Quantum Information Processing (2022) 21:206
https://doi.org/10.1007/s11128-022-03547-0

Construction of new entanglement-assisted quantum MDS codes via cyclic codes

Hongmei Lu[1] · Xiaoshan Kai[1] · Shixin Zhu[1]

Received: 9 December 2021 / Accepted: 10 May 2022 / Published online: 14 June 2022

Abstract
Entanglement-assisted quantum error-correcting (EAQEC) codes can be transformed from classical linear codes through entanglement-assisted formalism by loosing the dual-containing condition and using pre-shared entanglement. It has become a challenging task to construct optimal EAQEC codes and determine the required number of pre-shared entanglement pairs. In this work, we explore the structure of q^2-ary cyclic codes through analyzing two classes of cyclotomic cosets independently. By computing the number of maximally entangled states, we construct three classes of q-ary entanglement-assisted quantum maximum distance separable (EAQMDS) codes. This construction produces new EAQMDS codes with minimum distance more than $q + 1$.

Keywords Cyclic code · Defining set · EAQEC code · Cyclotomic coset

1 Introduction

Quantum error-correcting codes are the most effective coding scheme in reducing decoherence during quantum communications and quantum computations. Qudits are the basic unit of q-dimensional quantum systems used for quantum information processing. A standard quantum code of length n is a q^k-dimensional subspace of the Hilbert space $(\mathbb{C}^q)^{\otimes n}$, which can encode k qudits of a q-dimensional quantum system into n qudits. Such a quantum code is denoted by $[[n, k, d]]_q$, where d is the minimum distance of the code. A quantum code with minimum distance d can detect up to d

✉ Xiaoshan Kai
kxs6@sina.com

Hongmei Lu
lvhongmeiy@163.com

Shixin Zhu
zhushixin@hfut.edu.cn

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

quantum errors and correct up to $\lfloor \frac{d-1}{2} \rfloor$ quantum errors. It is well known that standard quantum codes can be obtained from classical linear codes that must satisfy certain dual-containing condition. The dual-containing constraint forms a great obstacle in the construction of quantum codes. A significant breakthrough is the discovery of entanglement-assisted quantum error-correcting (EAQEC) codes by Brun et al. [4]. They showed that non-dual-containing quaternary linear codes can be used to construct EAQEC codes if the sender and receiver share pre-existing entanglement. This indicates the construction of quantum codes is not limited by the dual-containing condition. Later, a general coding scheme of the construction of binary EAQEC codes was built and several explicit construction methods were proposed [20, 21, 25, 45]. Afterwards, lots of binary EAQEC codes were constructed by utilizing various classical linear codes over $\mathbb{F}_2$ or $\mathbb{F}_4$ (see [11, 26, 28]). With the realization of fault-tolerant quantum computation [1, 14, 38] and the construction of concatenation technology [16, 42], non-binary EAQEC codes have received much attention. Galindo et al. [12] extended binary construction methods to arbitrary finite fields and gave complete proofs. Many classes of non-binary EAQEC codes have been derived from classical linear codes such as constacyclic codes, LCD codes and Reed-Solomom codes (see [5, 7, 9, 10, 12, 18, 19, 24, 29, 30]). A difficulty in EAQEC code construction is to determine the number of (pairs of) maximally entangled states. There exist two techniques to find such number for present. One is through computing the hull dimension of linear codes [12, 18], and the other is through decomposing the defining sets of constacyclic codes [30].

Let q be a prime power. A q-ary EAQEC code $\mathcal{Q}$ encoding k logical qudits into n physical qudits by using c pairs of maximally entangled states, denoted by $[[n, k, d; c]]_q$, can correct up to $\lfloor \frac{d-1}{2} \rfloor$ quantum errors, where d is called the minimum distance of $\mathcal{Q}$. If $c = 0$, then $\mathcal{Q}$ is a standard $[[n, k, d]]_q$ quantum code. It is desirable to find EAQEC codes with good error-correcting ability. As in classical codes, the parameters of an EAQEC code are mutually restricted. In [4, 27], the authors gave a Singleton-type bound for binary EAQEC codes. Recently, in [2, 17], the authors used different methods to generalize the bound to q-ary EAQEC codes.

Theorem 1.1 ([2, 17]) *Suppose that $\mathcal{C}$ is an EAQEC code with parameters $[[n, k, d; c]]_q$. Then*

$$2(d-1) \leq n - k + c \tag{1}$$

if $d \leq \frac{n+2}{2}$, where $0 \leq c \leq n-1$.

For $d \leq \frac{n+2}{2}$, if an EAQEC code with parameters $[[n, k, d; c]]_q$ meets the bound (1) with equality, then it is said to be an entanglement-assisted quantum maximum distance separable (EAQMDS) code. For $d > \frac{n+2}{2}$, Grassl [15] gave examples of EAQEC codes with parameters beating the bound (1). When the number c of maximally entangled states is fixed, EAQMDS codes are optimal in the sense that they have the largest minimum distance. During the past decade, a number of EAQMDS codes with length n in the range $q + 2 \leq n \leq q^2 + 1$ were constructed from classical linear codes. Fan et al. [10] obtained EAQMDS codes with a few maximally entangled states from classical MDS codes. Qian and Zhang [41] constructed EAQMDS codes with maximal entangled states from classical LCD codes. Liu et al. [29] obtained EAQMDS codes from k-Galois dual codes. Recently, Hu and Liu [22] used Gabidulin codes to gain EAQMDS codes.

Due to good algebraic structure, constacyclic codes including cyclic codes and negacyclic codes are preferred objects on the construction of EAQMDS codes. In 2011, Lu et al. [28] introduced the decomposition of defining sets of cyclic codes to obtain EAQMDS codes with large minimum distance. The technique was extended to general constacyclic codes in [5, 30, 32], and many classes of EAQMDS codes with length n dividing q^2+1 or q^2-1 were derived from them (see [5, 6, 24, 30, 32, 33, 37, 39, 44]). Koroglu [24] obtained EAQMDS codes based on constacyclic codes. Wang et al. [44] obtained EAQMDS codes with less entangled states from cyclic codes. Recently, Chen et al. [7] constructed EAQMDS cyclic codes with flexible parameters and large minimum distance. Meanwhile, EAQMDS codes on various lengths were found through the generalized Reed-Solomon codes (see [9, 19, 34, 35]).

Let $n = \frac{q^2-1}{r}$, where $r \mid (q+1)$ and $r = 3, 5, 7$. In [33], Lu et al. used constacyclic codes to construct EAQMDS codes of length n with minimum distance $d \leq \frac{(q+1)(r+3)}{2r} - 1$. In [30], Liu et al. enlarged the minimum distance of EAQMDS codes up to $d = \frac{(q+1)(r+1)}{r} - 1$. In this work, we will further enlarge the range of the minimum distance by employing cyclic codes over $\mathbb{F}_{q^2}$ of length n. We analyze cyclotomic cosets whose elements are respectively from the sets of even integer numbers and odd integer numbers and determine the number of maximally entangled states. Our construction yields many new EAQEC codes with large minimum distance. In particular, in the case when $r = 3$, we obtain EAQEC codes with minimum distance greater than $2(q+1)$. The paper is organized as follows. In Sect. 2, some notations and results about classical cyclic codes and EAQEC codes are presented. In Sect. 3, we explore the structure of cyclic codes over $\mathbb{F}_{q^2}$ and give a formula of the number of maximally entangled states. In Sect. 4, new EAQEC codes of lengths $\frac{q^2-1}{r}$ $(r = 3, 5, 7)$ are constructed from cyclic codes. Comparisons and conclusions are made in the last section.

2 Preliminaries

Let q be a prime power. Let $\mathbb{F}_{q^2}$ be a finite field with q^2 elements. For any $\alpha \in \mathbb{F}_{q^2}$, define the conjugate of α as $\bar{\alpha} = \alpha^q$. For 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 as

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

The vectors $\mathbf{u}$ and $\mathbf{v}$ are called Hermitian orthogonal if $\langle \mathbf{u}, \mathbf{v} \rangle = 0$. A q^2-ary linear code $\mathcal{C}$ of length n with dimension k and minimum distance d, denoted by $[n, k, d]$, is a k-dimensional subspace of $\mathbb{F}_{q^2}^n$. It is known that, for a q^2-ary $[n, k, d]$ linear code, there exists the Singleton bound $d \leq n - k + 1$. If $d = n - k + 1$ then $\mathcal{C}$ is called a maximum distance separable (MDS) code. Define the Hermitian dual code of $\mathcal{C}$ as

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

Then, $\mathcal{C}^{\perp_H}$ is linear and has dimension $n - \dim(\mathcal{C})$. The Hermitian hull of $\mathcal{C}$, denoted by $Hull_H(\mathcal{C})$, is defined as the intersection of $\mathcal{C}$ and $\mathcal{C}^{\perp_H}$, i.e., $Hull_H(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^{\perp_H}$.

Let τ denote the cyclic shift on $\mathbb{F}_{q^2}^n$ given by $\tau(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, \ldots, c_{n-2})$. A q^2-ary linear code $\mathcal{C}$ of length n is called a cyclic code if $\tau(\mathcal{C}) = \mathcal{C}$. Identity $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_{q^2}^n$ with its polynomial representation $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$. Then, $xc(x)$ corresponds to a cyclic shift of $c(x)$ in the quotient ring $\mathcal{R} = \mathbb{F}_{q^2}[x]/\langle x^n - 1\rangle$. Hence, a q^2-ary cyclic code of length n is an ideal of $\mathcal{R}$. Note that each ideal of $\mathcal{R}$ is principal. Let $\mathcal{C} = \langle g(x)\rangle$ be a q^2-ary cyclic code of length n, where $g(x)$ is a monic polynomial of minimal degree in $\mathcal{C}$. Then $g(x)$ is a divisor of $x^n - 1$ and called the generator polynomial of $\mathcal{C}$. The polynomial $h(x) = (x^n - 1)/g(x)$ is called the check polynomial of $\mathcal{C}$.

Assume that $\gcd(n, q) = 1$. Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ denote the the ring of integers modulo n. For any $i \in \mathbb{Z}_n$, the q^2-cyclotomic coset modulo n containing i is defined by $C_i = \{iq^{2j} (\bmod\ n) \mid 0 \le j \le \ell - 1\} \subseteq \mathbb{Z}_n$, where ℓ is the smallest positive integer such that $iq^{2\ell} \equiv i (\bmod\ n)$. The smallest positive integer in C_i is called the coset leader of C_i. A q^2-cyclotomic coset C_i is said to be skew symmetric if $n - qi (\bmod\ n) \in C_i$, otherwise it is said to be skew asymmetric. Suppose that $\mathcal{C}$ is a q^2-ary cyclic code of length n with generator polynomial $g(x)$. Let β be a primitive n-th root of unity. The set $T = \{i \in \mathbb{Z}_n \mid g(\beta^i) = 0\}$ is called the defining set of $\mathcal{C}$. It is clear that T is a union of some q^2-cyclotomic cosets modulo n and $\dim(\mathcal{C}) = n - |T|$. The minimum distance of $\mathcal{C}$ can be estimated by the BCH bound.

Theorem 2.1 [36] (BCH bound) *Suppose that $\mathcal{C}$ is a cyclic code of length n with defining set T. If T consists of $\delta - 1$ consecutive elements, for $2 \le \delta \le n$, then $d(\mathcal{C}) \ge \delta$.*

Brun et al. [4] proved that binary EAQEC codes can be constructed from quaternary linear codes. The key to the construction is to determine the number of maximally entangled states. Formulas that obtain the number of maximally entangled states required for a binary EAQEC code were provided in [4, 20, 45]. Galindo et al. [12] proved that these formulas hold true for EAQEC codes over any finite field. The following is one of the construction methods of EAQEC codes, which will be used in the sequel.

Theorem 2.2 ([12]) *Let $\mathcal{C}$ be a q^2-ary $[n, k, d]$ linear code with parity check matrix H. Then there exists an $[[n, 2k - n + c, d; c]]_q$ EAQEC code, where $c = \mathrm{rank}(HH^\dagger)$ and $H^\dagger$ denotes the conjugate transport of H.*

A relation between $\mathrm{rank}(HH^\dagger)$ and the dimension of the Hermitian hull of a q^2-ary linear code is established in [12, 18].

Theorem 2.3 ([12, 18]) *Let $\mathcal{C}$ be a q^2-ary $[n, k, d]$ linear code with parity check matrix H. Then*

$$\mathrm{rank}(HH^\dagger) = n - k - \dim(Hull_H(\mathcal{C})). \tag{2}$$

Thus, the problem of determining the number of maximally entangled states is transformed into computing $\mathrm{rank}(HH^\dagger)$ or $\dim(Hull_H(\mathcal{C}))$. In the next section, we will use the relation to obtain an approach to finding the number c from the defining set.

3 The number of maximally entangled states

From now on, we assume that q is an odd prime power and n is an even positive integer with $\gcd(n, q) = 1$. Let $\mathcal{C}$ be a cyclic code over $\mathbb{F}_{q^2}$ of length n with parity check matrix H. Following the ideas and methods in [13], we provide a formula that derives the number of maximally entangled states for EAQEC codes from $\mathcal{C}$. By Theorems 2.2 and 2.3, it suffices to compute the value of either $\mathrm{rank}(HH^\dagger)$ or $\dim(Hull_H(\mathcal{C}))$.

Let $m = \frac{n}{2}$. Then $x^n - 1 = (x^m - 1)(x^m + 1)$ in $\mathbb{F}_{q^2}[x]$. Let ξ be a primitive n-th root of unity. Then ξ^2 is a primitive m-th root of unity. Then $x^m - 1$ has roots ξ^i for $i = 0, 2, \ldots, 2(m-1)$ and $x^m + 1$ has roots ξ^j for $j = 1, 3, \ldots, 2m - 1$. Let

$$\Omega_e = \{0, 2, \ldots, 2(m-1)\} \text{ and } \Omega_o = \{1, 3, \ldots, 2m-1\}.$$

Suppose that $\mathcal{C}$ is a cyclic code over $\mathbb{F}_{q^2}$ of length n with defining set T. Then $T = T_e \cup T_o$, where T_e and T_o are the unions of some q^2-cyclotomic cosets modulo n from Ω_e and Ω_o, respectively. Denote $T^{-q} = \{-qt(\text{mod } n) \mid t \in T\}$. It can be checked that T^{-q} is the complement of the defining set of $\mathcal{C}^{\perp_H}$ (see [3]).

Lemma 3.1 *Let $\mathcal{C}$ be a cyclic code over $\mathbb{F}_{q^2}$ of length n with defining set $T = T_e \cup T_o$. Then $T \cap T^{-q} = (T_e \cap T_e^{-q}) \cup (T_o \cap T_o^{-q})$ and $|T \cap T^{-q}| = |T_e \cap T_e^{-q}| + |T_o \cap T_o^{-q}|$.*

Proof Notice that $T_e \cap T_o = \emptyset$ and $T_e^{-q} \cap T_o^{-q} = \emptyset$. We have

$$\begin{aligned} T \cap T^{-q} &= (T_e \cup T_o) \cap (T_e^{-q} \cup T_o^{-q}) \\ &= (T_e \cap T_e^{-q}) \cup (T_e \cap T_o^{-q}) \cup (T_o \cap T_e^{-q}) \cup (T_o \cap T_o^{-q}) \\ &= (T_e \cap T_e^{-q}) \cup (T_o \cap T_o^{-q}). \end{aligned}$$

Hence, $|T \cap T^{-q}| = |T_e \cap T_e^{-q}| + |T_o \cap T_o^{-q}|$. □

It is known that the defining set of $\mathcal{C}^{\perp_H}$ is $T^{\perp_H} = \mathbb{Z}_n \backslash T^{-q}$. Denote $T_e^{\perp_H} = \Omega_e \backslash T_e^{-q}$ and $T_o^{\perp_H} = \Omega_o \backslash T_o^{-q}$.

Lemma 3.2 *Let $\mathcal{C}$ be a cyclic code over $\mathbb{F}_{q^2}$ of length n with defining set $T = T_e \cup T_o$. Then the defining set of $\mathcal{C}^{\perp_H}$ is given by $T^{\perp_H} = T_e^{\perp_H} \cup T_o^{\perp_H}$.*

Proof Using set operations, we have

$$\begin{aligned} T^{\perp_H} &= \mathbb{Z}_n \backslash T^{-q} \\ &= (\Omega_e \cup \Omega_o) \backslash (T_e^{-q} \cup T_o^{-q}) \\ &= (\Omega_e \backslash T_e^{-q}) \cup (\Omega_o \backslash T_o^{-q}) \\ &= T_e^{\perp_H} \cup T_o^{\perp_H}. \end{aligned}$$

The result follows. □

In the light of Lemmas 3.1 and 3.2, we can provide an expression for determining the value of rank$(HH^{\dagger})$, which will be helpful for computing the number of maximally entangled states.

Theorem 3.3 *Let $\mathcal{C}$ be a cyclic code over $\mathbb{F}_{q^2}$ of length n with defining set $T = T_e \cup T_o$ and parity check matrix H. Then* rank$(HH^{\dagger}) = |T_e \cap T_e^{-q}| + |T_o \cap T_o^{-q}|$.

Proof By Lemma 3.1, $Hull_H(\mathcal{C})$ has defining set

$$\begin{aligned} T_H &= (T_e \cup T_o) \cup (T_e^{\perp_H} \cup T_o^{\perp_H}) \\ &= (T_e \cup T_e^{\perp_H}) \cup (T_o \cup T_o^{\perp_H}). \end{aligned}$$

Hence,

$$\begin{aligned} \dim(Hull_H(\mathcal{C})) &= n - |T_H| = n - |T_e \cup T_e^{\perp_H}| - |T_o \cup T_o^{\perp_H}| \\ &= n - \left(|T_e| + |T_e^{\perp_H}| - |T_e \cap T_e^{\perp_H}|\right) - \left(|T_o| + |T_o^{\perp_H}| - |T_o \cap T_o^{\perp_H}|\right) \\ &= |T_e \cap T_e^{\perp_H}| + |T_o \cap T_o^{\perp_H}| \\ &= |T_e| + |T_o| - |T_e \cap T_e^{-q}| - |T_o \cap T_o^{-q}|. \end{aligned}$$

From (2),

$$\begin{aligned} c &= \text{rank}(HH^{\dagger}) \\ &= |T_e| + |T_o| - \dim(Hull_H(\mathcal{C})) \\ &= |T_e \cap T_e^{-q}| + |T_o \cap T_o^{-q}|. \end{aligned}$$

The result follows. □

Combining Theorem 2.2 with Theorem 3.3, we can immediately obtain the following result.

Corollary 3.4 *Let $\mathcal{C}$ be a cyclic code over $\mathbb{F}_{q^2}$ of length n with defining set $T = T_e \cup T_o$. Then there exists an $[[n, 2k - n + c, d; c]]_q$ EAQEC code, where*

$$c = |T_e \cap T_e^{-q}| + |T_o \cap T_o^{-q}|. \tag{3}$$

From Corollary 3.4, we see that the parameter c of an EAQEC cyclic code with even length can be calculated by the formula $|T_e \cap T_e^{-q}| + |T_o \cap T_o^{-q}|$. Notice that $T_e \cap T_e^{-q} \subseteq \Omega_e$, $T_o \cap T_o^{-q} \subseteq \Omega_o$ and $\Omega_e \cap \Omega_o = \emptyset$. So, we can analyze the cyclotomic cosets in the sets Ω_e and Ω_o independently. Compared with the known formula $|T \cap T^{-q}|$ [26, 28], the parameter c is more easily determined by (3) along the odd and even lines.

4 Construction of EAQMDS codes from cyclic codes

Let $n = \frac{q^2-1}{r}$, where q is an odd prime power and r is an odd divisor of $q+1$. In this section, we are going to use cyclic codes over $\mathbb{F}_{q^2}$ of length n to construct EAQMDS codes. Let $m = \frac{n}{2}$. Notice that m is even.

Lemma 4.1 *Let $n = \frac{q^2-1}{r}$ with odd $r \mid (q+1)$, and $a = \frac{q+1}{r}$. Then*

1) *C_{2k} is a skew symmetric coset if and only if $k = \frac{\ell(q-1)}{2}$, for $0 \leq \ell \leq a-1$.*
2) *For $2k+1 \in \Omega_o$, C_{2k+1} is a skew asymmetric coset.*

Proof 1) C_{2k} is a skew symmetric coset if and only if $C_{2k} = -qC_{2k}$, if and only if $2k + q \cdot 2k \equiv 0 (\text{mod } n)$, i.e., $(q+1)k \equiv 0(\text{mod } m)$. Hence, $m \mid (q+1)k$, which means $(q-1) \mid 2kr$. Notice that $\gcd(q-1, r) = 1$. This is equivalent to $(q-1) \mid 2k$. Therefore, $k = \frac{\ell(q-1)}{2}$, for $0 \leq \ell \leq a-1$.

2) Suppose that $C_{2k+1} = -qC_{2k+1}$. Then $(2k+1) + q(2k+1) \equiv 0(\text{mod } n)$. This implies $(q-1) \mid (2k+1)r$, which means $(q-1) \mid (2k+1)$. This is impossible since $q-1$ is even and $2k+1$ is odd. Hence, C_{2k+1} is a skew asymmetric coset. □

Lemma 4.2 *Let $n = \frac{q^2-1}{r}$ with odd $r \mid (q+1)$. If $1 \leq k_1, k_2 \leq \frac{q-3}{2}$ and $k_1 \neq k_2$, then $C_{2k_1} \neq -qC_{2k_2}$.*

Proof Suppose there exist two integers k_1, k_2 with $1 \leq k_1, k_2 \leq \frac{q-3}{2}$ such that $C_{2k_1} = -qC_{2k_2}$. Observe that, if $C_{2k_1} \neq -qC_{2k_2}$, then $C_{2k_2} \neq -qC_{2k_1}$ since $q^2 \equiv 1(\text{mod } n)$. So, we can assume $k_1 < k_2$. Hence,

$$2qk_1 + 2k_2 \equiv 0(\text{mod } 2m), \tag{4}$$

where $2 < k_1 + k_2 < q-3$. (4) is equivalent to

$$qk_1 + k_2 \equiv 0(\text{mod } m).$$

So, $qk_1 + k_2 = ms$, for some integer s. This gives

$$(q-1)\left[\frac{(q+1)s}{2r} - k_1\right] = k_1 + k_2,$$

which implies that $(q-1) \mid (k_1 + k_2)$. This produces a contradiction. □

Lemma 4.3 *Let $n = \frac{q^2-1}{r}$ with odd $r \mid (q+1)$. For any $k_1, k_2 \in \mathbb{Z}_m$, if $C_{2k_1+1} = -qC_{2k_2+1}$, then $k_1 + k_2 + 1 \equiv 0(\text{mod } \frac{q-1}{2})$.*

Proof We can assume $k_1 < k_2$. It can be seen that $C_{2k_1+1} = -qC_{2k_2+1}$ if and only if

$$2qk_1 + 2k_2 + q + 1 \equiv 0(\text{mod } n),$$

which is equivalent to

$$qk_1 + k_2 + \frac{q+1}{2} \equiv 0(\text{mod } m). \tag{5}$$

By taking both sides of (5) modulo $\frac{q-1}{2}$, we obtain $k_1 + k_2 + 1 \equiv 0(\text{mod } \frac{q-1}{2})$. The result follows. □

Lemma 4.4 *Let $n = \frac{q^2-1}{r}$ with odd $r \mid (q+1)$. If $0 \le k_1, k_2 \le \frac{q-3}{2}$, then $C_{2k_1+1} = -qC_{2k_2+1}$ if and only if $k_1 + k_2 = \frac{q-3}{2}$.*

Proof We can assume $k_1 < k_2$. It can be seen that $C_{2k_1+1} = -qC_{2k_2+1}$ if and only if

$$2qk_1 + 2k_2 + q + 1 \equiv 0(\text{mod } n),$$

which is equivalent to

$$qk_1 + k_2 + \frac{q+1}{2} \equiv 0(\text{mod } m). \tag{6}$$

By taking both sides of (6) modulo $\frac{q-1}{2}$, we obtain $k_1 + k_2 + 1 \equiv 0(\text{ mod } \frac{q-1}{2})$. Since $k_1 < k_2$ and $1 < k_1 + k_2 + 1 < q - 2$, it follows that $k_1 + k_2 = \frac{q-3}{2}$. The result follows. □

Based on the lemmas given above, we next explore the cases when $r = 3, 5$ and 7 respectively, and construct some classes of EAQMDS codes with larger minimum distance than the codes available in the literature.

4.1 Length $n = \frac{q^2-1}{3}$ with $3 \mid (q+1)$

Assume that $q \ge 11$ is an odd prime power. Let $r = 3$ and $3 \mid (q+1)$. Then $n = \frac{q^2-1}{3}$ and $m = \frac{n}{2}$. Now, we are going to find skew asymmetric pairs $(C_{\delta_1}, C_{\delta_2})$ with $1 \le \delta_2 < \delta_1 \le \frac{8q-10}{3}$. For cyclotomic cosets C_{2k} in Ω_e, by Lemma 4.2, we only need to consider the case when $k \ge \frac{q+1}{2}$.

Lemma 4.5 *Let $n = \frac{q^2-1}{3}$ with $3 \mid (q+1)$. Let k_1 and k_2 be integers with $\frac{q+1}{2} \le k_1 \le \frac{4q-8}{3}$ and $1 \le k_2 < k_1$. The pairs $(2k_1, 2k_2)$ such that $C_{2k_2} = -qC_{2k_1}$ are given by $(\frac{4q-2}{3}, \frac{2q-4}{3})$, $(\frac{5q-1}{3}, \frac{q-5}{3})$ and $(\frac{7q-5}{3}, \frac{5q-7}{3})$.*

Proof If $C_{2k_2} = -qC_{2k_1}$, then

$$k_1 q + k_2 \equiv 0(\text{mod } m). \tag{7}$$

Note that $(q-1) \mid m$. Taking both sides of (7) modulo $q-1$, we have $k_1 + k_2 \equiv 0(\text{mod } q-1)$. Since $\frac{q+3}{2} \le k_1 + k_2 < \frac{8q-16}{3}$, it follows that $k_1 + k_2 = q - 1$ or $2(q-1)$.

1) $k_1 + k_2 = q - 1$. Then $k_2 = q - 1 - k_1$. Putting it into (7) one obtains $k_1 + 1 \equiv 0(\text{mod } \frac{q+1}{6})$. Note that $\frac{q+1}{2} \le k_1 \le q - 2$, so $k_1 = \frac{2q-1}{3}$ or $\frac{5q-1}{6}$. Hence, $(2k_1, 2k_2) = (\frac{4q-2}{3}, \frac{2q-4}{3})$ or $(\frac{5q-1}{3}, \frac{q-5}{3})$.

2) $k_1 + k_2 = 2(q-1)$. Then $k_2 = 2(q-1) - k_1$. Putting it into (7) one obtains $k_1 + 2 \equiv 0(\mathrm{mod}\ \frac{q+1}{6})$. Note that $q-1 < k_1 \leq \frac{4q-8}{3}$, so $k_1 = \frac{7q-5}{6}$. Hence, $(2k_1, 2k_2) = (\frac{7q-5}{3}, \frac{5q-7}{3})$.

This completes the proof. □

Lemma 4.6 *Let $n = \frac{q^2-1}{3}$ with $3 \mid (q+1)$. Let k_1 and k_2 be integers with $0 \leq k_1 \leq \frac{4q-8}{3}$ and $1 \leq k_2 < k_1$. The pairs $(2k_1+1, 2k_2+1)$ such that $C_{2k_2+1} = -qC_{2k_1+1}$ are given by $(\frac{2q-1}{3}, \frac{q-2}{3})$, $(\frac{5q-4}{3}, \frac{4q-5}{3})$, $(2q-1, q-2)$ and $(\frac{7q-2}{3}, \frac{2q-7}{3})$.*

Proof From $C_{2k_2+1} = -qC_{2k_1+1}$, we can get

$$qk_1 + k_2 + \frac{q+1}{2} \equiv 0(\mathrm{mod}\ m). \tag{8}$$

By Lemma 4.3, $k_1 + k_2 + 1 \equiv 0(\mathrm{mod}\ \frac{q-1}{2})$. Since $1 \leq k_1 + k_2 + 1 < \frac{8q-13}{3}$, it follows that $k_1 + k_2 + 1 = t \cdot \frac{q-1}{2}$, for $1 \leq t \leq 5$. Notice that $k_1 + k_2 < 2k_1$ and $k_2 \geq 1$.

1) When $t = 1$, $\frac{q-3}{4} < k_1 \leq \frac{q-5}{2}$ and $k_2 = \frac{q-1}{2} - k_1 - 1$. From (8), we obtain $k_1 + 1 \equiv 0(\mathrm{mod}\ \frac{q+1}{6})$. This gives $k_1 = \frac{q-2}{3}$. Hence, $(2k_1+1, 2k_2+1) = (\frac{2q-1}{3}, \frac{q-2}{3})$.
2) When $t = 2$, $\frac{q-1}{2} < k_1 \leq q-3$ and $k_2 = q - k_1 - 2$. From (8), we obtain $k_1 + \frac{3}{2} \equiv 0(\ \mathrm{mod}\ \frac{q+1}{6})$, which has no solutions. Hence, such pairs $(2k_1+1, 2k_2+1)$ do not exist.
3) When $t = 3$, $\frac{3q-5}{4} < k_1 \leq \frac{3q-7}{2}$ and $k_2 = \frac{3(q-1)}{2} - k_1 - 1$. From (8), we obtain $k_1 + 2 \equiv 0(\mathrm{mod}\ \frac{q+1}{6})$. This gives $k_1 = \frac{5q-7}{6}$, $q-1$ or $\frac{7q-5}{6}$. Hence, $(2k_1+1, 2k_2+1) = (\frac{5q-4}{3}, \frac{4q-5}{3})$, $(2q-1, q-2)$ or $(\frac{7q-2}{3}, \frac{2q-7}{3})$.
4) When $t = 4$ or 5, as in Case 2), we can get the pairs $(2k_1+1, 2k_2+1)$ such that $C_{2k_2+1} = -qC_{2k_1+1}$ do not exist.

This completes the proof. □

Let $\mathcal{C}$ be a cyclic code over $\mathbb{F}_{q^2}$ of length n with defining set $T = T_e \cup T_o = \cup_{i=1}^{\delta} C_i$, where $1 \leq \delta \leq \frac{8q-10}{3}$. We use the cyclic codes $\mathcal{C}$ to construct EAQMDS codes with flexible parameters.

Theorem 4.7 *Let $n = \frac{q^2-1}{3}$ with $3 \mid (q+1)$. There exist q-ary EAQMDS codes with parameters*

1) $[[n, n-2d+5, d; 3]]_q$, where $q \leq d \leq \frac{4q-2}{3}$ $(q \geq 11)$.
2) $[[n, n-2d+7, d; 5]]_q$, where $\frac{4q+1}{3} \leq d \leq \frac{5q-4}{3}$ $(q \geq 11)$.
3) $[[n, n-2d+11, d; 9]]_q$, where $\frac{5q+2}{3} \leq d \leq 2q-2$ $(q \geq 11)$.
4) $[[n, n-2d+14, d; 12]]_q$, where $2q \leq d \leq \frac{7q-5}{3}$ $(q \geq 17)$.
5) $[[n, n-2d+18, d; 16]]_q$, where $\frac{7q+1}{3} \leq d \leq \frac{8q-7}{3}$ $(q \geq 17)$.

Proof Let $\mathcal{C}$ be defined as above. We know that $\mathcal{C}$ is an $[n, n-\delta, \delta+1]$ MDS code over $\mathbb{F}_{q^2}$.

1) If $q-1 \le \delta \le \frac{4q-5}{3}$, then $\{\frac{2q-1}{3}, \frac{q-2}{3}, q-1\} \subseteq T$. By Lemma 4.1 1) and Lemma 4.2, $T_e \cap T_e^{-q} = \{q-1\}$. By Lemma 4.1 2) and Lemma 4.6, $T_o \cap T_o^{-q} = \{\frac{2q-1}{3}, \frac{q-2}{3}\}$. By Theorem 3.3, $c = |T_e \cap T_e^{-q}| + |T_o \cap T_o^{-q}| = 3$. Applying Corollary 3.4 to $\mathcal{C}$ one obtains an $[[n, n-2\delta+3, \delta+1; 3]]_q$ EAQEC code. It can be checked that the parameters meet the Singleton-type bound (1), and hence $\mathcal{C}$ is an EAQMDS code. This produces the first class of codes.
2) If $\frac{4q-2}{3} \le \delta \le \frac{5q-7}{3}$, then $\{\frac{2q-1}{3}, \frac{q-2}{3}, q-1, \frac{4q-2}{3}, \frac{2q-4}{3}\} \subseteq T$. It can be seen that $T_e \cap T_e^{-q} = \{q-1, \frac{4q-2}{3}, \frac{2q-4}{3}\}$ and $T_o \cap T_o^{-q} = \{\frac{2q-1}{3}, \frac{q-2}{3}\}$. So, $c = |T_e \cap T_e^{-q}| + |T_o \cap T_o^{-q}| = 5$. This produces an $[[n, n-2\delta+5, \delta+1; 5]]_q$ EAQMDS code, which gives the second class of codes.
3) If $\frac{5q-1}{3} \le \delta \le 2q-3$, then $\{\frac{2q-1}{3}, \frac{q-2}{3}, q-1, \frac{4q-2}{3}, \frac{2q-4}{3}, \frac{5q-4}{3}, \frac{4q-5}{3}, \frac{5q-1}{3}, \frac{q-5}{3}\} \subseteq T$. We have $T_e \cap T_e^{-q} = \{q-1, \frac{4q-2}{3}, \frac{2q-4}{3}, \frac{5q-1}{3}, \frac{q-5}{3}\}$ and $T_o \cap T_o^{-q} = \{\frac{2q-1}{3}, \frac{q-2}{3}, \frac{5q-4}{3}, \frac{4q-5}{3}\}$. So, $c = 9$. This produces an $[[n, n-2\delta+9, \delta+1; 9]]_q$ EAQMDS code. This gives the third class of codes.
4) If $2q-1 \le \delta \le \frac{7q-8}{3}$, then $T_e \cap T_e^{-q} = \{q-1, \frac{4q-2}{3}, \frac{2q-4}{3}, \frac{5q-1}{3}, \frac{q-5}{3}, 2q-2\}$ and $T_o \cap T_o^{-q} = \{\frac{2q-1}{3}, \frac{q-2}{3}, \frac{5q-4}{3}, \frac{4q-5}{3}, 2q-1, q-2\}$. So, $c = 12$. Hence, we get an $[[n, n-2\delta+12, \delta+1; 12]]_q$ EAQMDS code. This gives the fourth class of codes.
5) If $\frac{7q-2}{3} \le \delta \le \frac{8q-10}{3}$, then $T_e \cap T_e^{-q} = \{q-1, \frac{4q-2}{3}, \frac{2q-4}{3}, 2q-2, \frac{5q-1}{3}, \frac{q-5}{3}, \frac{7q-5}{3}, \frac{5q-7}{3}\}$ and $T_o \cap T_o^{-q} = \{\frac{2q-1}{3}, \frac{q-2}{3}, \frac{5q-4}{3}, \frac{4q-5}{3}, 2q-1, q-2, \frac{7q-2}{3}, \frac{2q-7}{3}\}$. So, $c = 16$. Hence, we have an $[[n, n-2\delta+16, \delta+1; 16]]_q$ EAQMDS code. This gives the last class of codes. □

4.2 Length $n = \frac{q^2-1}{5}$ with $5 \mid (q+1)$

Assume that $q \ge 19$ is an odd prime power with $5 \mid (q+1)$. Let $n = \frac{q^2-1}{5}$ and $m = \frac{n}{2}$.

Lemma 4.8 *Let $n = \frac{q^2-1}{5}$ with $5 \mid (q+1)$. Let k_1, k_2 be integers with $\frac{q+1}{2} \le k_1 \le \frac{9q-16}{10}$ and $1 \le k_2 < k_1$. The pairs $(2k_1, 2k_2)$ with $C_{2k_2} = -qC_{2k_1}$ are given by $(\frac{6q-4}{5}, \frac{4q-6}{5})$, $(\frac{7q-3}{5}, \frac{3q-7}{5})$ and $(\frac{8q-2}{5}, \frac{2q-8}{5})$.*

Proof If $C_{2k_2} = -qC_{2k_1}$, then

$$k_1 q + k_2 \equiv 0 (\mathrm{mod}\ m). \tag{9}$$

Taking both sides of (9) modulo $q-1$, we have $k_1 + k_2 \equiv 0(\mathrm{mod}\ q-1)$. Since $\frac{q+3}{2} \le k_1 + k_2 < \frac{9q-16}{5}$, it follows that $k_1 + k_2 = q-1$ and $k_2 = q-1-k_1$. Putting it into (9) one obtains $k_1 + 1 \equiv 0(\mathrm{mod}\ \frac{q+1}{10})$. Note that $\frac{q+1}{2} \leq k_1 \leq q - 2$. So, we can get $(2k_1, 2k_2) = (\frac{6q-4}{5}, \frac{4q-6}{5}), (\frac{7q-3}{5}, \frac{3q-7}{5})$ or $(\frac{8q-2}{5}, \frac{2q-8}{5})$. □

Lemma 4.9 *Let $n = \frac{q^2-1}{5}$ with $5 \mid (q+1)$. Let k_1, k_2 be integers with $0 \leq k_1 \leq \frac{9q-16}{10}$ and $1 \leq k_2 < k_1$. The pairs $(2k_1 + 1, 2k_2 + 1)$ such that $C_{2k_2+1} = -qC_{2k_1+1}$ are given by $(2k_1 + 1, 2k_2 + 1) = (\frac{3q-2}{5}, \frac{2q-3}{5})$, $(\frac{4q-1}{5}, \frac{q-4}{5})$ and $(\frac{8q-7}{5}, \frac{7q-8}{5})$.*

Proof As in the proof of Lemma 4.6, we have

$$qk_1 + k_2 + \frac{q+1}{2} \equiv 0(\mathrm{mod}\ m)$$

and

$$k_1 + k_2 + 1 \equiv 0(\mathrm{mod}\ \frac{q-1}{2}). \tag{10}$$

Since $1 \leq k_1 + k_2 + 1 < \frac{9q-11}{5}$, it follows from (10) that $k_1 + k_2 = \frac{q-3}{2}$, $q - 2$ or $\frac{3q-5}{2}$. Notice that $k_1 + k_2 < 2k_1$. Then we can get

$$(2k_1 + 1, 2k_2 + 1) = \left(\frac{3q-2}{5}, \frac{2q-3}{5}\right), \left(\frac{4q-1}{5}, \frac{q-4}{5}\right) \text{ or } \left(\frac{8q-7}{5}, \frac{7q-8}{5}\right).$$

This gives the result. □

By using Lemmas 4.8 and 4.9, we can construct EAQMDS codes of length $n = \frac{q^2-1}{5}$.

Theorem 4.10 *Let $n = \frac{q^2-1}{5}$ with $5 \mid (q+1)$. There exist q-ary EAQMDS codes with parameters*

1) $[[n, n - 2d + 7, d; 5]]_q$, *where* $q \leq d \leq \frac{6q-4}{5}$.
2) $[[n, n - 2d + 9, d; 7]]_q$, *where* $\frac{6q+1}{5} \leq d \leq \frac{7q-3}{5}$.
3) $[[n, n - 2d + 11, d; 9]]_q$, *where* $\frac{7q+2}{5} \leq d \leq \frac{8q-7}{5}$.
4) $[[n, n - 2d + 15, d; 13]]_q$, *where* $\frac{8q+3}{5} \leq d \leq \frac{9q-6}{5}$.

Proof Let $\mathcal{C}$ be a cyclic code over $\mathbb{F}_{q^2}$ of length n with defining set $T = T_e \cup T_o = \cup_{i=1}^{\delta} C_i$, where $1 \leq \delta \leq \frac{9q-11}{5}$. Then $\mathcal{C}$ is an $[n, n - \delta, \delta + 1]$ MDS code over $\mathbb{F}_{q^2}$.

1) If $q - 1 \leq \delta \leq \frac{6q-9}{5}$, then $T_e \cap T_e^{-q} = \{q - 1\}$ and $T_o \cap T_o^{-q} = \{\frac{3q-2}{5}, \frac{2q-3}{5}, \frac{4q-1}{5}, \frac{q-4}{5}\}$. So, $c = 5$. By applying Corollary 3.4, we obtain an $[[n, n - 2\delta + 5, \delta + 1; 5]]_q$ EAQMDS code, which is the first class of codes.

2) If $\frac{6q-4}{5} \leq \delta \leq \frac{7q-8}{5}$, then $T_e \cap T_e^{-q} = \{q - 1, \frac{6q-4}{5}, \frac{4q-6}{5}\}$ and $T_o \cap T_o^{-q} = \{\frac{3q-2}{5}, \frac{2q-3}{5}, \frac{4q-1}{5}, \frac{q-4}{5}\}$. So, $c = 7$. Hence, we obtain an $[[n, n-2\delta+7, \delta+1; 7]]_q$ EAQMDS code, which is the second class of codes.

3) If $\frac{7q-3}{5} \leq \delta \leq \frac{8q-12}{5}$, then $T_e \cap T_e^{-q} = \{q-1, \frac{6q-4}{5}, \frac{4q-6}{5}, \frac{7q-3}{5}, \frac{3q-7}{5}\}$ and $T_o \cap T_o^{-q} = \{\frac{3q-2}{5}, \frac{2q-3}{5}, \frac{4q-1}{5}, \frac{q-4}{5}\}$. So, $c = 9$. Hence, we obtain an $[[n, n-2\delta+9, \delta+1; 9]]_q$ EAQMDS code, which gives the third class of codes.
4) If $\frac{8q-2}{5} \leq \delta \leq \frac{9q-11}{5}$, then $T_e \cap T_e^{-q} = \{q-1, \frac{6q-4}{5}, \frac{4q-6}{5}, \frac{7q-3}{5}, \frac{3q-7}{5}, \frac{8q-2}{5}, \frac{2q-8}{5}\}$ and $T_o \cap T_o^{-q} = \{\frac{3q-2}{5}, \frac{2q-3}{5}, \frac{4q-1}{5}, \frac{q-4}{5}, \frac{8q-7}{5}, \frac{7q-8}{5}\}$. So, $c = 13$. Hence, we obtain an $[[n, n-2\delta+13, \delta+1; 13]]_q$ EAQMDS code, which gives the last class of codes. □

4.3 Length $n = \frac{q^2-1}{7}$ with $7 \mid (q+1)$

Assume that $q \geq 27$ is an odd prime power with $7 \mid (q+1)$. Let $n = \frac{q^2-1}{7}$ and $m = \frac{n}{2}$.

Lemma 4.11 *Let $n = \frac{q^2-1}{7}$ with $7 \mid (q+1)$. Let k_1, k_2 be integers with $\frac{q+1}{2} \leq k_1 \leq \frac{11q-24}{14}$ and $1 \leq k_2 < k_1$. The pairs $(2k_1, 2k_2)$ with $C_{2k_2} = -qC_{2k_1}$ are given by $(\frac{8q-6}{7}, \frac{6q-8}{7})$, $(\frac{9q-5}{7}, \frac{5q-9}{7})$ and $(\frac{10q-4}{7}, \frac{4q-10}{7})$.*

Proof If $C_{2k_2} = -qC_{2k_1}$, then

$$k_1 q + k_2 \equiv 0 (\text{mod } m). \tag{11}$$

Taking both sides of (11) modulo $q-1$, we have $k_1 + k_2 \equiv 0 (\text{mod } q-1)$. Since $\frac{q+3}{2} \leq k_1 + k_2 < \frac{11q-24}{7}$, it follows that $k_1 + k_2 = q-1$ and $k_2 = q-1-k_1$. Putting it into (11) one obtains $k_1 + 1 \equiv 0 (\text{mod } \frac{q+1}{14})$. Note that $\frac{q+1}{2} \leq k_1 \leq q-2$. So, we can get $(2k_1, 2k_2) = (\frac{8q-6}{7}, \frac{6q-8}{7})$, $(\frac{9q-5}{7}, \frac{5q-9}{7})$ or $(\frac{10q-4}{7}, \frac{4q-10}{7})$. □

Lemma 4.12 *Let $n = \frac{q^2-1}{7}$ with $7 \mid (q+1)$. Let k_1, k_2 be integers with $0 \leq k_1 \leq \frac{11q-24}{14}$ and $1 \leq k_2 < k_1$. The pairs $(2k_1+1, 2k_2+1)$ such that $C_{2k_2+1} = -qC_{2k_1+1}$ are given by $(2k_1+1, 2k_2+1) = (\frac{4q-3}{7}, \frac{3q-4}{7})$, $(\frac{5q-2}{7}, \frac{2q-5}{7})$ and $(\frac{6q-1}{7}, \frac{q-6}{7})$.*

Proof As in the proof of Lemma 4.6, since $1 \leq k_1 + k_2 + 1 < \frac{11q-17}{7}$, it follows that $k_1 + k_2 = \frac{q-3}{2}$ or $q-2$. Notice that $k_1 + k_2 < 2k_1$. Then we can get $(2k_1+1, 2k_2+1) = (\frac{4q-3}{7}, \frac{3q-4}{7})$, $(\frac{5q-2}{7}, \frac{2q-5}{7})$ or $(\frac{6q-1}{7}, \frac{q-6}{7})$. □

By using Lemmas 4.11 and 4.12, we can find the following EAQMDS codes of length $n = \frac{q^2-1}{7}$.

Theorem 4.13 *Let $n = \frac{q^2-1}{7}$ with $7 \mid (q+1)$. There exist q-ary EAQMDS codes with parameters*

1) $[[n, n-2d+9, d; 7]]_q$, *where* $q \leq d \leq \frac{8q-6}{7}$.
2) $[[n, n-2d+11, d; 9]]_q$, *where* $\frac{8q+1}{7} \leq d \leq \frac{9q-5}{7}$.
3) $[[n, n-2d+13, d; 11]]_q$, *where* $\frac{9q+2}{7} \leq d \leq \frac{10q-4}{7}$.

4) $[[n, n-2d+15, d; 13]]_q$, *where* $\frac{10q+3}{7} \leq d \leq \frac{11q-10}{7}$.

Proof Let $\mathcal{C}$ be a cyclic code over $\mathbb{F}_{q^2}$ of length n with defining set $T = T_e \cup T_o = \cup_{i=1}^{\delta} C_i$, where $1 \leq \delta \leq \frac{11q-17}{7}$. Then $\mathcal{C}$ is an $[n, n-\delta, \delta+1]$ MDS code over $\mathbb{F}_{q^2}$.

1) If $q-1 \leq \delta \leq \frac{8q-13}{7}$, then $T_e \cap T_e^{-q} = \{q-1\}$ and $T_o \cap T_o^{-q} = \{\frac{4q-3}{7}, \frac{3q-4}{7}, \frac{5q-2}{7}, \frac{2q-5}{7}, \frac{6q-1}{7}, \frac{q-6}{7}\}$. So, $c = 7$. By applying Corollary 3.4, we obtain an $[[n, n-2\delta+7, \delta+1; 7]]_q$ EAQMDS code, which is the first class of codes.

2) If $\frac{8q-6}{7} \leq \delta \leq \frac{9q-12}{7}$, then $T_e \cap T_e^{-q} = \{q-1, \frac{8q-6}{7}, \frac{6q-8}{7}\}$ and $T_o \cap T_o^{-q} = \{\frac{4q-3}{7}, \frac{3q-4}{7}, \frac{5q-2}{7}, \frac{2q-5}{7}, \frac{6q-1}{7}, \frac{q-6}{7}\}$. So, $c = 9$. Hence, we obtain an $[[n, n-2\delta+9, \delta+1; 9]]_q$ EAQMDS code, which is the second class of codes.

3) If $\frac{9q-5}{7} \leq \delta \leq \frac{10q-11}{7}$, then $T_e \cap T_e^{-q} = \{q-1, \frac{8q-6}{7}, \frac{6q-8}{7}, \frac{9q-5}{7}, \frac{5q-9}{7}\}$ and $T_o \cap T_o^{-q} = \{\frac{4q-3}{7}, \frac{3q-4}{7}, \frac{5q-2}{7}, \frac{2q-5}{7}, \frac{6q-1}{7}, \frac{q-6}{7}\}$. So, $c = 11$. Hence, we obtain an $[[n, n-2\delta+11, \delta+1; 11]]_q$ EAQMDS code, which gives the third class of codes.

4) If $\frac{10q-4}{7} \leq \delta \leq \frac{11q-17}{7}$, then $T_e \cap T_e^{-q} = \{q-1, \frac{8q-6}{7}, \frac{6q-8}{7}, \frac{9q-5}{7}, \frac{5q-9}{7}, \frac{10q-4}{7}, \frac{4q-10}{7}\}$ and $T_o \cap T_o^{-q} = \{\frac{4q-3}{7}, \frac{3q-4}{7}, \frac{5q-2}{7}, \frac{2q-5}{7}, \frac{6q-1}{7}, \frac{q-6}{7}\}$. So, $c = 13$. Hence, we obtain an $[[n, n-2\delta+13, \delta+1; 13]]_q$ EAQMDS code, which gives the last class of codes. □

5 Comparisons and conclusions

In this paper, we have constructed EAQMDS codes with length $n = \frac{q^2-1}{r}$, where $r \mid (q+1)$ and $r = 3, 5, 7$. Through separating the defining set into the sets of even integer numbers and odd integer numbers, we have determined the number of maximally entangled states. Our construction has produced many new EAQMDS codes with large minimum distance. In [8, 23, 43], some standard quantum MDS codes with the same length have been obtained, and they have minimum distance not more than $q+1$. Our EAQMDS codes presented in this paper have minimum distance upper limit greater than $\frac{3(q+1)}{2}$. In particular, when $r = 3$, we obtain the EAQMDS codes with minimum distance upper limit greater than $2(q+1)$. We now compare our EAQMDS codes with the known ones in the literature.

In [10], Fan et al. constructed EAQMDS codes with parameters $[[\frac{q^2-1}{r}, \frac{q^2-1}{r} - 2d + r + 2, d; r]]_q$, where $r \mid (q+1)$ and $\frac{(r-1)(q+1)}{r} + 2 \leq d \leq \frac{(r+1)(q+1)}{r} - 2$. It is obvious that $\frac{3(q+1)}{2} > \frac{(r+1)(q+1)}{r} - 2$, hence our construction produces more codes processing bigger minimum distance.

In [40], Pang et al. obtained EAQMDS codes with parameters $[[\frac{q^2-1}{r}, \frac{q^2-1}{r} - 2d + 2m + 1, d; 2m-1]]_q$, where $r \mid (q+1)$, $1 \leq m \leq \frac{r-1}{2}$ and $\frac{(r+2m-1)(q+1)}{2r} \leq$

Table 1 EAQMDS codes of length $n = \frac{q^2-1}{3}$ with $3 \mid (q+1)$

$[[n, k, d; c]]_q$	d	d in [30]
$[[\frac{q^2-1}{3}, \frac{q^2-1}{3} - 2d + 5, d; 3]]_q (q \geq 11)$	$q \leq d \leq \frac{4q-2}{3}$	$q + 1 \leq d \leq \frac{4q-2}{3}$
$[[\frac{q^2-1}{3}, \frac{q^2-1}{3} - 2d + 7, d; 5]]_q (q \geq 11)$	$\frac{4q+1}{3} \leq d \leq \frac{5q-4}{3}$	$--$
$[[\frac{q^2-1}{3}, \frac{q^2-1}{3} - 2d + 11, d; 9]]_q (q \geq 11)$	$\frac{5q+2}{3} \leq d \leq 2q - 2$	$--$
$[[\frac{q^2-1}{3}, \frac{q^2-1}{3} - 2d + 14, d; 12]]_q (q \geq 17)$	$2q \leq d \leq \frac{7q-5}{3}$	$--$
$[[\frac{q^2-1}{3}, \frac{q^2-1}{3} - 2d + 18, d; 16]]_q (q \geq 17)$	$\frac{7q+1}{3} \leq d \leq \frac{8q-7}{3}$	$--$

Table 2 EAQMDS codes of length $n = \frac{q^2-1}{5}$ with $5 \mid (q+1)$

$[[n, k, d; c]]_q$	d	d in [30]
$[[\frac{q^2-1}{5}, \frac{q^2-1}{5} - 2d + 7, d; 5]]_q$	$q \leq d \leq \frac{6q-4}{5}$	$q + 1 \leq d \leq \frac{6q+1}{5}$
$[[\frac{q^2-1}{5}, \frac{q^2-1}{5} - 2d + 9, d; 7]]_q$	$\frac{6q+1}{5} \leq d \leq \frac{7q-3}{5}$	$--$
$[[\frac{q^2-1}{5}, \frac{q^2-1}{5} - 2d + 11, d; 9]]_q$	$\frac{7q+2}{5} \leq d \leq \frac{8q-7}{5}$	$--$
$[[\frac{q^2-1}{5}, \frac{q^2-1}{5} - 2d + 15, d; 13]]_q$	$\frac{8q+3}{5} \leq d \leq \frac{9q-6}{5}$	$--$

Table 3 EAQMDS codes of length $n = \frac{q^2-1}{7}$ with $7 \mid (q+1)$

$[[n, k, d; c]]_q$	d	d in [30]
$[[\frac{q^2-1}{7}, \frac{q^2-1}{7} - 2d + 9, d; 7]]_q$	$q \leq d \leq \frac{8q-6}{7}$	$q + 1 \leq d \leq \frac{8q+1}{7}$
$[[\frac{q^2-1}{7}, \frac{q^2-1}{7} - 2d + 11, d; 9]]_q$	$\frac{8q+1}{7} \leq d \leq \frac{9q-5}{7}$	$--$
$[[\frac{q^2-1}{7}, \frac{q^2-1}{7} - 2d + 13, d; 11]]_q$	$\frac{9q+2}{7} \leq d \leq \frac{10q-4}{7}$	$--$
$[[\frac{q^2-1}{7}, \frac{q^2-1}{7} - 2d + 15, d; 13]]_q$	$\frac{10q+3}{7} \leq d \leq \frac{11q-10}{7}$	$--$

$d \leq \frac{(q-1)r+(2m+1)(q+1)}{2r}$. It can be seen that these codes have minimum distance not more than q. Hence, our quantum codes have larger minimum distance and higher error-correcting capability.

In [30], by using constacyclic codes, Liu et al. constructed EAQMDS codes with minimum distance more than $q + 1$. We compare the parameters of our codes with those from [30] in Tables 1, 2 and 3. There for length $n = \frac{q^2-1}{r}$ $(r = 3, 5, 7)$, we show almost all the parameters constructed in [30] are covered by our construction based on cyclic codes. Furthermore, new classes of EQAMDS codes have been obtained, which have minimum distance with a wide range. As the minimum distance gets large, the required number of maximally entangled states becomes growing. However, the net rate $\frac{k-c}{n}$ remains unchanged. In Table 4, we make a comparison between our codes and the known ones in [30] for some special lengths. We find the number c of maximally entangled states changes with the values of r and d. However, it is not easy to describe the changeable rules among the three values. A further consideration is to present an explicit expression to reveal their relation.

Table 4 Some new EAQMDS codes and comparisons

q	r	Our parameters		Parameters in [30]
11	3	$[[40, 45-2d, d; 3]]_{11}$	$11 \le d \le 14$	$[[40, 45-2d, d; 3]]_{11}$ $12 \le d \le 14$
11	3	$[[40, 47-2d, d; 5]]_{11}$	$15 \le d \le 17$	New
11	3	$[[40, 51-2d, d; 9]]_{11}$	$19 \le d \le 20$	New
17	3	$[[96, 101-2d, d; 3]]_{17}$	$17 \le d \le 22$	$[[96, 101-2d, d; 3]]_{17}$ $18 \le d \le 22$
17	3	$[[96, 103-2d, d; 5]]_{17}$	$23 \le d \le 27$	New
17	3	$[[96, 107-2d, d; 9]]_{17}$	$29 \le d \le 32$	New
17	3	$[[96, 110-2d, d; 12]]_{17}$	$34 \le d \le 38$	New
17	3	$[[96, 114-2d, d; 16]]_{17}$	$40 \le d \le 43$	New
19	5	$[[72, 79-2d, d; 5]]_{19}$	$19 \le d \le 22$	$[[72, 79-2d, d; 5]]_{11}$ $20 \le d \le 23$
19	5	$[[72, 81-2d, d; 7]]_{19}$	$23 \le d \le 26$	New
19	5	$[[72, 83-2d, d; 9]]_{19}$	$27 \le d \le 29$	New
19	5	$[[72, 87-2d, d; 13]]_{19}$	$31 \le d \le 33$	New
23	3	$[[176, 181-2d, d; 3]]_{23}$	$23 \le d \le 30$	$[[176, 181-2d, d; 3]]_{23}$ $24 \le d \le 30$
23	3	$[[176, 183-2d, d; 5]]_{23}$	$31 \le d \le 37$	New
23	3	$[[176, 187-2d, d; 9]]_{23}$	$39 \le d \le 44$	New
23	3	$[[176, 190-2d, d; 12]]_{23}$	$46 \le d \le 52$	New
23	3	$[[176, 194-2d, d; 16]]_{23}$	$54 \le d \le 59$	New
27	7	$[[104, 113-2d, d; 7]]_{27}$	$27 \le d \le 30$	$[[104, 113-2d, d; 7]]_{11}$ $29 \le d \le 31$
27	7	$[[104, 115-2d, d; 9]]_{27}$	$31 \le d \le 34$	New
27	7	$[[104, 117-2d, d; 11]]_{27}$	$35 \le d \le 38$	New
27	7	$[[104, 119-2d, d; 13]]_{27}$	$39 \le d \le 41$	New
29	5	$[[168, 175-2d, d; 5]]_{29}$	$29 \le d \le 34$	$[[168, 175-2d, d; 5]]_{11}$ $30 \le d \le 35$
29	5	$[[168, 177-2d, d; 7]]_{29}$	$35 \le d \le 40$	New
29	5	$[[168, 179-2d, d; 9]]_{29}$	$41 \le d \le 45$	New
29	5	$[[168, 183-2d, d; 13]]_{29}$	$47 \le d \le 51$	New
41	7	$[[240, 249-2d, d; 7]]_{41}$	$41 \le d \le 46$	$[[240, 249-2d, d; 7]]_{41}$ $42 \le d \le 47$
41	7	$[[240, 251-2d, d; 9]]_{41}$	$47 \le d \le 52$	New
41	7	$[[240, 253-2d, d; 11]]_{41}$	$53 \le d \le 58$	New
41	7	$[[240, 255-2d, d; 13]]_{41}$	$59 \le d \le 63$	New

Our construction is based on classical cyclic codes over $\mathbb{F}_{q^2}$ with even length which enables us to deal with two classes of cyclotomic cosets independently. It requires the size of the finite field must be an odd prime power. Hence, the construction is generally invalid for the 2^{ℓ}-ary case. It is expected to provide a new method for finding new EAQMDS codes over finite fields with characteristic two. For a nonzero element $\lambda \in \mathbb{F}_{q^2}$, $x^n - \lambda$ probably factors as the product of two binomials $x^{n/2} - \lambda_1$ and $x^{n/2} - \lambda_2$ over a finite field. Hence, it is hopeful to construct new EAQMDS codes from certain types of constacyclic codes.

Acknowledgements We thank the anonymous referees for their valuable comments and suggestions that helped to improve greatly the quality of this paper. This research work is supported by the National Natural Science Foundation of China under Grant Nos. 61972126, U21A20428, 12171134, 61802102 and 12001002.

Data availability Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study

Declarations

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

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.

References

1. Ashikhmin, A.R., Knill, E.: Nonbinary quantum stablizer codes. IEEE Trans. Inf. Theory **47**, 3065–3072 (2001)
2. Allahmadi, A., AlKenani, A., Hijazi, R., Muthana, H., Özbudak, F., Solé, P.: New constructions of entanglement-assisted quantum codes. Cryptogr. Commun. **14**, 15–37 (2022)
3. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: On quantum and classical BCH codes. IEEE Trans. Inf. Theory **53**, 1183–1188 (2007)
4. Brun, T., Devetak, I., Hsieh, M.H.: Correcting quantum errors with entanglement. Science **314**, 436–439 (2006)
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. Chen, X., Zhu, S., Jing, W.: Cyclic codes and some new entanglement-assisted quantum MDS codes. Des. Codes Cryptogr. **89**, 2533–2551 (2021)
8. Chen, B., Ling, S., Zhang, G.: Applications of constacyclic codes of quantum MDS codes. IEEE Trans. Inf. Theory **61**, 1474–1484 (2015)
9. 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)
10. 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)
11. Fujiwara, Y., Clark, D., Vandendriessche, P., De Boeck, M., Tonchev, V.D.: Entanglement-assisted quantum low-density parity-check codes. Phys. Rev. A **82**, 042338 (2010)
12. 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)
13. Galindo, C., Hernando, F., Matsumoto, R., Ruano, D.: Entanglement-assisted quantum error-correcting codes from RS codes and BCH codes with extension degree 2. Quantum Inf. Process. **20**, 158 (2021)
14. Gedik, Z., Silva, I.A., Cakmak, B., Karpat, G., Vidoto, E.L.G., Soares-Pinto, D.O., deAzevedo, E.R., Fanchini, F.F.: Computational speed-up with a single qudit. Sci. Rep. **5**, 14671 (2015)
15. Grassl, M.: Entanglement-assisted quantum communication beating the quantum Singleton bound. Phys. Rev. A **103**, L020601 (2021)
16. Grassl, M., Geiselmann, W., Beth, T.: Quantum Reed-Solomon codes. In: Proceedings of AAECC-**13**, 231–244 (1999)
17. Grassl, M., Huber, F., Winter, A.: Entropic proofs of Singleton bounds for quantum error-correcting codes, arXiv:quant-ph/2010.07902v2 (2021-11-29)
18. Guenda, K., Jitman, S., Gulliver, T.A.: Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr. **86**, 121–136 (2018)

19. Guo, G., Li, R.: New entanglement-assisted quantum MDS codes derived from generalized Reed-Solomom codes. Int. J. Theor. Phys. **59**, 1241–1254 (2020)
20. Hsieh, M.H., Brun, T.A., Devetak, I.: Entanglement-assisted quantum quasi-cyclic low-density paritycheck codes. Phys. Rev. A **79**, 032340 (2009)
21. Hsieh, M.H., Devetak, I., Brun, T.: General entanglement-assisted quantum error-correcting codes. Phys. Rev. A **76**, 62313 (2007)
22. Hu, P., Liu, X.: Three classes of new EAQEC MDS codes. Quantum Inf. Process. **20**, 103 (2021)
23. Kai, X., Zhu, S., Li, P.: Constacyclic codes and some new quantum MDS codes. IEEE Trans. Inf. Theory **60**, 2080–2086 (2014)
24. Koroglu, M.E.: New entanglement-assisted MDS quantum codes from constacyclic codes. Quantum Inf. Process. **18**, 44 (2019)
25. Lai, C.Y., Brun, T.A.: Entanglement-assisted quantum error-correcting codes with imperfect ebits. Phys. Rev. A **86**, 032319 (2012)
26. Lai, C., Brun, T., Wilde, M.: Dualities and identities for entanglement-assisted quantum codes. Quantum Inf. Process. **13**, 957–990 (2014)
27. Lai, C., Ashikhmin, A.: Linear programming bounds for entanglement-assisted quantum error-correcting codes by split weight enumerators. IEEE Trans. Inf. Theory **64**, 622–639 (2018)
28. Lu, L., Li, R.: Entanglement-assisted quantum codes constructed from primitive quaternary BCH codes. Int. J. Quantum Inf. **12**, 1450015 (2014)
29. Liu, X., Yu, L., Hu, P.: New entanglement-assisted quantum codes from k-Galois dual codes. Finite Fields Appl. **55**, 21–32 (2019)
30. 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)
31. Li, R., Zuo, F., Liu, Y.: A study of skew symmetric q^2-cyclotomic coset and its applications. J. Air Force Eng. Univ. Nat. Sci. Ed. **12**, 87 (2011)
32. Lu, L., Li, R., Guo, L., Ma, Y., Liu, Y.: Entanglement-assisted quantum MDS codes from negacyclic codes. Quantum Inf. Process. **17**, 69 (2018)
33. 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)
34. Luo, G., Cao, X.: Two new families of entanglement-assisted quantum MDS codes from generalized Reed-Solomon codes. Quantum Inf. Process. **18**, 89 (2019)
35. Luo, G., Cao, X., Chen, X.: MDS codes with hulls of arbitrary dimensions and their quantum error correction. IEEE Trans. Inf. Theory **65**, 2944–2952 (2019)
36. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error Correcting Codes. North-Holland, Amsterdam (1977)
37. Mustafa, S., Emre, K.: An application of constacyclic codes to entanglement-assisted quantum MDS codes. Comput. Appl. Math. **38**, 1–13 (2019)
38. Nadkarni, P.J., Garani, S.S.: Non-binary entanglement-assisted stabilizer codes. Quantum Inf. Process. **20**, 256 (2021)
39. Pang, B., Zhu, S., Li, F., Chen, X.: New entanglement-assisted quantum MDS codes with larger minimum distance. Quantum Inf. Process. **19**, 207 (2020)
40. Pang, B., Zhu, S., Wang, L.: New entanglement-assisted quantum MDS codes. Int. J. Quantum Inf. **19**, 2150016 (2021)
41. Qian, J., Zhang, L.: On MDS linear complementary dual codes and entanglement-assisted quantum codes. Des. Codes Cryptogr. **86**, 1565–1572 (2018)
42. Thangaraj, A., McLaughlin, S.W.: Quantum codes from cyclic codes over GF(4^m). IEEE Trans. Inf. Theory **47**, 1176–1178 (2001)
43. Wang, L., Zhu, S.: New quantum MDS codes derived from constacyclic codes. Quantum Inf. Process. **14**, 881–889 (2015)
44. Wang, L., Zhu, S., Sun, Z.: Entanglement-assisted quantum MDS codes from cyclic codes. Quantum Inf. Process. **19**, 65 (2020)
45. Wilde, M.M., Brun, T.A.: Optimal entanglement formulas for entanglement-assisted quantum coding. Phys. Rev. A **77**, 64302 (2008)