Quantum Information Processing (2020) 19:289
https://doi.org/10.1007/s11128-020-02771-w

New classes of entanglement-assisted quantum MDS codes

Renjie Jin[1] · Derong Xie[1] · Jinquan Luo[1]

Received: 29 October 2019 / Accepted: 17 July 2020 / Published online: 24 August 2020

Abstract
In this paper, two new classes of entanglement-assisted quantum MDS codes (EAQMDS codes for short) with length n being a factor of $q^2 \pm 1$ are presented via cyclic codes over finite fields of odd characteristic. Among our constructions, there are several EAQMDS codes with new parameters which have never been reported. Moreover, some of them have much larger minimum distance than known results.

Keywords MDS code · EAQEC code · EAQMDS code · Cyclic code

1 Introduction

Quantum information can protect messages between sender and receiver avoiding decoherence by encoding it into quantum error-correcting codes. Entanglement-assisted quantum error-correcting codes (EAQEC codes for short) are crucial to quantum information theory (see [1–4,12]). Recently, construction of good quantum codes via classical codes is a hot topic for quantum information and quantum computing (see [16,17,20,22,24]). EAQEC codes use preexisting entanglement between the sender and the receiver to improve information rate. Many researchers have been devoted to obtaining EAQEC codes via classical liner codes, such as negacyclic codes and generalized Reed–Solomon codes. It has been shown that EAQEC codes have some advantages over standard stabilizer codes. For example, only a dual-containing classical linear quaternary code can be transformed into a standard stabilizer code, but

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

Renjie Jin
jinrenjie@mails.ccnu.edu.cn

Derong Xie
derongxie@yahoo.com

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

any classical linear quaternary code can be transformed into an EAQEC code. Some of them can be summarized as follows.

In [13,23], some new EAQEC codes with good parameters via cyclic and constacyclic codes are constructed. In [5], new decomposition of negacyclic codes are proposed, by which four new classes of EAQEC codes have been constructed. In [7], Fan et al. constructed some classes of EAQMDS codes based on classical maximum distance separable (MDS for short) codes by exploiting one or more pre-shared maximally entangled states. In [22], Qian and Zhang constructed some new classes of MDS linear complementary dual (LCD) codes with respect to Hermitian inner product. As applications, they have constructed new families of EAQMDS codes. In [9], Guenda et al. showed that the number of shared pairs required to construct an EAQEC code is related to the hull of classical codes. Using this fact, they put forward new methods to construct EAQEC codes requiring desirable amounts of entanglements. The $EA\text{-}Singleton\ bound$ for an $[[n, k, d; c]]_q$ EAQEC code is

$$2(d-1) \leq n-k+c.$$

A q-ary EAQEC code attaining this bound is said to be an EAQMDS code. In this paper, we will construct EAQMDS codes via cyclic codes by improving the method introduced in [23].

Our main contribution is the construction of EAQMDS codes with parameters

(1) $\Big[\Big[n, n-4qm+4m^2+3, 2m(q-1); (2m-1)^2\Big]\Big]_q$ where $1 \leq m \leq \lfloor \frac{q+1}{4t} \rfloor$, $n = \frac{q^2-1}{t}$ and $t \mid q^2-1$. (Theorem 3.1)

(2) $\Big[\Big[n, n-4mq+4q+4m^2-8m+3, 2(m-1)q+2; 4(m-1)^2+1\Big]Big]_q$ where $2 \leq m \leq \lfloor \frac{q+1}{4t} \rfloor$, $n = \frac{q^2+1}{t}$ and $t \mid q^2+1$. (Theorem 3.2)

We will present some known results of EAQMDS codes, which are depicted in Table 1.

This paper is organized as follows: In Sect. 2, we will introduce some basic acknowledge and useful results on cyclic codes and EAQEC codes. In Sect. 3, we will present our main results on the constructions of new EAQMDS codes. In Sect. 4, we will make a conclusion.

2 Preliminaries

2.1 Cyclic code

In this section, we introduce some basic notations and useful results on linear codes and cyclic codes. Let $\mathbb{F}_q$ be the $finite\ field$ of cardinality q, where q is an odd prime power. An $[n, k, d]_q$ code is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ with dimension k and minimum distance d. The $Singleton\ bound$ states that

$$d \leq n-k+1.$$

Table 1 Some known constructions on EAQMDS codes with parameters $[[n, k, d; c]]_q$ (q is an odd prime power)

Parameters	Constraints	References
$[[q^2+1, q^2-4(m-1)(q-m-1),$ $2(m-1)q+2; 4(m-1)^2+1]]_q$	$q \geq 5$ and $2 \leq m \leq \frac{q-1}{2}$	[23]
$[[q^2+1, q^2-2q-4m+5, 2m+q+1; 4]]_q$	$q \geq 5, q = 4t+1$ where t is an integer and $2 \leq m \leq \frac{q-1}{2}$	[5]
$[[\frac{q^2+1}{2}, \frac{q^2+1}{2}-2q-4m+5, 2m+q+1; 5]]_q$	$q > 7$ and $2 \leq m \leq \frac{q-1}{2}$	[5]
$[[\frac{q^2-1}{5}, \frac{q^2-5q-20m+4}{5}, \frac{4m+q+5}{2}; 4]]_q$	$q = 20t+3$ or $q = 20t+7$ and $t \leq m \leq \frac{q-3}{4}$	[6]]
$[[\frac{q^2+1}{10}, \frac{q^2+1}{10}-2d+3, d; 1]]_q$	$q = 10m+3$ and d is even, $2 \leq d \leq 6m+2$	[18]
$[[\frac{q^2+1}{10}, \frac{q^2+1}{10}-2d+3, d; 1]]_q$	$q = 10m+7$ and d is even, $2 \leq d \leq 6m+4$	[18]
$[[\frac{q^2-1}{h}, \frac{q^2-1}{h}-2d+3, d; 1]]_q$	$h \in \{3, 5, 7\}$ is a factor of $q+1$ and d is even, $\frac{q+1}{h} \leq d \leq \frac{(q+1)(h+3)}{2h}-1$	[18]
$[[\frac{q^2-1}{t}, \frac{q^2-1}{t}-4qm+4m^2+3,$ $2m(q-1); (2m-1)^2]]_q$	$q \geq 3, t \mid q^2-1, 1 \leq m \leq \lfloor\frac{q+1}{4t}\rfloor$	Theorem 3.1
$[[\frac{q^2+1}{t}, \frac{q^2+1}{t}-4qm+4q+4m^2-8m+3,$ $2q(m-1)+2; 4(m-1)^2+1]]_q$	$q \geq 7, t \mid q^2+1, 2 \leq m \leq \lfloor\frac{q+1}{4t}\rfloor$	Theorem 3.2

The code attaining the Singleton bound is called *MDS* code. When $d = n - k$, the code is called *almost MDS*. Let $\mathbf{u} = (u_0, \ldots, u_{n-1})$ and $\mathbf{v} = (v_0, \ldots, v_{n-1})$ be two vectors in $\mathbb{F}_{q^2}^n$. The *Hermitian inner product* is defined by

$$\langle \mathbf{u}, \mathbf{v} \rangle_H = u_0 v_0^q + u_1 v_1^q + \cdots + u_{n-1} v_{n-1}^q.$$

The *Hermitian dual* of an $\mathbb{F}_{q^2}$-linear code $\mathcal{C}$ of length n is defined as

$$\mathcal{C}^{\perp_H} = \{\mathbf{u} \in F_{q^2}^n \mid \langle \mathbf{u}, \mathbf{v} \rangle_H = 0 \quad \text{for all} \quad \mathbf{v} \in \mathcal{C}\}.$$

The code $\mathcal{C}$ is *Hermitian self-orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^{\perp_H}$, and is *Hermitian self-dual* if $\mathcal{C} = \mathcal{C}^{\perp_H}$.

For $\gcd(n, q) = 1$, the *q^2-cyclotomic coset* of i modulo n is defined by

$$C_i = \{iq^{2j} (\text{mod } n) \mid j \in \mathbb{Z}\}.$$

A linear code $\mathcal{C}$ over $\mathbb{F}_{q^2}$ is a *cyclic code* if for every codeword $(c_1, c_2, \ldots, c_n) \in \mathcal{C}$, its cyclic shift $(c_n, c_1, \ldots, c_{n-1})$ is also a codeword in $\mathcal{C}$. The cyclic code $\mathcal{C}$ can be generated by a polynomial $g(x)$, where $g(x) \mid x^n - 1$. The *defining set* of $\mathcal{C}$ is given by $T = \{0 \leq i \leq n-1 \mid g(\alpha^i) = 0\}$, where α is an n-th root of unity in some extension field of $\mathbb{F}_{q^2}$. It is easy to see that the defining set T is a union of some q^2-cyclotomic cosets. Then, the following property is given in [10,19].

Proposition 2.1 (BCH bound) *Let δ be a positive integer with $2 \leq \delta \leq n$. Assume that $\mathcal{C}$ is a cyclic code of length n with defining set T. If T contains $\delta - 1$ consecutive elements $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$, then minimum distance of $\mathcal{C}$ is at least δ.*

2.2 EAQEC code

In this section, we introduce some notations and useful results on EAQEC codes. For more details, see [7,8,11,14,21].

A q-ary $[[n, k, d; c]]_q$ *EAQEC* code $\mathcal{C}$ has length n and can encode k logical qubits with minimum distance d. Here, c is the copies of maximally entangled Bell states. The code $\mathcal{C}$ can correct up to at least $[\frac{d-1}{2}]$ quantum errors.

Recently, researchers proved that EAQEC code can be constructed from any classical linear code over $\mathbb{F}_q$. The remaining problem is to calculate c. In [15], a new approach to determine c is proposed by Li et al.

Proposition 2.2 ([15]) *Let $\mathcal{C}$ be an $[n, k, d]_{q^2}$ cyclic code with defining set T. Assume the decomposition of T is $T = T_{ss} \bigcup T_{as}$, where $T_{ss} = -qT \bigcap T$ and $T_{as} = T \backslash T_{ss}$.*

(1) *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be cyclic codes with defining set T_{ss} and T_{as}, respectively. Then, $\mathcal{C}_1^{\perp_H} \bigcap \mathcal{C}_1 = \{0\}$ and $\mathcal{C}_2^{\perp_H} \subseteq \mathcal{C}_2$.*
(2) *There exists an $[[n, n - 2|T| + |T_{ss}|, d; |T_{ss}|]]_q$ EAQEC code.*

3 New EAQMDS codes

3.1 Length $n \mid q^2 - 1$

In this subsection, we apply cyclic codes of length $n \mid q^2 - 1$ to construct a new family of EAQMDS codes with length $n \mid q^2 - 1$, where $q \geq 3$ is an odd prime power. Firstly, the q^2-ary cyclotomic coset modulo n are singletons: $C_i = \{i \pmod{n}\}$. The following two lemmas will be used in our constructions.

Lemma 3.1 *Let q be an odd prime power, $t \mid q^2 - 1$ and $n = \frac{q^2-1}{t}$. Then,*

$$-qC_{aq+b} = C_{-bq-a}$$

where $-\lfloor \frac{q-1}{2t} \rfloor \leq a, b \leq \lfloor \frac{q-1}{2t} \rfloor$, with $(a, b) \neq (-\lfloor \frac{q-1}{2t} \rfloor, -\lfloor \frac{q-1}{2t} \rfloor)$.

Proof Note that $|aq + b| \leq \lfloor \frac{q^2-1}{2t} \rfloor$ and $aq + b \neq -\lfloor \frac{q^2-1}{2t} \rfloor$. Hence, all of $aq + b$ are distinct. A straightforward calculation shows

$$\begin{aligned} -q(aq + b) &= -aq^2 - bq \\ &= -a(q^2 - 1) - a - bq \\ &\equiv -bq - a \pmod{n}, \end{aligned}$$

which implies $-qC_{aq+b} = C_{-bq-a}$. □

Lemma 3.2 *Let m be a positive integer with $1 \leq m \leq \lfloor \frac{q+1}{4t} \rfloor$ and $n \mid q^2 - 1$ where q is an odd prime power. Decompose*

$$T_0 = \bigcup_{-m \leq i \leq m-1, i \neq 0} A_i$$

where

$$A_i = \begin{cases} \{-mq + j \mid m + 1 \leq j \leq q - m\}, & i = -m; \\ \{iq + j \mid m \leq j \leq q - m\}, & -m + 1 \leq i \leq m - 2,\ i \neq 0; \\ \{mq + j \mid -q + m \leq j \leq -m - 1\}, & i = m - 1. \end{cases}.$$

Then, $-qT_0 \bigcap T_0 = \emptyset$.

Proof To show $-qT_0 \bigcap T_0 = \emptyset$, it suffices to prove the following cases.

- **Case 1:** $-qA_i \bigcap A_{i'} = \emptyset$. On the contrary, suppose there exist j, j' such that

$$\begin{aligned} -q(iq + j) &= -iq^2 - jq \pmod{n} \\ &= -jq - i \pmod{n}. \end{aligned}$$

It is easy to verify that

$$i^{'} = -j \quad \text{and} \quad j^{'} = -i.$$

It follows that $-(q-m) \leq i^{'} \leq -m$ and $-(m-2) \leq j^{'} \leq m-1$. Since $-m+1 \leq i \leq m-2$ and $m \leq j \leq q-m$, which leads to a contradiction. Hence, $-qA_i \bigcap A_{i^{'}} = \emptyset$.

- **Case 2:** $-qA_i \bigcap A_{-m} = \emptyset$ and $-qA_i \bigcap A_m = \emptyset$. On the contrary, suppose $-qA_i \bigcap A_{-m} \neq \emptyset$, then there exist $j, j^{'}$ such that

$$\begin{aligned} -q(iq+j) &= -jq - i \pmod{n} \\ &= -mq + j^{'} \pmod{n}. \end{aligned}$$

where $m \leq j \leq q-m$ and $-q+m \leq j^{'} \leq -m-1$. As a consequence, $-(m-2) \leq -i \leq m-1$ which is a contradiction.
Assume $-qA_i \bigcap A_m \neq \emptyset$, then there exist $j, j^{''}$ such that

$$\begin{aligned} -q(iq+j) &= -jq - i \pmod{n} \\ &= mq + j^{''} \pmod{n} \end{aligned}$$

where $m \leq j \leq q-m$ and $m+1 \leq j^{''} \leq q-m$. As a consequence, $-(q-m) \leq -j \leq -m$. It is easy to verify $-qA_i \bigcap A_m = \emptyset$.

- **Case 3:** $-qA_{-m} \bigcap A_m = \emptyset$ and $-qA_m \bigcap A_{-m} = \emptyset$.
On the contrary, suppose $-qA_{-m} \bigcap A_m \neq \emptyset$, then there exist $j, l^{'}$ such that

$$\begin{aligned} -q(-mq+j) &= m(q^2-1) - jq + m \pmod{n} \\ &= -jq + m \pmod{n} \\ &= mq + l^{'} \pmod{n} \end{aligned}$$

where $m+1 \leq j \leq q-m$ and $-(q-m) \leq l^{'} \leq -(m+1)$, which is a contradiction. Hence, $-qA_{-m} \bigcap A_m = \emptyset$. Assume $-qA_m \bigcap A_{-m} \leq \emptyset$, then there exist $j, l^{''}$ such that

$$\begin{aligned} -q(mq+j) &= -m(q^2-1) - jq - m \pmod{n} \\ &= -jq - m \pmod{n} \\ &= -mq + l^{''} \pmod{n} \end{aligned}$$

where $-(q-m) \leq j \leq -(m+1)$ and $m+1 \leq l^{''} \leq q-m$ which is a contradiction. Hence, $-qA_{-m} \bigcap A_m = \emptyset$.

- The remaining cases $-qA_{-m} \bigcap A_{-m} = \emptyset$ and $-qA_m \bigcap A_m = \emptyset$ can be proved in a similar way, and we omit the details.

Hence, we have $-qT_0 \bigcap T_0 = \emptyset$, which completes the proof. □

Now we will construct new EAQMDS codes with length $n \mid q^2 - 1$.

Theorem 3.1 *Let q be an odd prime power, $t \mid q^2 - 1$ and $n = \frac{q^2-1}{t}$. For any $1 \leq m \leq \lfloor \frac{q+1}{4t} \rfloor$, there exists EAQMDS code with parameters*

$$[[n, n - 4qm + 4m^2 + 3, 2m(q-1); (2m-1)^2]]_q.$$

Proof For $1 \leq m \leq \lfloor \frac{q+1}{4t} \rfloor$, assume that $\mathcal{C}$ is a cyclic code of length $n \mid q^2 - 1$ with defining set

$$T = \bigcup_{i=-mq+m+1}^{mq-m-1} C_i$$

It is easy to check that $\mathcal{C}$ has $2qm - 2m - 1$ consecutive roots. Then, by Proposition 2.1, the minimum distance of $\mathcal{C}$ is at least $2qm - 2m$. It follows that $\mathcal{C}$ is a cyclic code with parameters $[n,\ n - 2qm + 2m + 1,\ 2qm - 2m]_{q^2}$. In the following, we show that $c = |T_{ss}| = (2m-1)^2$. Denote by

$$T_0 = \bigcup_{i=-m, i\neq 0}^{m-1} A_i.$$

According to Lemma 3.2, $-qT_0 \bigcap T_0 = \emptyset$. By Lemma 3.1,

$$\begin{gathered}
-qC_1 = C_{-q},\ -qC_{q+1} = C_{-q-1}, \ldots, -qC_{(m-1)q-1} = C_{q-(m-1)}, \\
-qC_2 = C_{-2q},\ -qC_{q+2} = C_{-2q-1}, \ldots, -qC_{(m-1)q-2} = C_{2q-(m-1)}, \\
\vdots \\
-qC_{m-1} = C_{-(m-1)q},\ -qC_{q+(m-1)} \\
= C_{-(m-1)q-1}, \ldots, -qC_{(m-1)q-(m-1)} = C_{(m-1)q-(m-1)}.
\end{gathered}$$

Obviously, $-qC_0 = C_0$ and it suffices to prove

$$T_{ss} = -qT \bigcap T = \bigcup_{-(m-1) \leq a,b \leq m-1} C_{aq+b}.$$

For $C_{aq+b} \subseteq T_{ss}$, there exist $a^{'}, b^{'}$ such that $-qC_{aq+b} = C_{a^{'}q+b^{'}}$. The equality

$$-q(aq+b) \equiv a^{'}q + b^{'} \pmod{n}$$

Table 2 Some new parameters of EAQMDS codes

Parameters	t	m
$[[280, 171, 56; 1]]_{29}$	3	1
$[[280, 67, 112; 9]]_{29}$	3	2
$[[560, 403, 80; 1]]_{41}$	3	1
$[[560, 251, 160; 9]]_{41}$	3	2
$[[368, 187, 92; 1]]_{47}$	6	1
$[[368, 9, 184; 9]]_{47}$	6	2

implies

$$a^{'} = -b, b^{'} = -a.$$

Then, by Lemma 3.1, $-qT_{ss} = T_{ss}$ and by Lemma 3.2 $-qT_0 \bigcap T_0 = \emptyset$. By the standard counting arguments, $|T_{ss}| = (2m-1)^2$.

By Proposition 2.2, the EAQEC code with defining set T has parameters

$$[[n, n - 4qm + 4m^2 + 3, 2m(q-1); (2m-1)^2]]_q.$$

Also this code reaches the EA-$Singleton$ bound,

$$n - k + c + 2 = 4qm - 4m = 2d.$$

Hence, the EAQMDS code with desired parameters is constructed. □

Example 3.1 We list some new parameters of EAQMDS codes of Theorems 3.1 in Table 2.

3.2 Length $n|q^2+1$

In this subsection, we try to construct some new EAQMDS codes with length $n \mid q^2+1$. Here we assume n is even. Denote by $t = \frac{q^2+1}{n}$(it is an integer). The q^2-ary cyclotomic coset modulo n are

$$C_0 = \{0\},\ C_1 = \{1,\ n-1\},\ C_2 = \{2,\ n-2\}, \ldots, C_{\frac{n}{2}} = \left\{\frac{n}{2}\right\}.$$

The following two lemmas are similar to Lemmas 3.1 and 3.2.

Lemma 3.3 *Let* $n = \frac{q^2+1}{t}$. *Then,*

$$-qC_{cq+d} = C_{dq-c},$$

where $1 \le c \le \lfloor \frac{q-1}{2t} \rfloor$ *and* $0 \le d \le \lfloor \frac{q-1}{2t} \rfloor$.

Proof Note that $C_{cq+d} = \{cq + d, \ -(cq + d)\}$ with $cq + d \leq \lfloor \frac{q^2-1}{2t} \rfloor$ for $1 \leq c \leq \lfloor \frac{q-1}{2t} \rfloor$ and $0 \leq d \leq \lfloor \frac{q-1}{2t} \rfloor$. A straightforward calculation shows

$$\begin{aligned} -q \cdot (-(cq + d)) &= cq^2 + dq \\ &= c(q^2 + 1) - c + dq \\ &\equiv dq - c \pmod{n} \end{aligned}$$

which implies $-qC_{cq+d} = C_{dq-c}$. □

Lemma 3.4 *Let* $n = \frac{q^2+1}{t}$*, notations as in Lemma 3.3. For* $2 \leq m \leq \lfloor \frac{q+1}{4t} \rfloor$*, let*

$$T_1 = \bigcup_{0 \leq c \leq m-2, \ m \leq d \leq \lfloor \frac{q-1}{2t} \rfloor} C_{cq+d} \bigcup_{1 \leq e \leq m-1 \leq f \leq \lfloor \frac{q-1}{2t} \rfloor} C_{eq-f}.$$

Then, $-qT_1 \bigcap T_1 = \emptyset$.

Proof By Lemma 3.3,

$$-qT_1 = \bigcup_{0 \leq c \leq m-2, \ m \leq d \leq \lfloor \frac{q-1}{2t} \rfloor} C_{dq-c} \bigcup_{1 \leq e \leq m-1 \leq f \leq \lfloor \frac{q-1}{2t} \rfloor} C_{fq+e}.$$

When $m \leq d \leq \lfloor \frac{q-1}{2t} \rfloor$ and $0 \leq c \leq m - 2$,

$$cq + d \leq (m - 2)q + \lfloor \frac{q - 1}{2t} \rfloor \quad \text{and} \quad mq - m + 2 \leq dq - c.$$

Similarly,

$$eq - f \leq (m - 1)q + 1 - m \quad \text{and} \quad (m - 1)q + 1 \leq fq + e.$$

It is easy to verify

$$cq + d \leq dq - c, \ cq + d \leq fq + e, \ eq - f \leq dq - c, \ eq - f \leq fq + e.$$

Therefore, $-qT_1 \bigcap T_1 = \emptyset$. □

Theorem 3.2 *Let* $n = \frac{q^2+1}{t}$*. For any* $2 \leq m \leq \lfloor \frac{q+1}{4t} \rfloor$*, there exists an EAQMDS code with parameters*

$$\left[\left[n, n - 4mq + 4q + 4m^2 - 8m + 3, 2(m - 1)q + 2; 4(m - 1)^2 + 1\right]\right]_q$$

Table 3 Some new parameters of EAQMDS codes

Parameters	t	m
$[[370, 201, 88; 5]]_{43}$	5	2
$[[466, 113, 180; 9]]_{89}$	17	2
$[[898, 633, 136; 5]]_{67}$	5	2
$[[898, 377, 270; 17]]_{67}$	5	3

Proof For $2 \le m \le \lfloor\frac{q+1}{4t}\rfloor$, suppose $\mathcal{C}$ is a cyclic code with length $n = \frac{q^2+1}{t}$ and defining set $T = C_0 \bigcup C_1 \bigcup C_2 \bigcup \cdots \bigcup C_{(m-1)q}$. It is easy to see that $\mathcal{C}$ has $2(m-1)q+1$ consecutive roots. Then, by Proposition 2.1, the minimum distance of $\mathcal{C}$ is at least $2(m-1)q+2$. It follows that $\mathcal{C}$ is a cyclic code with parameters $[n,\ n-2(m-1)q-1,\ 2(m-1)q+1]_{q^2}$. In the following, we show that $|T_{ss}| = 4(m-1)^2+1$. Let

$$T_1 = \bigcup_{0\le c\le m-2,\ m\le d\le\lfloor\frac{q-1}{2t}\rfloor} C_{cq+d} \bigcup_{1\le e\le m-1\le f\le\lfloor\frac{q-1}{2t}\rfloor} C_{eq-f}.$$

According to Lemma 3.3,

$$\begin{gathered}
-qC_1 = C_q,\ -qC_{q+1} = C_{q-1}, \ldots, -qC_{(m-2)q+1} = C_{q-(m-2)},\\
-qC_2 = C_{2q},\ -qC_{q+2} = C_{2q-1}, \ldots, -qC_{(m-2)q+2} = C_{2q-(m-2)},\\
\vdots\\
-qC_{m-1} = C_{(m-1)q},\ -qC_{q+(m-1)} = C_{(m-1)q-1} \ldots,\ -qC_{(m-2)q+(m-1)} = C_{(m-1)q-(m-2)}.
\end{gathered}$$

Obviously, $-qC_0 = C_0$. It is easy to verify that $T_{ss} = T\backslash T_1$. Then, $-qT_{ss} = T_{ss}$ and $-qT_1 \bigcap T_1 = \emptyset$. It is easy to see $|T_{ss}| = 4(m-1)^2+1$. By Proposition 2.2, the EAQEC code with defining set T has parameters

$$\left[\left[n, n-4mq+4q+4m^2-8m+3, 2(m-1)q+2; 4(m-1)^2+1\right]\right]_q$$

Also this code reaches the EA-$Singleton$ bound,

$$n-k+c+2 = 4(m-1)q+4 = 2d.$$

Hence, the code $\mathcal{C}$ is an EAQMDS code. □

Example 3.2 We list some new parameters of EAQMDS codes of Theorems 3.2 in Table 3.

Remark 3.1 From Examples 3.1 and 3.2, we can conclude that the required parameters of the EAQMDS codes constructed in Theorems 3.1 and 3.2 are more flexible than all codes listed in Table 1, since our results covers almost all possible factors of $q^2 \pm 1$. What's more, the parameter c in our codes is unfixed. Compared to [23], we introduced a more general method (see Lemma 3.2) to find T_{as} and T_{ss}; then, we solved the case length $n \mid q^2 - 1$. Since the four parameters in our codes are flexible, it is easier to obtain a large number of EAQMDS codes from our constructions than those listed in Table 1. In [25], the authors constructed EAQMDS codes with length $n = \frac{q-1}{a}(q+1)$. Since the length of their codes satisfies $n \mid q - 1$, our length can be a factor of $q + 1$. Then, we can construct some EAQMDS codes with new parameters that have never been reported. Besides, employing the EAQMDS codes obtained by Theorems 3.1 and 3.2, we can obtain EAQMDS codes with length different from $q + 1$ and the required parameters can take all or almost all possible values. Some of them are listed in Table 2.

4 Conclusion

In this paper, we construct two new classes of EAQMDS codes with length $n|q^2 - 1$ and $n|q^2 + 1$ via classical cyclic codes. Our codes have more flexible parameters than known EAQEC codes. It may be possible to apply our methods to construct new EAQMDS codes via classical linear codes, such as generalized Reed–Solomon codes or constacyclic codes.

Funding Funding was provided by National Science Fundation of China (Grant No. 11471008) and Self-determined research funds of CCNU from the colleges' basic research and operation of MOE (Grant No. CCNU18TS028).

References

1. Ashikhmin, A., Litsyn, S., Tsfasman, M.: Asymptotically good quantum codes. Phys. Rev. A **63**, 032311 (2001)
2. Calderbank, A.R., Shor, P.W.: Good quantum error-correcting codes exist. Phys. Rev. A **54**, 1098 (1996)
3. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over GF(4). IEEE Trans. Inf. Theory **44**, 1369–1387 (1998)
4. Chen, H.: Some good quantum error-correcting codes from algebraic-geometric codes. IEEE Trans. Inf. Theory **47**, 2059–2061 (2001)
5. Chen, J., Huang, Y., Feng, C., Chen, R.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. Quantum Inf. Process. **16**, 303 (2017)
6. Chen, X., Zhu, S., Kai, X.: Entanglement-assisted quantum MDS codes constructed from constacyclic codes. Quantum Inf. Process. **17**, 273 (2018)
7. 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**, 0423–0434 (2016)
8. Fujiwara, Y., Clark, D., Vandendriessche, P., Boeck, M.D., Tonchev, V.D.: Entanglement-assisted quantum low-density parity-check codes. Phys. Rev. A **82**, 042338 (2010)
9. Guenda, K., Jitman, S., Gulliver, T.A.: Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr. **86**, 121–136 (2018)
10. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
11. Hsieh, M.H., Yen, W.T., Hsu, L.Y.: High performance entanglement-assisted quantum LDPC codes need little entanglement. IEEE Trans. Inf. Theory **57**, 1761–1769 (2011)
12. Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K.: Nonbinary stabilizer codes over finite fields. IEEE Trans. Inf. Theory **52**, 4892–4914 (2006)

13. Koroglu, M.E.: New entanglement-assisted MDS quantum codes from constacyclic codes. Quantum Inf. Process. **18**, 44 (2019)
14. Lai, C.Y., Brun, T.A., Wilde, M.M.: Duality in entanglement-assisted quantum error correction. IEEE Trans. Inf. Theory **59**, 4020–4024 (2013)
15. Li, R., Xu, G., Lu, L.: Decomposition of defining sets of BCH codes and its applications. J. Air Force Eng. Univ. (Nat. Sci. Ed.) **14**(2), 86–89 (2013). (in Chinese)
16. Li, X.: Quantum cyclic and constacyclic codes. IEEE Trans. Inf. Theory **50**, 547–549 (2004)
17. Lu, L., Li, R., Guo, L., Ma, Y., Liu, Y.: Entanglement-assisted quantum MDS codes from negacyclic codes. Quantum Inf. Process. **17**, 69 (2018)
18. Lu, L., Li, R., Ma, W., Li, R., Ma, Y., Liu, Y., Cao, H.: Entanglement-assisted quantum MDS codes from constacyclic codes with large minimum distance. arXiv:1803.04168
19. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error Correcting Codes. North-Holland, Amsterdam (1977)
20. Qian, J., Zhang, L.: Nonbinary quantum codes derived from group character codes. Int. J. Quantum Inf. Process. **10**, 1250042 (2012)
21. Qian, J., Zhang, L.: New optimal subsystem codes. Discrete Math. **313**, 2451–2455 (2013)
22. Qian, J., Zhang, L.: On MDS linear complementary dual codes and entanglement-assisted quantum codes. Des. Codes Cryptogr. **86**, 1565–1572 (2017)
23. Qian, J., Zhang, L.: Constructions of new entanglement-assisted quantum MDS and almost MDS codes. Quantum Inf. Process. **18**, 71 (2019)
24. Steane, A.M.: Simple quantum error-correcting codes. Phys. Rev. A **54**, 4741 (1996)
25. Wang, J., Li, R., Lv, J., Song, H.: Entanglement-assisted quantum codes from cyclic codes and negacyclic codes. Quantum Inf. Process. **19**, 5 (2020)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.