 3 with the EA quantum Singleton bound, $\mathscr{C}_{III,t}$ is an EAQMDS code with parameters

$$\left[\left[\frac{q^2+1}{10}, \frac{q^2+1}{10} - 2d + 6, d; 4\right]\right]_q.$$

The result follows. □

Example 3 We list some new EAQMDS codes of length $\frac{q^2+1}{10}$ obtained from Theorem 6 in Table 5.

Remark 3 EAQMDS codes of length $\frac{q^2+1}{10}$ with $c = 1$ had been constructed in [2] from negacyclic codes. EAQMDS codes of the same length with $c = 5$ and $c = 9$ had been constructed in [13] utilizing constacyclic codes with order $q+1$. We list all the known results of EAQMDS codes of length $\frac{q^2+1}{10}$ in Table 6.

4 Conclusion

In this paper, EAQMDS codes of three different lengths, i.e., $\frac{q^2+1}{2}$, $\frac{q^2+1}{5}$, $\frac{q^2+1}{10}$, have been constructed by exploiting less pre-shared maximally entangled states. Comparing

Table 6 Entanglement-assisted quantum MDS codes of length $\frac{q^2+1}{10}$

q	Parameters $[[n, k, d; c]]_q$	d	References
$10m+3$	$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - 2d + 3, d; 1]]_q$	$2 \leqslant d \leqslant \frac{q+7}{5}$ is even	[5]
$10m+7$	$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - 2d + 3, d; 1]]_q$	$2 \leqslant d \leqslant \frac{q+3}{5}$ is even	[5]
$10m+3$	$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - 2d + 3, d; 1]]_q$	$2 \leqslant d \leqslant 6m+2$ is even	[27]
$10m+7$	$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - 2d + 3, d; 1]]_q$	$2 \leqslant d \leqslant 6m+4$ is even	[27]
$10m+3$	$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - 2d + 7, d; 5]]_q$	$\frac{3q+11}{5} \leqslant d \leqslant \frac{4q-2}{5}$ is even	[13]
$10m+7$	$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - 2d + 7, d; 5]]_q$	$\frac{3q+9}{5} \leqslant d \leqslant \frac{4q+2}{5}$ is even	[13]
$10m+3$	$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - 2d + 11, d; 9]]_q$	$\frac{4q+8}{5} \leqslant d \leqslant q-1$ is even	[13]
$10m+7$	$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - 2d + 11, d; 9]]_q$	$\frac{4q+22}{5} \leqslant d \leqslant q+3$ is even	[13]
$10m+3$	$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - 2d + 6, d; 4]]_q$	$\frac{2q+9}{5} \leqslant d \leqslant \frac{4q+3}{5}$ is odd	New
$10m+7$	$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - 2d + 6, d; 4]]_q$	$\frac{2q+11}{5} \leqslant d \leqslant \frac{4q-3}{5}$ is odd	New

the parameters of the obtained EAQMDS codes with all known EAQMDS codes of such lengths, one can find that these EAQMDS codes are new in the sense that their parameters are not covered by the codes available in the literature, except the length $\frac{q^2+1}{5}$, where $q = 10m + 3$ and $q = 10m + 7$ with m even, which is the same as the results in [27].

Acknowledgements We are grateful to the anonymous referees and the associate editor Travis S Humble for useful comments and suggestions that improved the presentation and quality of this paper. The work was supported by the National Natural Science Foundation of China (61802102, 61772168, 61972126), the Natural Science Foundation of Anhui Province (1708085QA01, 1808085MA15), the China Scholarship Council (201806695004) and the Fundamental Research Funds for the Central Universities of China (PA2019GDZC0097).

References

1. Brun, T.A., Devetak, I., Hsieh, M.H.: Correcting quantum errors with entanglement. Science **314**(5798), 436–439 (2006)
2. Chen, J., Huang, Y., Feng, C., Chen, R.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. Quantum Inf. Process. **16**, 303 (2017)
3. Chen, X., Zhu, S., Kai, X.: Entangle-assisted quantum MDS codes constructed from constacyclic codes. Quantum Inf. Process. **17**, 273 (2018)
4. Chen, X., Zhu, S., Kai, X.: Entanglement-assisted quantum negacyclic BCH codes. Int. J. Theor. Phys. **58**(5), 1509–1523 (2019)
5. Fan, J., Chen, H., Xu, J.: Constructions of q-ary entanglement-assisted quantum MDS codes with minimum distance greater than $q + 1$. Quantum Inf. Comput. **16**(5, 6), 0423–0434 (2016)
6. Galindo, C., Hernando, F., Matsumoto, R., Ruano, D.: Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. Quantum Inf. Process. **18**, 116 (2019)
7. Grassl, M.: Entanglement-Assisted Quantum Communication Beating the Quantum Singleton Bound. AQIS, Taiwan (2016)
8. Guenda, K., Jitman, S., Gulliver, T.A.: Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr. **86**(1), 121–136 (2018)

9. Guenda, K., Gulliver, T.A., Jitman, S., Thipworawimon, S.: Linear l-intersection pairs of codes and their applications. (arXiv Preprint: 1810.05103v1) (2018)
10. Guo, L., Li, R.: Linear plotkin bound for entanglement-assisted quantum codes. Phys. Rev. A **87**, 032309 (2013)
11. Hsieh, M.H., Brun, T.A., Devetak, I.: Entanglement-assisted quantum quasi-cyclic low-density parity-check codes. Phys. Rev. A **79**, 032340 (2009)
12. Hsich, M.H., Devetak, I., Brun, T.A.: General entanglement-assisted quantum error-correcting codes. Phys. Rev. A **76**, 064302 (2007)
13. Koroglu, M.E.: New entanglement-assisted MDS quantum codes from constacyclic codes. Quantum Inf. Process. **18**, 44 (2019)
14. La Guardia, G.G.: New quantum MDS codes. IEEE Trans. Inf. Theory **57**(8), 5551–5554 (2011)
15. Lai, C.Y., Ashikhmin, A.: Linear programming bounds for entanglement-assisted quantum error-correcting codes by split weight enumerators. IEEE Trans. Inf. Theory **64**(1), 622–639 (2018)
16. Lai, C.Y., Brun, T.A.: Entanglement-assisted quantum error-correcting codes with imperfect ebits. Phys. Rev. A **86**, 032319 (2012)
17. Lai, C.Y., Brun, T.A.: Entanglement increases the error-correcting ability of quantum error-correcting codes. Phys. Rev. A **88**, 012320 (2013)
18. Li, L., Zhu, S., Liu, L., Kai, X.: Entanglement-assisted quantum MDS codes from generalized Reed–Solomon codes. Quantum Inf. Process. **18**, 153 (2019)
19. Li, R., Guo, G., Song, H., Liu, Y.: New constructions of entanglement-assisted quantum MDS codes from negacyclic codes. Int. J. Quantum Inf. (2019). https://doi.org/10.1142/S0219749919500229
20. Li, R., Zuo, F., Liu, Y.: A study of skew asymmetric q^2-cyclotomic coset and its application. J. Air Force Eng. Univ. (Nat. Sci. Ed.) **12**(1), 87–89 (2011). **(in Chinese)**
21. Liu, X., Liu, H., Yu, L.: Entanglement-assisted quantum codes from matrix-product codes. Quantum Inf. Process. **18**, 183 (2019)
22. Liu, X., Yu, L., Hu, P.: New entanglement-assisted quantum codes from k-Galois dual codes. Finite Fields Appl. **55**, 21–32 (2019)
23. Liu, Y., Li, R., Lv, L., Ma, Y.: Applications of constacyclic codes to entanglement-assited quantum maximum distance separable codes. Quantum Inf. Process. **17**, 210 (2018)
24. Lu, L., Li, R.: Entanglement-assisted quantum codes constructed from primitive quaternary BCH codes. Int. J. Quantum Inf. **12**(3), 1450015 (2014)
25. Lu, L., Li, R., Guo, L., Fu, Q.: Maximal entanglement entanglement-assisted quantum codes constructed from linear codes. Quantum Inf. Process. **14**, 165–182 (2015)
26. Lu, L., Li, R., Guo, L., Ma, Y., Liu, Y.: Entanglement-assisted quantum MDS codes from negacyclic codes. Quantum Inf. Process. **17**, 69 (2018)
27. Lu, L., Ma, W., Li, R., Ma, Y., Liu, Y., Cao, H.: Entanglement-assisted quantum MDS codes from constacyclic codes with large minimum distance. Finite Fields Appl. **53**, 309–325 (2018)
28. Luo, G., Cao, X.: Two new families of entanglement-assisted quantum MDS codes from generalized Reed-Solomon codes. Quantum Inf. Process. **18**, 89 (2019)
29. Luo, G., Cao, X., Chen, X.: MDS codes with hulls of arbitrary dimensions and their quantum error correction. IEEE Trans. Inf. Theory **65**(5), 2944–2952 (2019)
30. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error Correcting Codes. North-Holland, Amsterdam (1977)
31. Qian, J., Zhang, L.: Entanglement-assisted quantum codes from arbitrary binary linear codes. Des. Codes Cryptogr. **77**(1), 193–202 (2015)
32. Qian, J., Zhang, L.: On MDS linear complementary dual codes and entanglement-assisted quantum codes. Des. Codes Cryptogr. **86**(7), 1565–1572 (2018)
33. Qian, J., Zhang, L.: Constructions of new entangle-assisted quantum MDS and almost MDS codes. Quantum Inf. Process. **18**, 71 (2019)
34. Sari, M., Kolotoğlu, E.: An application of constacyclic codes to entanglement-assisted quantum MDS codes. Comput. Appl. Math. **8**, 75 (2019)
35. Shin, J., Heo, J., Brun, T.A.: Entanglement-assisted codeword stabilized quantum codes. Phys. Rev. A **84**, 062321 (2011)

36. Wilde, M.M., Brun, T.A.: Optimal entanglement formulas for entanglement-assisted quantum coding. Phys. Rev. A **77**, 064302 (2008)