International Journal of Theoretical Physics (2023) 62:100
https://doi.org/10.1007/s10773-023-05348-2

RESEARCH

Two Families of Entanglement-Assisted Quantum Codes Constructed from Cyclic Codes

Wei Cao[1] · **Xiaoshan Kai**[1] · **Jin Li**[1]

Received: 15 December 2022 / Accepted: 30 March 2023 / Published online: 12 May 2023

Abstract
Entanglement-assisted quantum error-correcting (EAQEC) codes are a significant extension of quantum error-correcting codes. It has been found that an EAQEC code can be constructed by an arbitrary classical linear code if the encoder and the decoder share the entangled state c in advance. In this paper, we construct two families of q-ary entanglement-assisted quantum maximum-distance-separable (EAQMDS) codes. This construction produces new EAQMDS codes with variable parameters with respect to the minimum distance d and the number c of maximally entangled states. Moreover, the resulting EAQMDS codes have minimum distance not less than q.

Keywords EAQMDS codes · Cyclic codes · Maximally entangled states · Skew symmetric cosets

1 Introduction

The class of quantum error-correcting codes provides an effective coding framework for guarding quantum information just as classical error-correcting codes guard classical information. After the discovery by Shor and Steane [29, 30], quantum error-correcting codes have undergone tremendous development. Many well-parameterized quantum error-correcting codes have been constructed by the aid of classical error-correcting codes. Among the known construction methods, the most common construction method is through using classical linear codes and satisfying certain dual-containing requirement. However, it is difficult to find the class of dual-containing codes. The dual-containing constraint has become a serious obstacle to the evolution of quantum coding theory. In 2006, Brun et al. made a great breakthrough in quantum error-correction by proposing entanglement-assisted quantum

✉ Wei Cao
cwei0925@163.com

Xiaoshan Kai
kxs6@sina.com

Jin Li
lijin_0102@126.com

[1] School of Mathematics, Hefei University of Technology, Hefei 230601, China

error-correcting (EAQEC) codes [2]. They found that classical linear binary codes, which are not self-orthogonal, can be applied to construct quantum codes if the sender and receiver share the entanglement bits beforehand. This discovery has inspired researchers to concentrate on the construction of EAQEC codes.

Let q be a prime power. An $[[n, k, d; c]]_q$ code $\mathcal{C}$ is a q-ary EAQEC code of length n, which encodes k logical qudits into n physical qudits and corrects quantum errors up to $\lfloor \frac{d-1}{2} \rfloor$ by utilizing c pairs of maximally entangled states. Here, d is the minimum distance of the code. If $c = 0$, then an EAQEC code is a standard $[[n, k, d]]_q$ quantum code. The parameters of an $[[n, k, d; c]]_q$ EAQEC code are mutually restricted and meet the following entanglement-assisted quantum Singleton bound.

Lemma 1 [2, 11, 14] *For an* $[[n, k, d; c]]_q$ *EAQEC code, if* $d \leq \frac{n+2}{2}$, *then*

$$n + c + 2 - k \geq 2d,$$

where $1 \leq c \leq n - 1$.

An $[[n, k, d; c]]_q$ EAQEC code that attains the entanglement-assisted quantum Singleton bound is called an entanglement-assisted quantum maximum-distance-separable (EAQMDS) code. Since entanglement can improve the error-correcting performance of quantum codes [15], it is more desirable that we can construct EAQMDS codes for large distance. Recently, many researchers found an amount of EAQMDS codes from constacyclic codes, generalized Reed-Solomon (GRS) codes and linear complement dual (LCD) codes, see Refs. [4, 6–10, 25]. Since cyclic codes have a good algebraic structure, they are the preferred objects for constructing EAQMDS codes. However, it is a hard problem to fix on the number of maximally entangled states. In [21], the concept of the decomposition of defining set of a cyclic BCH code was introduced to solve the problem of computing the number c and construct some good EAQEC codes. After that, more and more scholars have extended this approach to general constacyclic codes, so as to result in the construction of many new EAQMDS codes. In particular, EAQMDS codes with length dividing $q^2 + 1$ or $q^2 - 1$ were massively obtained [3, 5, 6, 17–19, 25, 28, 31, 33].

Generally, as entanglement bits are more used, it would be more difficult to find the parameters of EAQEC codes. Recently, in [7, 27, 28, 33], several families of EAQMDS codes with variable parameters were derived from constacyclic codes, GRS codes, and extended GRS codes. In these works, the formula of the relation between the minimum distance d and the number c of maximally entangled states was explicitly described and the change rules of the parameters of EAQMDS codes were revealed. Motivated by the above ideas, we construct two new families of q-ary EAQMDS codes from cyclic codes with minimum distance not less than q. Specific parameters are as follows.

- Length $n = \frac{q^2-1}{3}$ with $3 \mid (q + 1)$ and $1 \leq t \leq \lceil \frac{q-8}{6} \rceil$.

(i) $[[n, n - 2d + 3t^2 + 2, d; 3t^2]]_q$, where $tq \leq d \leq t(q - 1) + \frac{q+1}{3}$.
(ii) $[[n, n - 2d + 3t^2 + 2t + 2, d; 3t^2 + 2t]]_q$, $tq + \frac{q+1}{3} \leq d \leq t(q - 1) + \frac{2q-1}{3}$.
(iii) $[[n, n - 2d + 3t^2 + 4t + 4, d; 3t^2 + 4t + 2]]_q$, where $tq + \frac{2(q+1)}{3} \leq d \leq (t + 1)(q - 1)$.

- Length $n = \frac{q^2-1}{5}$ with $5 \mid (q + 1)$ and $1 \leq t \leq \lceil \frac{q-14}{10} \rceil$.

(i) $[[n, n - 2d + 5t^2 + 2, d; 5t^2]]_q$, where $tq \leq d \leq t(q - 1) + \frac{q+1}{5}$.
(ii) $[[n, n - 2d + 5t^2 + 2t + 2, d; 5t^2 + 2t]]_q$, where $tq + \frac{q+1}{5} \leq d \leq t(q - 1) + \frac{2q+2}{5}$.
(iii) $[[n, n - 2d + 5t^2 + 4t + 2, d; 5t^2 + 4t]]_q$, where $tq + \frac{2q+2}{5} \leq d \leq t(q - 1) + \frac{3q-2}{5}$.

(iv) $[[n, n-2d+5t^2+6t+4, d; 5t^2+6t+2]]_q$, where $tq+\frac{3q+3}{5} \leq d \leq t(q-1)+\frac{4q-1}{5}$.
(v) $[[n, n-2d+5t^2+8t+6, d; 5t^2+8t+4]]_q$, where $tq+\frac{4q+4}{5} \leq d \leq (t+1)(q-1)$.

Compared with the known constructions in Refs. [16, 18, 22, 27], our constructions produce EAQMDS codes processing minimum distance not less than the size q of the finite field, which indicates our codes can correct more quantum errors. Meanwhile, we describe the exact relation between the minimum distance d and the maximally entangled state c by introducing the variable t. In addition, our constructions place the size q on a general case, not only take an odd prime power.

The material is organized as below. In Section 2, we review some basic concepts on cyclic codes, cyclotomic cosets, and EAQMDS codes. In Section 3, two classes of EAQMDS codes are gained from cyclic codes. In Section 4, detailed comparison and discussion are made.

2 Preliminaries

We recall some basic results on cyclic code, defining set of cyclic code and EAQECCs. For more details, please refer to Refs. [1, 12, 13, 23]. Let q be any prime power and $\mathbb{F}_{q^2}$ be the finite field with q^2 elements. For any element $\beta \in \mathbb{F}_{q^2}$, $\bar{\beta} = \beta^q$ is the conjugation of β. Given two vectors $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ and $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_{q^2}^n$, define their Hermitian inner product by

$$\langle \mathbf{u}, \mathbf{v} \rangle_h = u_0\bar{v}_0 + u_1\bar{v}_1 + \cdots + u_{n-1}\bar{v}_{n-1}.$$

An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_{q^2}$ is a subspace of $\mathbb{F}_{q^2}^n$ with dimension k. Define the Hermitian dual code of $\mathcal{C}$ as

$$\mathcal{C}^{\perp_h} = \{\mathbf{u} \in \mathbb{F}_{q^2}^n \mid \langle \mathbf{u}, \mathbf{v} \rangle_h = 0, \ \forall\, \mathbf{v} \in \mathcal{C}\}.$$

If $\mathcal{C}$ is contained in $\mathcal{C}^{\perp_h}$, then $\mathcal{C}$ is said to be Hermitian self-orthogonal. Particularly, if $\mathcal{C} = \mathcal{C}^{\perp h}$, then $\mathcal{C}$ is said to be Hermitian self-dual. A subspace $\mathcal{C} \subseteq \mathbb{F}_{q^2}^n$ is a cyclic code if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, then $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. Any codeword $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ can be written as a polynomial $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ in the quotient ring $\mathbb{F}_{q^2}[x]/\langle x^n - 1\rangle$. This means that $\mathcal{C}$ is a cyclic code is equivalent to the set of polynomial representations of the codewords of $\mathcal{C}$ forms an ideal of $\mathbb{F}_{q^2}[x]/\langle x^n - 1\rangle$. Because every ideal of $\mathbb{F}_{q^2}[x]/\langle x^n - 1\rangle$ is a principal ideal, $\mathcal{C}$ can be generated by a monic polynomial $g(x) \mid (x^n - 1)$ with the least degree. That is, $\mathcal{C} = \langle g(x)\rangle \subseteq \mathbb{F}_{q^2}[x]/\langle x^n - 1\rangle$, where $g(x)$ is referred to as the generator polynomial of $\mathcal{C}$ and $h(x) = (x^n - 1)/g(x)$ is referred to as the check polynomial of $\mathcal{C}$. Assume that $\gcd(n, q) = 1$. Let α be a primitive n-th root of unity in some extension field of $\mathbb{F}_{q^2}$. Denote $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Define the defining set of $\mathcal{C} = \langle g(x)\rangle$ by

$$T = \{i \in \mathbb{Z}_n \mid g(\alpha^i) = 0\}.$$

It is well known that there is a close connection between cyclic codes and cyclotomic cosets. Define the q^2-cyclotomic coset modulo n containing the integer i by

$$C_i = \{i, iq^2, iq^4, \ldots, iq^{2(m-1)}\} (\mathrm{mod}\ n),$$

where m is the smallest positive integer such that $iq^{2m} \equiv i\,(\mathrm{mod}\ n)$. Notice that the defining set T forms the union of some q^2-cyclotomic cosets. It follows that $\mathcal{C}$ has dimension $k = n - \mid T \mid$. The following lemma is a known fact on the minimum distance of cyclic codes.

Lemma 2 *(The BCH bound for cyclic codes)* [2, 11, 32] *Suppose that $\mathcal{C}$ is a cyclic code of length n with defining set T, which contains δ consecutive elements, where $1 \leq \delta \leq n-1$. Then $d(\mathcal{C}) \geq \delta + 1$.*

To explore the characters of cyclotomic cosets, we follow some notations from the literature [21]. A q^2-cyclotomic coset C_i modulo n is said to be skew asymmetric if $C_i \neq C_{-qi}$; otherwise it is said to be skew symmetric. If C_i is a skew asymmetric coset, then (C_i, C_{-qi}) forms a skew asymmetric pair. By using any linear code $\mathcal{C}$ over $\mathbb{F}_{q^2}$, we can construct an EAQEC code. However, there exists a barrier to calculate the parameter c. In [21], the idea of the decomposition of defining set of a cyclic code was proposed. For any cyclic code over $\mathbb{F}_{q^2}$ of length n with defining set T, $T \bigcap -qT$ contains all the skew symmetric cosets and skew asymmetric pairs [22]. Moreover, the cyclotomic cosets $T \setminus (T \bigcap -qT)$ are all skew asymmetric.

Definition 1 [21] Suppose that $\mathcal{C}$ is a cyclic code over $\mathbb{F}_{q^2}$ of length n with defining set T. Write $T_1 = T \bigcap -qT$ and $T_2 = T \setminus T_1$, where $-qT = \{-qx(\text{mod } n) \mid x \in T\}$. The intersection $T = T_1 \bigcup T_2$ is called the decomposition of T.

The following lemma provides an effective method for determining the number c of maximally entangled states.

Lemma 3 [22] *Let $\mathcal{C}$ be a $[n, k, d]_{q^2}$ cyclic code over $\mathbb{F}_{q^2}$ with defining set T. If $T = T_1 \bigcup T_2$, then there exists an EAQEC code with parameters $[[n, n-2 \mid T \mid + \mid T_1 \mid, d; \mid T_1 \mid]]_q$.*

Let q be arbitrary prime power. Let $n = \frac{q^2-1}{r}$ with $r \mid (q+1)$. In the next two sections, we will construct some EAQMDS codes from cyclic codes with length $n = \frac{q^2-1}{r}$, for $r = 3, 5$. In order to calculate $\mid T_1 \mid$, we need to find skew symmetric cosets C_i and skew asymmetric pairs (C_i, C_j). From $C_j = -qC_i$, we can obtain $C_i = -qC_j$ since $q^2 \equiv 1(\text{mod } n)$. Thus, we only consider the case when $j \leq i$.

Lemma 4 *Assume that $n = \frac{q^2-1}{r}$, where r is odd with $r \mid (q+1)$ and $r' = \frac{q+1}{r}$. Then C_i is skew symmetric if and only if $i = \frac{\ell(q-1)}{2}$, where ℓ is even and $2 \leq \ell \leq 2(r'-1)$.*

Proof Suppose that $C_j = -qC_i$, for $i, j \in \mathbb{Z}_n$. Then,

$$iq + j \equiv 0(\text{mod } n). \tag{1}$$

Notice that $(q-1) \mid n$. By operating both sides of (1) modulo $q-1$, we get $i + j \equiv 0(\text{mod } q-1)$. Hence, $i + j = \ell(q-1)$, for some positive integer ℓ. We consider two cases.

(i) q is even. C_i is skew symmetric if and only if $i = j = \frac{\ell(q-1)}{2}$, where $2 \leq \ell \leq 2(r'-1)$ is even.

(ii) q is odd. We first prove that C_i is a skew asymmetric coset if $i = 2s+1 \in \mathbb{Z}_n$. Assume that $C_{2s+1} = -qC_{2s+1}$. Then $(2s+1)(q+1) \equiv 0(\text{mod } n)$, equivalently, $(2s+1)r \equiv 0(\text{mod } q-1)$. It follows that $(q-1) \mid (2s+1)r$. Observe that $q-1$ is even and $(2s+1)r$ is odd. This produces a contradiction. So, C_{2s+1} is skew asymmetric. It remains to find all skew symmetric cosets in C_{2s}. Clearly, C_{2s} is skew symmetric if and only if $C_{2s} = -qC_{2s}$. That is, $2s(q+1) \equiv 0(\text{mod } n)$. Hence, $2sr \equiv 0(\text{mod } q-1)$, equivalently, $(q-1) \mid 2sr$. Since $\gcd(q-1, r) = 1$, it must be $(q-1) \mid 2s$. Therefore, $i = 2s = h(q-1)$, where $1 \leq h \leq r'-1$. This means that $i = \frac{\ell(q-1)}{2}$, where $\ell = 2h$ is even and $2 \leq \ell \leq 2(r'-1)$.

This completes the proof. □

3 Construction of EAQMDS Codes of Length $\frac{q^2-1}{3}$

In this section, we assume that $q \geq 11$ is a power of any prime. Let $n = \frac{q^2-1}{3}$, where $3 \mid (q+1)$. We are going to seek EAQMDS codes with length n based on the structure of cyclic codes. We present the explicit expressions of the relation between the number c of entangled states and minimum distance d. Some properties about cyclotomic cosets are described as below.

Lemma 5 *Assume that $n = \frac{q^2-1}{3}$, where $q \geq 11$ and $3 \mid (q+1)$. Let t be an integer with $1 \leq t \leq \lceil \frac{q-8}{6} \rceil$.*

(i) *If $tq - 1 \leq \delta \leq t(q-1) + \frac{q-2}{3}$ and $1 \leq j < i \leq \delta$, then (C_i, C_j) is a skew asymmetric pair if and only if $i = \frac{mq+m-3\ell}{3}$ and $j = \frac{3\ell q - mq - m}{3}$, where $1 \leq \ell \leq 2t$ and $\frac{3\ell}{2} < m \leq \min\{3t, 3\ell - 1\}$.*

(ii) *If $tq + \frac{q-2}{3} \leq \delta \leq t(q-1) + \frac{2q-4}{3}$ and $1 \leq j < i \leq \delta$, then (C_i, C_j) is a skew asymmetric pair if and only if $i = \frac{mq+m-3\ell}{3}$ and $j = \frac{3\ell q - mq - m}{3}$, where $1 \leq \ell \leq 2t+1$ and $\frac{3\ell}{2} < m \leq \min\{3t+1, 3\ell - 1\}$.*

(iii) *If $tq + \frac{2q-1}{3} \leq \delta \leq t(q-1) + q - 2$ and $1 \leq j < i \leq \delta$, then (C_i, C_j) is a skew asymmetric pair if and only if $i = \frac{mq+m-3\ell}{3}$ and $j = \frac{3\ell q - mq - m}{3}$, where $1 \leq \ell \leq 2t+1$ and $\frac{3\ell}{2} < m \leq \min\{3t+2, 3\ell - 1\}$.*

Proof We only show the result (i). The proofs of (ii) and (iii) are similar. We first consider the case when $\delta = t(q-1) + \frac{q-2}{3}$.

Let i and j be integers with $1 \leq j < i \leq t(q-1) + \frac{q-2}{3}$. If $C_j = -qC_i$, then

$$iq + j \equiv 0 (\text{mod } n). \tag{2}$$

Notice that $(q-1)$ is a divisor of n. Operating both sides of (2) modulo $q-1$ gets $i + j \equiv 0 (\text{ mod } q-1)$. Since $2 < i + j < 2\delta \leq 2t(q-1) + \frac{2(q-2)}{3}$, we have $i + j = \ell(q-1)$, where $1 \leq \ell \leq 2t$. Then $j = \ell(q-1) - i$. Putting it into (2) we obtain $i + \ell \equiv 0 (\text{ mod } \frac{q+1}{3})$. Hence, $i = \frac{mq+m-3\ell}{3}$ and $j = \frac{3\ell q - mq - m}{3}$, for some positive integer m. We now determine the range of m. Since $1 \leq j < i$ and $i + j = \ell(q-1)$, it follows that $\frac{\ell(q-1)}{2} < i \leq \ell(q-1) - 1$. From $i > \frac{\ell(q-1)}{2}$, we obtain $m > \frac{3\ell}{2}$. From $2 \leq i \leq \frac{(3t+1)q - 3t - 2}{3}$ and $1 \leq \ell \leq 2t$, we obtain $m(q+1) - 6t \leq m(q+1) - 3\ell \leq 3t(q+1) + q - 6t - 2$ and $m \leq 3t$. Hence, $\frac{3\ell}{2} < m \leq 3t$. From $i \leq \ell(q-1) - 1$, if $m \geq 3\ell$, then $i \geq \ell q$, which is a contradiction. So, it must be $m \leq 3\ell - 1$, implying that $i \leq \ell q - \frac{q+1}{3}$. Notice that $\ell \leq 2t \leq \lceil \frac{q-8}{3} \rceil$ and $q \geq 11$. This means that the condition $i \leq \ell(q-1) - 1$ is met. Hence, $\frac{3\ell}{2} < m \leq \min\{3t, 3\ell - 1\}$.

Conversely, suppose $i = \frac{mq+m-3\ell}{3}$ and $j = \frac{3\ell q - mq - m}{3}$, where $1 \leq \ell \leq 2t$ and $\frac{3\ell}{2} < m \leq \min\{3t, 3\ell - 1\}$. It easy to compute that $1 \leq j < i$ and $iq + j = \frac{m(q^2-1)}{3} \equiv 0 (\text{mod } n)$. Hence, $C_j = -qC_i$, i.e., (C_i, C_j) is a skew asymmetric pair.

Hence, we already show that the result (i) holds true for $\delta = t(q-1) + \frac{q-2}{3}$. For a given integer t with $1 \leq t \leq \lceil \frac{q-8}{6} \rceil$, notice that when $\ell = t+1$ and $m = 3t$, the integer $i \in \mathbb{Z}_n$ such that (C_i, C_j) is a skew asymmetric pair has the largest value $tq - 1$. Thus, the result (i) holds true for $tq - 1 \leq \delta \leq t(q-1) + \frac{q-2}{3}$. □

Lemma 6 *Assume that $n = \frac{q^2-1}{3}$, where $q \geq 11$ and $3 \mid (q+1)$. Then C_i is skew symmetric if and only if $i = \frac{mq+m-3\ell}{3}$ and $m = \frac{3\ell}{2}$, where ℓ is even and $2 \leq \ell \leq \frac{2(q-2)}{3}$.*

Proof The result can be easily obtained from Lemma 4. □

Let $T = \bigcup_{i=1}^{\delta} C_i$, where δ is in one of the three ranges:

- (R1) $tq - 1 \le \delta \le t(q-1) + \frac{q-2}{3}$.
- (R2) $tq + \frac{q-2}{3} \le \delta \le t(q-1) + \frac{2q-4}{3}$.
- (R3) $tq + \frac{2q-1}{3} \le \delta \le t(q-1) + q - 2$.

Next, we compute the cardinality of T_1 in the above three ranges, respectively. We first consider the range (R1). To facilitate our calculation, we introduce the following notations. For a given integer ℓ with $1 \le \ell \le 2t$, let

$$\mathcal{L}_m^{(\ell)} = \left\{ m \mid \frac{3\ell}{2} < m \le \min\{3t, 3\ell - 1\} \right\},$$
$$\mathcal{S}_i^{(\ell)} = \left\{ i \mid i = \frac{mq + m - 3\ell}{3}, \text{ for } \frac{3\ell}{2} < m \le \min\{3t, 3\ell - 1\} \right\},$$
$$\mathcal{T}_j^{(\ell)} = \left\{ j \mid j = \frac{3\ell q - mq - m}{3}, \text{ for } \frac{3\ell}{2} < m \le \min\{3t, 3\ell - 1\} \right\}.$$

Write $N^{(\ell)} = \mid \mathcal{S}_i^{(\ell)} \cup \mathcal{T}_j^{(\ell)} \mid$.

Lemma 7 *Assume that* $n = \frac{q^2-1}{3}$, *where* $q \ge 11$ *and* $3 \mid (q+1)$. *Let* t *be an integer with* $1 \le t \le \lceil \frac{q-8}{6} \rceil$. *If* $T = \bigcup_{i=1}^{\delta} C_i$, *where* $tq - 1 \le \delta \le t(q-1) + \frac{q-2}{3}$, *then* $\mid T_1 \mid = 3t^2$.

Proof For a given integer t with $1 \le t \le \lceil \frac{q-8}{6} \rceil$, set $\lambda = t(q-1) + \frac{q-2}{3}$ and $T_\lambda = \bigcup_{i=1}^{\lambda} C_i$. By Lemma 5 (i), we only need to compute $\mid T_\lambda \cap -qT_\lambda \mid$.

Let i and j be integers with $1 \le j \le i \le \lambda$. From Lemmas 5 (i) and 6, $i = \frac{mq+m-3\ell}{3}$, where $1 \le \ell \le 2t$ and

$$\frac{3\ell}{2} \le m \le \min\{3t, 3\ell - 1\}. \tag{3}$$

When $1 \le \ell \le t$, $\min\{3t, 3\ell - 1\} = 3\ell - 1$; when $t + 1 \le \ell \le 2t$, $\min\{3t, 3\ell - 1\} = 3t$. Note that $1 \le \ell \le 2t$. Denote $T_\ell^{(o)} = \{1, 3, \ldots, 2t - 1\}$ and $T_\ell^{(e)} = \{2, 4, \ldots, 2t\}$. Let

$$T_i^{(o)} = \left\{ i \mid i = \frac{mq + m - 3\ell}{3}, \text{ for } \ell \in T_\ell^{(o)} \right\},$$
$$T_i^{(e)} = \left\{ i \mid i = \frac{mq + m - 3\ell}{3}, \text{ for } \ell \in T_\ell^{(e)} \right\},$$
$$T_j^{(o)} = \left\{ j \mid j = \frac{3\ell q - mq - m}{3}, \text{ for } \ell \in T_\ell^{(o)} \right\},$$
$$T_j^{(e)} = \left\{ j \mid j = \frac{3\ell q - mq - m}{3}, \text{ for } \ell \in T_\ell^{(e)} \right\}.$$

Hence,

$$\mid T_1 \mid = \mid T_\lambda \cap -qT_\lambda \mid = \mid T_i^{(o)} \cup T_j^{(o)} \mid + \mid T_i^{(e)} \cup T_j^{(e)} \mid .$$

We now deal with the two cases where t is odd and even.

- **Case 1**: t is odd.
  When ℓ takes an odd integer with $1 \le \ell \le 2t$, then $\frac{3\ell+1}{2} \le m \le \min\{3t, 3\ell - 1\}$. From Lemma 6, we have $j < i$. If $1 \le \ell \le t$, then $\mid \mathcal{L}_m^{(\ell)} \mid = 3\ell - 1 - \frac{3\ell+1}{2} + 1 = \frac{3\ell-1}{2}$ and

$N^{(\ell)} = 2 \mid \mathcal{L}_m^{(\ell)} \mid = 3\ell - 1$. If $t+1 \le \ell \le 2t$, then $\mid \mathcal{L}_m^{(\ell)} \mid = 3t - \frac{3\ell+1}{2} + 1 = 3t - \frac{3\ell}{2} + \frac{1}{2}$ and $N^{(\ell)} = 2 \mid \mathcal{L}_m^{(\ell)} \mid = 6t - 3\ell + 1$. We have

$$N^{(1)} + N^{(3)} + \cdots + N^{(t)} = \frac{\left(N^{(1)} + N^{(t)}\right) \cdot \frac{t+1}{2}}{2} = \frac{3t^2 + 4t + 1}{4}$$

and

$$N^{(t+2)} + N^{(t+4)} + \cdots + N^{(2t-1)} = \frac{\left(N^{(t+2)} + N^{(2t-1)}\right) \cdot \frac{t-1}{2}}{2} = \frac{3t^2 - 4t + 1}{4}.$$

Hence,

$$\mid T_i^{(o)} \cup T_j^{(o)} \mid = \frac{3t^2 + 4t + 1}{4} + \frac{3t^2 - 4t + 1}{4} = \frac{3t^2 + 1}{2}.$$

When ℓ takes an even integer with $1 \le \ell \le 2t$, then $\frac{3\ell+1}{2} \le m \le \min\{3t, 3\ell - 1\}$. From Lemma 6, C_i is skew symmetric if and only if $i = j$; if and only if $m = \frac{3\ell}{2}$. When $j < i$, $\frac{3\ell+1}{2} \le m \le \min\{3t, 3\ell - 1\}$. If $1 \le \ell \le t$, then $\mid \mathcal{L}_m^{(\ell)} \mid = 3\ell - 1 - \frac{3\ell+2}{2} + 1 = \frac{3\ell-2}{2}$ and $N^{(\ell)} = 2 \mid \mathcal{L}_m^{(\ell)} \mid +1 = 3\ell - 1$. If $t+1 \le \ell \le 2t$, then $\mid \mathcal{L}_m^{(\ell)} \mid = 3t - \frac{3\ell+2}{2} + 1 = 3t - \frac{3\ell}{2}$ and $N^{(\ell)} = 2 \mid \mathcal{L}_m^{(\ell)} \mid +1 = 6t - 3\ell + 1$. We have

$$N^{(2)} + N^{(4)} + \cdots + N^{(t-1)} = \frac{\left(N^{(2)} + N^{(t-1)}\right) \cdot \frac{t-1}{2}}{2} = \frac{3t^2 - 2t - 1}{4}$$

and

$$N^{(t+1)} + N^{(t+3)} + \cdots + N^{(2t)} = \frac{\left(N^{(t+1)} + N^{(2t)}\right) \cdot \frac{t+1}{2}}{2} = \frac{3t^2 + 2t - 1}{4}.$$

Hence, $\mid T_i^{(e)} \cup T_j^{(e)} \mid = \frac{3t^2-2t-1}{4} + \frac{3t^2+2t-1}{4} = \frac{3t^2-1}{2}$. Thus, $\mid T_1 \mid = \frac{3t^2+1}{2} + \frac{3t^2-1}{2} = 3t^2$.

- **Case 2**: t is even.
  When ℓ takes an odd integer with $1 \le \ell \le 2t$, in the same way, we get

$$N^{(1)} + N^{(3)} + \cdots + N^{(t-1)} = \frac{\left(N^{(1)} + N^{(t-1)}\right) \cdot \frac{t}{2}}{2} = \frac{3t^2 - 2t}{4}$$

and

$$N^{(t+1)} + N^{(t+4)} + \cdots + N^{(2t-1)} = \frac{\left(N^{(t+1)} + N^{(2t-1)}\right) \cdot \frac{t}{2}}{2} = \frac{3t^2 + 2t}{4}.$$

Hence,

$$\mid T_i^{(o)} \cup T_j^{(o)} \mid = \frac{3t^2 - 2t}{4} + \frac{3t^2 + 2t}{4} = \frac{3t^2}{2}.$$

When ℓ takes an even integer with $1 \le \ell \le 2t$, in the same way, we have

$$N^{(2)} + N^{(4)} + \cdots + N^{(t)} = \frac{\left(N^{(2)} + N^{(t)}\right) \cdot \frac{t}{2}}{2} = \frac{3t^2 + 4t}{4}$$

and

$$N^{(t+2)} + N^{(t+4)} + \cdots + N^{(2t)} = \frac{\left(N^{(t+2)} + N^{(2t)}\right) \cdot \frac{t}{2}}{2} = \frac{3t^2 - 4t}{4}.$$

Hence, $\mid T_i^{(e)} \cup T_j^{(e)} \mid = \frac{3t^2+4t}{4} + \frac{3t^2-4t}{4} = \frac{3t^2}{2}$. Thus, $\mid T_1 \mid = \frac{3t^2}{2} + \frac{3t^2}{2} = 3t^2$.

This completes the proof. □

For the ranges (R2) and (R3), we can compute the exact values of $| T_1 |$ by using an analogues technique as in the range (R1). The proofs are omitted here.

Lemma 8 *Assume that* $n = \frac{q^2-1}{3}$, *where* $q \geq 11$ *and* $3 \mid (q+1)$. *Let* t *be an integer with* $1 \leq t \leq \lceil \frac{q-8}{6} \rceil$.

(i) *If* $tq + \frac{q-2}{3} \leq \delta \leq t(q-1) + \frac{2q-4}{3}$, *then* $| T_1 | = 3t^2 + 2t$.
(ii) *If* $tq + \frac{2q-1}{3} \leq \delta \leq t(q-1) + q - 2$, *then* $| T_1 | = 3t^2 + 4t + 2$.

Let $\mathcal{C}$ be a cyclic code in $\mathbb{F}_{q^2}[x]/\langle x^n - 1\rangle$ and have defining set $T = \bigcup_{i=1}^{\delta} C_i$. Now, we can find EAQMDS codes with length $n = \frac{q^2-1}{3}$ stemmed from the cyclic code $\mathcal{C}$.

Theorem 1 *Let* $q \geq 11$ *be a power of any prime. Let* $n = \frac{q^2-1}{3}$ *with* $3 \mid (q+1)$. *For any integer* t *with* $1 \leq t \leq \lceil \frac{q-8}{6} \rceil$, q*-ary EAQMDS codes with the following parameters can be constructed from* $\mathcal{C}$

(i) $[[n, n-2d+3t^2+2, d; 3t^2]]_q$, *where* $tq \leq d \leq t(q-1) + \frac{q+1}{3}$.
(ii) $[[n, n-2d+3t^2+2t+2, d; 3t^2+2t]]_q$, *where* $tq + \frac{q+1}{3} \leq d \leq t(q-1) + \frac{2q-1}{3}$.
(iii) $[[n, n-2d+3t^2+4t+4, d; 3t^2+4t+2]]_q$, *where* $tq + \frac{2(q+1)}{3} \leq d \leq (t+1)(q-1)$.

Proof Fix an integer t with $1 \leq t \leq \lceil \frac{q-8}{6} \rceil$. Let $\mathcal{C}$ be the cyclic code over $\mathbb{F}_{q^2}$ of length $n = \frac{q^2-1}{3}$ having defining set $T = \bigcup_{i=1}^{\delta} C_i$, where $tq - 1 \leq \delta \leq t(q-1) + \frac{q-2}{3}$. Notice that every cyclotomic coset C_i has only one element. So, $| T | = \delta$ and $\dim(\mathcal{C}) = n - \delta$. Since the defining set of $\mathcal{C}$ contains δ consecutive integers, by Lemma 2, $d(\mathcal{C}) \geq \delta + 1$. Hence, $\mathcal{C}$ is an $[n, n-\delta, \delta+1]$ MDS cyclic code over $\mathbb{F}_{q^2}$. From Lemma 7, $| T_1 | = 3t^2$. By Lemma 3, there exists an $[[n, n-2d+3t^2+2, d; 3t^2]]_q$ EAQEC code, where $tq \leq d \leq t(q-1) + \frac{q+1}{3}$. It is easy to check that its parameters attain the bound $2d = n - k + c + 2$, moreover, $d \leq \frac{n+2}{2}$. Thus, the resulting code is an EAQMDS code. This proves the result (i). Apply Lemma 8 to the cyclic codes $\mathcal{C}$ with the ranges (R2) and (R3), respectively. Then we can get the latter two classes of EAQMDS codes in a similar way. □

4 Construction of EAQMDS Codes of Length $\frac{q^2-1}{5}$

We are now ready to construct EAQMDS codes with $n = \frac{q^2-1}{5}$. Assume that $q \geq 19$ is a power of any prime power with $5 \mid (q+1)$.

Lemma 9 *Assume that* $n = \frac{q^2-1}{5}$, *where* $q \geq 19$ *and* $5 \mid (q+1)$. *Let* t *be a positive integer with* $1 \leq t \leq \lceil \frac{q-14}{10} \rceil$.

(i) *If* $tq - 1 \leq \delta \leq t(q-1) + \frac{q-4}{5}$ *and* $1 \leq j < i \leq \delta$, *then* (C_i, C_j) *is a skew asymmetric pair with* $1 \leq j < i \leq \delta$ *if and only if* $i = \frac{mq+m-5\ell}{5}$ *and* $j = \frac{5\ell q - mq - m}{5}$, *where* $1 \leq \ell \leq 2t$ *and* $\frac{5\ell}{2} < m \leq \min\{5t, 5\ell - 1\}$.
(ii) *If* $tq + \frac{q-4}{5} \leq \delta \leq t(q-1) + \frac{2q-3}{5}$ *and* $1 \leq j < i \leq \delta$, *then* (C_i, C_j) *is a skew asymmetric pair with* $1 \leq j < i \leq \delta$ *if and only if* $i = \frac{mq+m-5\ell}{5}$ *and* $j = \frac{5\ell q - mq - m}{5}$, *where* $1 \leq \ell \leq 2t$ *and* $\frac{5\ell}{2} < m \leq \min\{5t+1, 5\ell - 1\}$.

(iii) *If* $tq + \frac{2q-3}{5} \le \delta \le t(q-1) + \frac{3q-7}{5}$ *and* $1 \le j < i \le \delta$, *then* (C_i, C_j) *is a skew asymmetric pair with* $1 \le j < i \le \delta$ *if and only if* $i = \frac{mq+m-5\ell}{5}$ *and* $j = \frac{5\ell q-mq-m}{5}$, *where* $1 \le \ell \le 2t+1$ *and* $\frac{5\ell}{2} < m \le \min\{5t+2, 5\ell-1\}$.

(iv) *If* $tq + \frac{3q-2}{5} \le \delta \le t(q-1) + \frac{4q-6}{5}$ *and* $1 \le j < i \le \delta$, *then* (C_i, C_j) *is a skew asymmetric pair with* $1 \le j < i \le \delta$ *if and only if* $i = \frac{mq+m-5\ell}{5}$ *and* $j = \frac{5\ell q-mq-m}{5}$, *where* $1 \le \ell \le 2t+1$ *and* $\frac{5\ell}{2} < m \le \min\{5t+3, 5\ell-1\}$.

(v) *If* $tq + \frac{4q-1}{5} \le \delta \le t(q-1) + q - 2$ *and* $1 \le j < i \le \delta$, *then* (C_i, C_j) *is a skew asymmetric pair with* $1 \le j < i \le \delta$ *if and only if* $i = \frac{mq+m-5\ell}{5}$ *and* $j = \frac{5\ell q-mq-m}{5}$, *where* $1 \le \ell \le 2t+1$ *and* $\frac{5\ell}{2} < m \le \min\{5t+4, 5\ell-1\}$.

Proof We only prove the part (iv). The others are similar. We first handle the case when $\delta = t(q-1) + \frac{4q-6}{5}$.

Let i and j be integers with $1 \le j < i \le t(q-1) + \frac{4q-6}{5}$. If $C_j = -qC_i$, then $iq + j \equiv 0 (\bmod\ n)$. By carrying on two sides modulo $q-1$, we have $i + j \equiv 0 (\bmod\ q-1)$. Since $2 < i+j < (2t+1)(q-1) + \frac{3q-7}{5}$, it follows that $i+j = \ell(q-1)$, where $1 \le \ell \le 2t+1$. Then $j = \ell(q-1) - i$. Plugging it into $iq + j \equiv 0 (\bmod\ n)$, we have $i + \ell \equiv 0 (\bmod\ \frac{q+1}{5})$. So, i and j can be written in the form $i = \frac{mq+m-5\ell}{5}$ and $j = \frac{5\ell q-mq-m}{5}$, respectively. We now work out the range of m and ℓ.

Since $1 \le j < i$ and $i + j = \ell(q-1)$, it follows that $\frac{\ell(q-1)}{2} < i \le \ell(q-1) - 1$. From $i > \frac{\ell(q-1)}{2}$, we have $m > \frac{5\ell}{2}$. From $2 \le i \le \frac{(5t+4)q-5t-6}{5}$ and $1 \le t \le 2t+1$, we get $m(q+1) - 5\ell \le (5t+3)(q+1) + q - 10t - 9$, which implies that $m \le 5t+3$. Suppose $m \ge 5\ell$, then $i \ge \ell q$, which contradicts the condition $i \le \ell(q-1) - 1$. So, it must be $m \le 5\ell - 1$, which means $i \le \ell q - \frac{q+1}{5}$. Since $\ell \le 2t \le \lceil \frac{q-14}{5} \rceil$ and $q \ge 19$, the condition $i \le \ell(q-1) - 1$ is met. Thus, $\frac{5\ell}{2} < m \le \min\{5t+3, 5\ell-1\}$.

Conversely, suppose that $i = \frac{mq+m-5\ell}{5}$ and $j = \frac{5\ell q-mq-m}{5}$, where $1 \le \ell \le 2t+1$ and $\frac{5\ell}{2} < m \le \min\{5t+3, 5\ell-1\}$. It can be checked that $1 \le j < i$ and $iq + j = \frac{m(q^2-1)}{5} \equiv 0 (\bmod\ n)$. Hence, $C_j = -qC_i$, i.e., (C_i, C_j) is a skew asymmetric pair.

So far, we already show that the result (iv) holds true for $\delta = t(q-1) + \frac{4q-6}{5}$. For a given integer t with $1 \le t \le \lceil \frac{q-14}{10} \rceil$, notice that when $\ell = t+1$ and $m = 5t+3$, the integer $i \in \mathbb{Z}_n$ such that (C_i, C_j) is a skew asymmetric pair has the largest value $tq + \frac{3q-2}{5}$. Thus, the result (iv) works for $tq + \frac{3q-2}{5} \le \delta \le t(q-1) + \frac{4q-6}{5}$. □

The following result is necessary to compute the number c of maximally entangled states, which can be directly derived from Lemma 4.

Lemma 10 *Assume that* $n = \frac{q^2-1}{5}$, *where* $q \ge 19$ *and* $5 \mid (q+1)$. *Then* C_i *is skew symmetric if and only if* $i = \frac{mq+m-5\ell}{5}$ *and* $m = \frac{5\ell}{2}$, *where* ℓ *is even and* $2 \le \ell \le \frac{2(q-4)}{5}$.

Let $T = \bigcup_{i=1}^{\delta} C_i$, where δ is in one of the five ranges:

- (R1) $tq - 1 \le \delta \le t(q-1) + \frac{q-4}{5}$.
- (R2) $tq + \frac{q-4}{5} \le \delta \le t(q-1) + \frac{2q-3}{5}$.
- (R3) $tq + \frac{2q-3}{5} \le \delta \le t(q-1) + \frac{3q-7}{5}$.
- (R4) $tq + \frac{3q-2}{5} \le \delta \le t(q-1) + \frac{4q-6}{5}$.
- (R5) $tq + \frac{4q-1}{5} \le \delta \le t(q-1) + q - 2$.

Next, we calculate the number of the elements in T_1 in the above five ranges, respectively. We first consider the range (R1). Similar to the case in Section 3, we define the following notations. For a fixed integer ℓ with $1 \le \ell \le 2t$, let

$$\mathcal{L}_m^{(\ell)} = \left\{ m \mid \frac{5\ell}{2} < m \le \min\{5t, 5\ell - 1\} \right\},$$
$$\mathcal{S}_i^{(\ell)} = \left\{ i \mid i = \frac{mq + m - 5\ell}{5}, \text{ for } \frac{5\ell}{2} < m \le \min\{5t, 5\ell - 1\} \right\},$$
$$\mathcal{T}_j^{(\ell)} = \left\{ j \mid j = \frac{5\ell q - mq - m}{5}, \text{ for } \frac{5\ell}{2} < m \le \min\{5t, 5\ell - 1\} \right\}.$$

Write $N^{(\ell)} = \mid \mathcal{S}_i^{(\ell)} \cup \mathcal{T}_j^{(\ell)} \mid$.

Lemma 11 *Let $n = \frac{q^2-1}{5}$, where $q \ge 19$ and $5 \mid (q+1)$. Assume that $1 \le t \le \lceil \frac{q-14}{10} \rceil$. If $T = \bigcup_{i=1}^{\delta} C_i$, where $tq - 1 \le \delta \le t(q-1) + \frac{q-4}{5}$, then $\mid T_1 \mid = 5t^2$.*

Proof For a given integer t with $1 \le t \le \lceil \frac{q-14}{10} \rceil$, set $\lambda = t(q-1) + \frac{q-4}{5}$ and $T_\lambda = \bigcup_{i=1}^{\lambda} C_i$. By Lemma 9 (i), we only need to compute $\mid T_\lambda \cap -qT_\lambda \mid$.

Let i and j be integers with $1 \le j \le i \le \lambda$. From Lemmas 9 (i) and 10, $i = \frac{mq+m-5\ell}{5}$, where $1 \le \ell \le 2t$ and

$$\frac{5\ell}{2} \le m \le \min\{5t, 5\ell - 1\}. \tag{4}$$

When $1 \le \ell \le t$, $\min\{5t, 5\ell - 1\} = 5\ell - 1$; when $t + 1 \le \ell \le 2t$, $\min\{5t, 5\ell - 1\} = 5t$. Note that $1 \le \ell \le 2t$. Denote $T_\ell^{(o)} = \{1, 3, \ldots, 2t - 1\}$ and $T_\ell^{(e)} = \{2, 4, \ldots, 2t\}$. Let

$$T_i^{(o)} = \left\{ i \mid i = \frac{mq + m - 5\ell}{5}, \text{ for } \ell \in T_\ell^{(o)} \right\},$$
$$T_i^{(e)} = \left\{ i \mid i = \frac{mq + m - 5\ell}{5}, \text{ for } \ell \in T_\ell^{(e)} \right\},$$
$$T_j^{(o)} = \left\{ j \mid j = \frac{5\ell q - mq - m}{5}, \text{ for } \ell \in T_\ell^{(o)} \right\},$$
$$T_j^{(e)} = \left\{ j \mid j = \frac{5\ell q - mq - m}{5}, \text{ for } \ell \in T_\ell^{(e)} \right\}.$$

Hence,

$$\mid T_1 \mid = \mid T_\lambda \cap -qT_\lambda \mid = \mid T_i^{(o)} \cup T_j^{(o)} \mid + \mid T_i^{(e)} \cup T_j^{(e)} \mid .$$

We now deal with the two cases where t is odd and even.

- **Case 1**: t is odd.
  When ℓ takes an odd integer with $1 \le \ell \le 2t$, then $\frac{5\ell+1}{2} \le m \le \min\{5t, 5\ell - 1\}$. From Lemma 10, we have $j < i$. If $1 \le \ell \le t$, then $\mid \mathcal{L}_m^{(\ell)} \mid = 5\ell - 1 - \frac{5\ell+1}{2} + 1 = \frac{5\ell-1}{2}$ and $N^{(\ell)} = 2 \mid \mathcal{L}_m^{(\ell)} \mid = 5\ell - 1$. If $t+1 \le \ell \le 2t$, then $\mid \mathcal{L}_m^{(\ell)} \mid = 5t - \frac{5\ell+1}{2} + 1 = 5t - \frac{5\ell}{2} + \frac{1}{2}$ and $N^{(\ell)} = 2 \mid \mathcal{L}_m^{(\ell)} \mid = 10t - 5\ell + 1$. Moreover,

$$N^{(1)} + N^{(3)} + \cdots + N^{(t)} = \frac{\left(N^{(1)} + N^{(t)}\right) \cdot \frac{t+1}{2}}{2} = \frac{5t^2 + 8t + 3}{4}$$

and

$$N^{(t+2)} + N^{(t+4)} + \cdots + N^{(2t-1)} = \frac{\left(N^{(t+2)} + N^{(2t-1)}\right) \cdot \frac{t-1}{2}}{2} = \frac{5t^2 - 8t + 3}{4}.$$

Hence,

$$| T_i^{(o)} \cup T_j^{(o)} | = \frac{5t^2+8t+3}{4} + \frac{5t^2-8t+3}{4} = \frac{5t^2+3}{2}.$$

When ℓ takes an even integer with $1 \le \ell \le 2t$, then $\frac{5\ell+1}{2} \le m \le \min\{5t, 5\ell-1\}$. From Lemma 10, C_i is skew symmetric, which is equivalent to $i = j$ or $m = \frac{5\ell}{2}$. When $j < i$, $\frac{5\ell+1}{2} \le m \le \min\{5t, 5\ell-1\}$. If $1 \le \ell \le t$, then $| \mathcal{L}_m^{(\ell)} | = 3\ell - 1 - \frac{3\ell+2}{2} + 1 = \frac{3\ell-2}{2}$ and $N^{(\ell)} = 2 | \mathcal{L}_m^{(\ell)} | + 1 = 5\ell - 1$. If $t+1 \le \ell \le 2t$, then $| \mathcal{L}_m^{(\ell)} | = 5t - \frac{5\ell+2}{2} + 1 = 5t - \frac{5\ell}{2}$ and $N^{(\ell)} = 2 | \mathcal{L}_m^{(\ell)} | + 1 = 10t - 5\ell + 1$. Moreover,

$$N^{(2)} + N^{(4)} + \cdots + N^{(t-1)} = \frac{\left(N^{(2)} + N^{(t-1)}\right) \cdot \frac{t-1}{2}}{2} = \frac{5t^2-2t-3}{4}$$

and

$$N^{(t+1)} + N^{(t+3)} + \cdots + N^{(2t)} = \frac{\left(N^{(t+1)} + N^{(2t)}\right) \cdot \frac{t+1}{2}}{2} = \frac{5t^2+2t-3}{4}.$$

Hence, $| T_i^{(e)} \cup T_j^{(e)} | = \frac{5t^2-2t-3}{4} + \frac{5t^2+2t-3}{4} = \frac{5t^2-3}{2}$. Thus, $| T_1 | = \frac{5t^2+3}{2} + \frac{5t^2-3}{2} = 5t^2$.

- **Case 2**: t is even.
  When ℓ takes an odd integer with $1 \le \ell \le 2t$, in the same way, we have

$$N^{(1)} + N^{(3)} + \cdots + N^{(t-1)} = \frac{\left(N^{(1)} + N^{(t-1)}\right) \cdot \frac{t}{2}}{2} = \frac{5t^2-2t}{4}$$

and

$$N^{(t+1)} + N^{(t+4)} + \cdots + N^{(2t-1)} = \frac{\left(N^{(t+1)} + N^{(2t-1)}\right) \cdot \frac{t}{2}}{2} = \frac{5t^2+2t}{4}.$$

Hence,

$$| T_i^{(o)} \cup T_j^{(o)} | = \frac{5t^2-2t}{4} + \frac{5t^2+2t}{4} = \frac{5t^2}{2}.$$

When ℓ takes an even integer with $1 \le \ell \le 2t$, in the same way, we have

$$N^{(2)} + N^{(4)} + \cdots + N^{(t)} = \frac{\left(N^{(2)} + N^{(t)}\right) \cdot \frac{t}{2}}{2} = \frac{5t^2+8t}{4}$$

and

$$N^{(t+2)} + N^{(t+4)} + \cdots + N^{(2t)} = \frac{\left(N^{(t+2)} + N^{(2t)}\right) \cdot \frac{t}{2}}{2} = \frac{5t^2-8t}{4}.$$

Hence, $| T_i^{(e)} \cup T_j^{(e)} | = \frac{5t^2+8t}{4} + \frac{5t^2-8t}{4} = \frac{5t^2}{2}$. Thus, $| T_1 | = \frac{5t^2}{2} + \frac{5t^2}{2} = 5t^2$.

This completes the proof. □

For the ranges (R2) to (R5), we can similarly compute the exact values of $| T_1 |$. The proofs are omitted here.

Lemma 12 *Let* $n = \frac{q^2-1}{5}$, *where* $q \ge 19$ *and* $5 \mid (q+1)$. *Assume that* $1 \le t \le \lceil \frac{q-14}{10} \rceil$.

(i) *If* $tq + \frac{q-4}{5} \le \delta \le t(q-1) + \frac{2q-3}{5}$, *then* $| T_1 | = 5t^2 + 2t$.
(ii) *If* $tq + \frac{2q-3}{5} \le \delta \le t(q-1) + \frac{3q-7}{5}$, *then* $| T_1 | = 5t^2 + 4t$.
(iii) *If* $tq + \frac{3q-2}{5} \le \delta \le t(q-1) + \frac{4q-6}{5}$, *then* $| T_1 | = 5t^2 + 6t + 2$.

(iv) *If* $tq + \frac{4q-1}{5} \leq \delta \leq t(q-1) + q - 2$, *then* $| T_1 | = 5t^2 + 8t + 4$.

Let $\mathcal{C}$ be a cyclic code in $\mathbb{F}_{q^2}[x]/\langle x^n - 1\rangle$ and have defining set $T = \bigcup_{i=1}^{\delta} C_i$. Now, we construct EAQMDS codes with length $n = \frac{q^2-1}{5}$ from the cyclic code $\mathcal{C}$.

Theorem 2 *Let* $q \geq 19$ *be a power of any prime. Let* $n = \frac{q^2-1}{5}$ *with* $5 \mid (q+1)$. *For an integer* t *with* $1 \leq t \leq \lceil \frac{q-14}{10} \rceil$, q*-ary EAQMDS codes with the following parameters can be constructed from* $\mathcal{C}$.

(i) $[[n, n-2d+5t^2+2, d; 5t^2]]_q$, *where* $tq \leq d \leq t(q-1) + \frac{q+1}{5}$.
(ii) $[[n, n-2d+5t^2+2t+2, d; 5t^2+2t]]_q$, *where* $tq + \frac{q+1}{5} \leq d \leq t(q-1) + \frac{2q+2}{5}$.
(iii) $[[n, n-2d+5t^2+4t+2, d; 5t^2+4t]]_q$, *where* $tq + \frac{2q+2}{5} \leq d \leq t(q-1) + \frac{3q-2}{5}$.
(iv) $[[n, n-2d+5t^2+6t+4, d; 5t^2+6t+2]]_q$, *where* $tq + \frac{3q+3}{5} \leq d \leq t(q-1) + \frac{4q-1}{5}$.
(v) $[[n, n-2d+5t^2+8t+6, d; 5t^2+8t+4]]_q$, *where* $tq + \frac{4q+4}{5} \leq d \leq (t+1)(q-1)$.

Proof For a fixed integer t with $1 \leq t \leq \lceil \frac{q-14}{10} \rceil$, suppose that $\mathcal{C}$ is the cyclic code in $\mathbb{F}_{q^2}[x]/\langle x^n - 1\rangle$ with defining set $T = \bigcup_{i=1}^{\delta} C_i$, where $tq - 1 \leq \delta \leq t(q-1) + \frac{q-4}{5}$. Note that C_i contains only one element. This gives that $| T | = \delta$ and $\dim(\mathcal{C}) = n - \delta$. From the BCH bound, $d(\mathcal{C}) \geq \delta + 1$. Therefore, $\mathcal{C}$ has parameters $[n, n-\delta, \delta+1]$ and is a MDS code. From Lemma 11, $| T_1 | = 5t^2$. By Lemma 3, an $[[n, n-2d+5t^2+2, d; 5t^2]]_q$ EAQEC code can be obtained from $\mathcal{C}$, where $tq \leq d \leq t(q-1) + \frac{q+1}{5}$. It can be verified that its parameters meet the equality $2d = n - k + c + 2$. Moreover, $d \leq \frac{n+2}{2}$. Thus, the resulting EAQEC code is EAQMDS. This proves the result (i). By using Lemma 12 to the cyclic codes with the ranges (R2)-(R5) respectively, we can gained the latter four classes of EAQMDS codes in a similar way. □

5 Comparison and Discussion

In this paper, by exploring cyclotomic cosets, we find new EAQMDS codes with length $\frac{q^2-1}{r}$ in the cases when $r = 3$ and $r = 5$, where $r \mid (q+1)$. We introduce the parameter t and describe the relation between the minimum distances d and the number c of maximally entangled states, where the range of t is determined by the field size q. This enables us to construct many EAQMDS codes with minimum distance not less than q and flexible parameters for pre-shared entangled states. Most of the previously known work on EAQMDS codes of length $n = \frac{q^2-1}{r}$ only considered the case that q is an odd prime power [3, 6, 16–19]. The constructions in this paper place on the general case that q is any prime power. We list the resulting EAQMDS codes in Table 1. In the following, we compare our EAQMDS codes with those in the known literature.

In [16], by using cyclic code, Lu et al. found EAQMDS codes with even length and minimum distance greater than $q+1$. We list and compare the parameters between the EAQMDS codes in [16] and the EAQMDS codes here in Table 2. It is easy to find that the parameters in [16] are a special case when $t = 1$. So, the EAQMDS codes here contain all the EAQMDS codes in [16]. In addition, the finite size q can take any even prime power. Thus, the EAQMDS codes here not only generalize the results in [16], but also resolve the case when q is an even prime power.

Table 1 Parameters of the EAQMDS codes constructed in this paper

n	$[[n,k,d;c]]_q$	d
$\frac{q^2-1}{3}$	$[[n, n-2d+3t^2+2, d; 3t^2]]_q$	$tq \le d \le t(q-1)+\frac{q+1}{3}$
	$[[n, n-2d+3t^2+2t+2, d; 3t^2+2t]]_q$	$tq+\frac{q+1}{3} \le d \le t(q-1)+\frac{2q-1}{3}$
	$[[n, n-2d+3t^2+4t+4, d; 3t^2+4t+2]]_q$	$tq+\frac{2(q+1)}{3} \le d \le t(q-1)+q-1$
$\frac{q^2-1}{5}$	$[[n, n-2d+5t^2+2, d; 5t^2]]_q$	$tq \le d \le t(q-1)+\frac{q+1}{5}$
	$[[n, n-2d+5t^2+2t+2, d; 5t^2+2t]]_q$	$tq+\frac{q+1}{5} \le d \le t(q-1)+\frac{2q+2}{5}$
	$[[n, n-2d+5t^2+4t+2, d; 5t^2+4t]]_q$	$tq+\frac{2q+2}{5} \le d \le t(q-1)+\frac{3q-2}{5}$
	$[[n, n-2d+5t^2+6t+4, d; 5t^2+6t+2]]_q$	$tq+\frac{3q+3}{5} \le d \le t(q-1)+\frac{4q-1}{5}$
	$[[n, n-2d+5t^2+8t+6, d; 5t^2+8t+4]]_q$	$tq+\frac{4q+4}{5} \le d \le t(q-1)+q-1$

In [27], Pang et al. gained EAQMDS codes with parameters $[[\frac{q^2-1}{r}, \frac{q^2-1}{r}-2d+2m+1, d; 2m-1]]_q$, where $r \mid (q+1)$, $1 \le m \le \frac{r-1}{2}$ and $\frac{(r+2m-1)(q+1)}{2r} \le d \le \frac{(q-1)r+(2m+1)(q+1)}{2r}$. It is easy to see that the minimum distance of these codes is less than q. We list some EAQMDS codes when q is an even prime power in Table 3 and compare them with our parameters. It can be seen that the EAQMDS codes here have higher error-correcting capability.

In [33], Wang et al. constructed EAQEC codes of length $n = \frac{q-1}{r}(q+1)$ with flexible the number of maximally entanglement bits, where q is any prime power. However, the construction was considered under the condition that $r \mid (q-1)$. As $\gcd(q-1, q+1) = 1$ or 2, the code lengths are different from those of the EAQMDS codes here.

Table 2 Comparison with the EAQMDS codes constructed in Ref. [16]

q	r	t	$[[n,k,d;c]]_q$	d	Reference
17	3	1	$[[96, 101-2d, d; 3]]_{17}$	$17 \le d \le 22$	[16]
17	3	1	$[[96, 103-2d, d; 5]]_{17}$	$23 \le d \le 27$	[16]
17	3	1	$[[96, 107-2d, d; 9]]_{17}$	$29 \le d \le 32$	[16]
17	3	2	$[[96, 110-2d, d; 12]]_{17}$	$34 \le d \le 38$	[16]
17	3	2	$[[96, 114-2d, d; 16]]_{17}$	$40 \le d \le 43$	[16]
17	3	2	$[[96, 120-2d, d; 22]]_{17}$	$46 \le d \le 48$	New
29	5	1	$[[175, 826-2d, d; 5]]_{29}$	$29 \le d \le 34$	[16]
29	5	1	$[[177, 828-2d, d; 7]]_{29}$	$35 \le d \le 40$	[16]
29	5	1	$[[179, 830-2d, d; 9]]_{29}$	$41 \le d \le 45$	[16]
29	5	1	$[[183, 834-2d, d; 13]]_{29}$	$47 \le d \le 51$	[16]
29	5	1	$[[187, 838-2d, d; 17]]_{29}$	$53 \le d \le 56$	New
29	5	2	$[[190, 841-2d, d; 20]]_{29}$	$58 \le d \le 62$	New
29	5	2	$[[194, 845-2d, d; 24]]_{29}$	$64 \le d \le 68$	New
29	5	2	$[[198, 849-2d, d; 28]]_{29}$	$70 \le d \le 73$	New
29	5	2	$[[204, 855-2d, d; 34]]_{29}$	$76 \le d \le 79$	New
29	5	2	$[[210, 861-2d, d; 40]]_{29}$	$82 \le d \le 84$	New

Table 3 Some new EAQMDS codes and comparisons

q	r	t	Our parameters	d	Parameters in [27]
32	3	–	–	–	$[[341, 344-2d, d; 1]]_{32}$ $22 \le d \le 33$
32	3	1	$[[341, 346-2d, d; 3]]_{32}$	$32 \le d \le 42$	New
32	3	1	$[[341, 348-2d, d; 5]]_{32}$	$43 \le d \le 52$	New
32	3	1	$[[341, 352-2d, d; 9]]_{32}$	$54 \le d \le 62$	New
32	3	2	$[[341, 355-2d, d; 12]]_{32}$	$64 \le d \le 73$	New
32	3	2	$[[341, 359-2d, d; 16]]_{32}$	$75 \le d \le 83$	New
32	3	2	$[[341, 365-2d, d; 22]]_{32}$	$86 \le d \le 93$	New
			...		
32	3	4	$[[341, 391-2d, d; 48]]_{32}$	$128 \le d \le 135$	New
32	3	4	$[[341, 399-2d, d; 56]]_{32}$	$139 \le d \le 145$	New
32	3	4	$[[341, 409-2d, d; 66]]_{32}$	$150 \le d \le 155$	New
64	5	–	–	–	$[[819, 822-2d, d; 1]]_{64}$ $39 \le d \le 51$
64	5	–	–	–	$[[819, 824-2d, d; 3]]_{64}$ $52 \le d \le 65$
64	5	1	$[[819, 826-2d, d; 5]]_{64}$	$64 \le d \le 76$	New
64	5	1	$[[819, 828-2d, d; 7]]_{64}$	$77 \le d \le 89$	New
64	5	1	$[[819, 830-2d, d; 9]]_{64}$	$90 \le d \le 101$	New
64	5	1	$[[819, 834-2d, d; 13]]_{64}$	$103 \le d \le 114$	New
64	5	1	$[[819, 838-2d, d; 17]]_{64}$	$116 \le d \le 126$	New
64	5	2	$[[819, 841-2d, d; 20]]_{64}$	$128 \le d \le 139$	New
64	5	2	$[[819, 845-2d, d; 24]]_{64}$	$141 \le d \le 154$	New
64	5	2	$[[819, 849-2d, d; 28]]_{64}$	$154 \le d \le 166$	New
64	5	2	$[[819, 855-2d, d; 34]]_{64}$	$167 \le d \le 179$	New
64	5	2	$[[819, 861-2d, d; 40]]_{64}$	$180 \le d \le 191$	New
			...		
64	5	5	$[[819, 896-2d, d; 125]]_{64}$	$320 \le d \le 328$	New
64	5	5	$[[819, 956-2d, d; 135]]_{64}$	$333 \le d \le 341$	New
64	5	5	$[[819, 966-2d, d; 145]]_{64}$	$346 \le d \le 353$	New
64	5	5	$[[819, 978-2d, d; 157]]_{64}$	$359 \le d \le 366$	New
64	5	5	$[[819, 990-2d, d; 169]]_{64}$	$372 \le d \le 378$	New

The construction here is through determining the number of cyclotomic cosets in T_1 associated with the defining set of a cyclic code over $\mathbb{F}_{q^2}$. By introducing the variable t, the parameter t and c are linked in an expression. In addition, the construction allows the finite size q to take any prime power. Hence, our construction can produce many new EAQMDS codes with large minimum distance and changeable parameters. However, we only establish the connection among the minimum distance d, the number c of maximally entangled states and the variable t. It would be interesting to find the relation among d, c and r so as to construct more new EAQMDS codes.

Funding This study is supported by the National Natural Science Foundation of China under Grant Nos. 61972126, U21A20428, 12171134, 61802102 and 12001002.

Declarations

Ethical approval All the procedures performed in this study were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki Declaration and its later amendments or comparable ethical standards.

Informed consent Informed consent was obtained from all individual participants included in the study.

Conflicts of interest All the authors declare that they have no conflict of interest.

References

1. Berlekamp, E.: Algebraic coding theory, Revised 1984. Aegean Park, Laguna Hills (1984)
2. Brun, T., Devetak, I., Hsieh, M.H.: Correcting quantum errors with entanglement. Science **52**, 436–439 (2006)
3. Chen, J., Huang, Y., Feng, C., Chen, R.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. Quantum Inf. Process. **16**, 303 (2017)
4. Chen, X., Zhu, S., Jing, W.: Cyclic codes and some new entanglement-assisted quantum MDS codes. Des. Codes Cryptogr. **89**, 2533–2551 (2021)
5. Chen, X., Zhu, S., Kai, X.: Entanglement-assisted quantum MDS codes constructed from constacyclic codes. Quantum Inf. Process. **17**, 273 (2018)
6. 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)
7. Fang, W., Fu, F., Li, L., Zhu, S.: Euclidean and Hermitian hulls of MDS codes and their applications to EAQECCs. IEEE Trans. Inf. Theory **66**, 3527–3537 (2020)
8. Galindo, C., Hernando, F., Matsumoto, R., Ruano, D.: Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. Quantum Inf. Process. **18**(116), 1–18 (2019)
9. Guo, G., Li, R.: New entanglement-assisted quantum MDS codes derived from generalized Reed-Solomom codes. Int. J. Theor. Phys. **59**, 1241–1254 (2020)
10. Guenda, K., Jitman, S., Gulliver, T.A.: Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr. **86**, 121–136 (2018)
11. Grassl, M.: Entanglement-assisted quantum communication beating the quantum Singleton bound. Talk at AQIS, Taiwan (2016)
12. Hsieh, M., Devetak, I., Brun, T.: General entanglement-assisted quantum error-correcting codes. Phys. Rev. A **76**, 062313 (2007)
13. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
14. Lai, C., 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)
15. Lai, C., Brun, T.: Entanglement increases the error-correcting ability of quantum error-correcting codes. Phys. Rev. A **88**, 012320 (2013)
16. Lu, H., Kai, X., Zhu, S.: Construction of new entanglement-assisted quantum MDS codes via cyclic codes. Quantum Inf. Process. **21**, 206 (2022)
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., 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)
19. Li, L., Zhu, S., Liu, L., Kai, X.: Entanglement-assisted quantum MDS codes from generalized Reed-Solomon codes. Quantum Inf. Process. **18**, 153 (2019)
20. 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)
21. Li, R., Zuo, F., Liu, Y.: A study of skew symmetric q^2-cyclotomic coset and its applications. J. AirForce Eng. Univ. (Nat. Sci. Ed.) **12**(1), 87 (2011). (In Chinese)
22. Liu, Y., Li, R., Lv, L., Ma, Y.: Application of constacyclic codes to entanglement-assisted quantum maximum distance separable codes. Quantum Inf. Process. **17**, 210 (2018)
23. Macwilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, Amsterdam (1977)

24. Mustafa, S., Emre, K.: An application of constacyclic codes to entanglement-assisted quantum MDS codes. Comput. Appl. Math. **38**, 1–13 (2019)
25. Koroglu, M.E.: New entanglement-assisted MDS quantum codes from constacyclic codes. Quantum Inf. Process. **18**, 44 (2019)
26. Pang, B., Zhu, S., Li, F., Chen, X.: New entanglement-assisted quantum MDS codes with larger minimum distance. Quantum Inf. Process. **19**, 207 (2020)
27. Pang, B., Zhu, S., Wang, L.: New entanglement-assisted quantum MDS codes. Int. J. Quantum Inf. **19**, 2150016 (2021)
28. Qian, J., Zhang, L.: Constructions of new entanglement-assisted quantum MDS and almost MDS codes. Quantum Inf. Process. **18**, 71 (2019)
29. Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A **52**(4), 2493–2496 (1995)
30. Steane, A.M.: Error correcting codes in quantum theory. Phys. Rev. Lett. **77**, 793–797 (1996)
31. Wang, L., Zhu, S., Sun, Z.: Entanglement-assisted quantum MDS codes from cyclic codes. Quantum Inf. Process. **19**, 65 (2020)
32. Wilde, M., Brun, T.: Optimal entanglement formulas for entanglement-assisted quantum coding. Phys. Rev. A **77**, 064302 (2008)
33. Wang, J., Li, R., Lv, J., Song, H.: Entanglement-assisted quantum codes from cyclic codes and negacyclic codes. Quantum Inf. Process. **19**, 138 (2020)