Quantum Information Processing (2020) 19:207
https://doi.org/10.1007/s11128-020-02698-2

New entanglement-assisted quantum MDS codes with larger minimum distance

Binbin Pang[1] · Shixin Zhu[1] · Fulin Li[1] · Xiaojing Chen[2]

Received: 22 July 2019 / Accepted: 12 May 2020 / Published online: 8 June 2020

Abstract

In this paper, we construct some new entanglement-assisted quantum maximum distance separable (EAQMDS) codes with lengths $n = q^2 + 1$ and $n = (q^2 + 1)/2$ from negacyclic MDS codes and constacyclic MDS codes, respectively. All of them have flexible parameters. These EAQMDS codes we constructed have larger minimum distance and contain the known EAQMDS codes with same length in previous papers.

Keywords q^2-Cyclotomic coset · Constacyclic codes · EAQMDS codes

1 Introduction

In 2006, Brun et al. [1] proposed entanglement-assisted quantum error-correcting codes (EAQECCs for short) that do not require the dual-containing constraint necessary for standard quantum error-correcting codes. The EAQECCs play an important role in protecting quantum information from decoherence and quantum noise. Since then, it has attracted many scholars to study EAQECCs [4,7–10,16–19,25,28,29].

This research is supported by the National Natural Science Foundation of China under Grant Nos. 61772168, 61802102 and 11501156, and the Anhui Provincial Natural Science Foundation under Grant No. 1708085QA01.

✉ Shixin Zhu
zhushixinmath@hfut.edu.cn

Binbin Pang
pbbmath@126.com

Fulin Li
lflsxx66@163.com

Xiaojing Chen
chenxiaojing0909@ahu.edu.cn

[1] School of Mathematics, Hefei University of Technology, Hefei 230009, Anhui, People's Republic of China

[2] School of Internet, Anhui University, Hefei 230039, Anhui, People's Republic of China

Many good EAQECCs are constructed by some classical codes. The generalized Reed–Solomon codes, LCD codes, cyclic codes and constacyclic codes are good codes used for constructing EAQECCs.

A q-ary $[[n, k, d; c]]_q$ EAQECC that encodes k information qubits into n channel qubits with the help of c pairs of maximally entangled Bell states (ebits) can correct up to $\lfloor (d-1)/2 \rfloor$ errors, where d is the minimum distance of the code. What is more, the parameters of EAQECCs satisfy the following EA-quantum Singleton bound

$$2d \leq n - k + c + 2.$$

Clearly, if $c = 0$, the above bound is quantum Singleton bound. If a q-ary EAQECC achieves this bound, it is called an EAQMDS code. It is well known that the length n of nontrivial EAQMDS codes is less than or equal to $q^2 + 1$. In recent years, many work have been done in EAQMDS codes [3,5,6,12,20–23,26]. In particular, when $n = q^2 + 1$ and $(q^2 + 1)/2$, there are abundant results about EAQMDS codes whose minimum distance is larger than all known EAQMDS codes with same length.

In [5], Fan et al. obtained a class of EAQMDS codes with parameters $[[q^2+1, q^2-2d+4, d; 1]]_q$ by using cyclic codes, where $2 \leq d \leq 2q$ is an even integer. After that, Qian et al. constructed two new classes of q-ary EAQMDS codes with parameters $[[q^2+1, q^2-4(m-1)(q-m+1), 2(m-1)q+2; 4(m-1)2+1]]_q$ and $[[q^2+1, q^2-4(m-1)(q-m+1), 2(m-1)q-2l+2; 4(m-1)2+1-4l]]_q$, where $2 \leq m \leq \lfloor q/2 \rfloor$ and $1 \leq l \leq m-1$ [27]. By using negacyclic codes, Chen et al. constructed a new class of EAQMDS codes with parameters $[[q^2+1, q^2+5-2q-4t, q+2t+1; 4]]_q$, where $q \equiv 1 \bmod 4$ and $2 \leq t \leq (q-1)/2$ [2]. By using LCD codes, Qian et al. [26] constructed some new EAQMDS codes with maximal entanglement (i.e., $c = n - k$) with length $n = q^2 + 1$. By using constacyclic codes, Lu et al. [20] constructed a new class of EAQMDS codes with parameters $[[q^2+1, q^2-2d+7, d; 4]]_q$, where q is an odd prime power and $q+3 \leq d \leq 3q-1$ is even. In [24], Mustafa et al. constructed new EAQMDS codes with parameters $[[q^2+1, q^2-4q+4, 2q+2; 5]]_q$ and $[[q^2+1, q^2-4\lambda+8, 2\lambda+2; 9]]_q$, where $q+1 \leq \lambda \leq 2q-2$ and $q \equiv 3 \bmod 4$.

As for $n = (q^2+1)/2$, Fan et al. obtained a class of EAQMDS codes with parameters $[[n, n-2d+3, d; 1]]_q$, where $2 \leq d \leq 2\left\lfloor (n)/(q+1) \right\rfloor$ is an even integer [5]. Chen et al. constructed a new class of EAQMDS codes with parameters $[[n, n-2q-4t+5, q+2t+1; 5]]_q$, where $2 \leq t \leq (q-1)/2$ [2]. They also obtained a class of maximal entanglement-assisted quantum codes with parameters $[[n, n-5, d \geq 3; 5]]_q$.

Inspired by these works, we consider to construct new EAQMDS codes with larger minimum distance whose lengths n are equal to $q^2 + 1$ and $(q^2+1)/2$. This paper is organized as follows. In Sect. 2, some basic knowledge about constacyclic codes and EAQECCs are recalled. In Sect. 3, we construct three classes of EAQMDS codes with length $n = q^2 + 1$. In Sect. 4, we construct a class of EAQMDS codes with length $n = (q^2+1)/2$. Finally, we give the conclusion in Sect. 5.

2 Preliminaries

In this section, we give some basic results and notations of negacyclic codes and EAQECCs. The readers also can refer to [2–12,14] for more details.

Throughout this paper, let $\mathbb{F}_{q^2}$ be a finite field with q^2 elements, where q is a prime power. For any $a \in \mathbb{F}_{q^2}$, the conjugation of a is denoted by $\overline{a} = a^q$. For two vectors $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ and $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1}) \in \mathbb{F}_{q^2}^n$, their Hermitian inner product is defined as

$$(\mathbf{a}, \mathbf{b})_h = \sum_{i=0}^{n-1} \overline{a_i} b_i = a_0^q b_0 + a_1^q b_1 + \cdots + a_{n-1}^q b_{n-1}.$$

An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_{q^2}$ is a k-dimensional linear subspace of $\mathbb{F}_{q^2}^n$ and minimum distance d. The parameters of the code $\mathcal{C}$ satisfy the Singleton bound

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

If minimum distance d meets this bound, then $\mathcal{C}$ is called an MDS code. The Hermitian dual code of $\mathcal{C}$ is defined as

$$\mathcal{C}^{\perp_h} = \{\mathbf{a} \in \mathbb{F}_{q^2}^n \,|(\mathbf{a}, \mathbf{b})_h = 0 \text{ for all } \mathbf{b} \in \mathcal{C}\}.$$

For an element $\eta \in \mathbb{F}_{q^2}^*$, let the order of η be r. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_{q^2}$ is called an η-constacyclic code if any $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies its constacyclic shift $(\eta c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. Particularly, if $\eta = 1$, then $\mathcal{C}$ is cyclic code. If $\eta = -1$, then $\mathcal{C}$ is negacyclic code. By identifying any vector $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_{q^2}^n$ with a polynomial $c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_{q^2}[x]/\langle x^n - \eta\rangle$, then a constacyclic code over $\mathbb{F}_{q^2}$ is an ideal of $\mathbb{F}_{q^2}[x]/\langle x^n - \eta\rangle$. In fact, every ideal of $\mathbb{F}_{q^2}[x]/\langle x^n - \eta\rangle$ is a principal ideal, so every constacyclic code $\mathcal{C}$ has generator polynomial $g(x)$. Let $\mathcal{C} = \langle g(x)\rangle$, where $g(x)$ is a unique monic polynomial which has minimal degree in $\mathcal{C}$. And $h(x) = (x^n - \eta)/g(x)$ is the check polynomial of $\mathcal{C}$.

Note that $x^n - \eta$ has no repeated root over $\mathbb{F}_{q^2}$ if and only if $\gcd(n, q) = 1$. Let γ be a primitive rnth root of unity such that $\eta = \gamma^n$ in $\mathbb{F}_{q^{2m}}$, where m is the multiplicative order of q^2 modulo rn, i.e., $m = \mathrm{ord}_{rn}(q^2)$. The roots of $x^n - \eta$ are $\gamma^{1+ir}, 0 \leq i \leq n-1$. Let $\mathbb{Z}_{rn} = \{0, 1, \ldots, rn-1\}$ and Ω_{rn} be a set with form $1 + ir$ in $\mathbb{Z}_{rn}$. For any $i \in \mathbb{Z}_{rn}$, the q^2-cyclotomic coset modulo rn is given by

$$C_i = \{i, iq^2, iq^4, \ldots, iq^{2(d_i-1)}\},$$

where d_i is the smallest positive integer such that $iq^{2d_i} \equiv i \bmod rn$, which is also called the size of C_i. Hence, $M_i(x) = \Pi_{j \in C_i}(x - \gamma^j)$ is the minimal polynomial of γ^i over $\mathbb{F}_{q^2}$. For a constacyclic code $\mathcal{C} = \langle g(x)\rangle$ with length n over $\mathbb{F}_{q^2}$, its defining set is the set $T = \{i \in \Omega_{rn} \mid g(\gamma^i) = 0\}$. It is well known that Ω_{rn} is an union of some q^2-cyclotomic coset modulo rn.

Lemma 2.1 (The BCH Bound for η-Constacyclic Codes [11]) *Let $\mathcal{C}$ be a q^2-ary η-constacyclic code of length n. If the generator polynomial $g(x)$ of $\mathcal{C}$ has the elements $\{\gamma^{1+ir} \mid 0 \leq i \leq d-2\}$ as the roots, where γ is a primitive rnth root of unity, then the minimum distance of $\mathcal{C}$ is at least d.*

As we all know, the key to construct EAQECCs from any classical linear code over $\mathbb{F}_{q^2}$ is to determine the number of entangled states c. Recently, for constacyclic codes, scholars have utilized decompose defining set of constacyclic codes to obtain the number of entangled qubits c of corresponding EAQECCs. The classical Hermitian constructions can be referred to [2,14,15].

Lemma 2.2 *If $\mathcal{C}$ is an $[n, k, d]_{q^2}$ classical code and H is its parity check matrix over $\mathbb{F}_{q^2}$, then there exist entanglement-assisted quantum codes with parameters $[[n, 2k-n+c, d; c]]_q$, where $c = \operatorname{rank}(HH^{\dagger})$ and $H^{\dagger}$ is the conjugate transpose matrix of H over $\mathbb{F}_{q^2}$.*

Definition 2.3 Let $\mathcal{C}$ be a q^2-ary η-constacyclic code of length n with defining set T. Assume that $T_{\mathrm{ss}} = T \bigcap (-qT)$ and $T_{\mathrm{sas}} = T \backslash T_{\mathrm{ss}}$, where $-qT = \{rn - qx \mid x \in T\}$ and $r \mid q+1$. Then, $T = T_{\mathrm{ss}} \bigcup T_{\mathrm{sas}}$ is called a decomposition of the defining set of $\mathcal{C}$.

Lemma 2.4 *Let $\mathcal{C}$ be a constacyclic code with length n over $\mathbb{F}_{q^2}$, where $\gcd(n, q) = 1$. Suppose that T is the defining set of the constacyclic code $\mathcal{C}$ and $T = T_{\mathrm{ss}} \cup T_{\mathrm{sas}}$ is a decomposition of T. Then, the number of entangled states required is $c = |T_{\mathrm{ss}}|$.*

Let $[a, b] = \{i \in \mathbb{Z}_+ \mid a \leq i \leq b\}$ and $[i] = [0, i]$, where $\mathbb{Z}_+$ denote the set of all nonnegative integers. For integers a, b and x, $a \leq x \leq b \Leftrightarrow x \in [a, b]$ if $a \leq b$, $\Leftrightarrow x \in \emptyset$ if $a > b$.

3 New EAQMDS codes of length $q^2 + 1$

In this section, let $r = 2$. We construct some new EAQMDS codes from negacyclic codes of length $q^2 + 1$.

Lemma 3.1 ([13,20]) *Let $n = q^2 + 1$ and $s = n/2$, where $q \geq 5$ is an odd prime power. Then the q^2-cyclotomic coset modulo $2n$ containing all odd integers from 1 to $2n$ are $C_s = \{s\}$, $C_{3s} = \{3s\}$ and $C_{s+2i} = \{s+2i, s-2i\}$ with $1 \leq i \leq s-1$.*

Based on the result of Lemma 3.1, we give another expression of the q^2-cyclotomic coset modulo $2n$ containing integers in Ω_{2n} as follows

$$C_{s+2(iq+j)} = \{s + 2(iq+j), s - 2(iq+j)\},$$

where $0 \leq j \leq q-1$ if $0 \leq i \leq (q-3)/2$, and $0 \leq j \leq (q+1)/2$ if $i = (q-1)/2$. Note that the subscripts of $C_{s+2(iq+j)}$ are all belong to $[s, 3s]$.

Lemma 3.2 *Let $n = q^2 + 1$ and $q \geq 5$ be an odd prime power and i, j be defined as above,* *(1) If* $q \equiv 1 \bmod 4$, *we have*

$$-qC_{s+2(iq+j)} = \begin{cases} C_{s+2\left(\left(\frac{q-1}{2}-j\right)q+\left(\frac{q+1}{2}+i\right)\right)}, & \text{if } 0 \le j \le \frac{q-1}{2}, \\ C_{s+2\left(\left(j-\frac{q+1}{2}\right)q+\left(\frac{q-1}{2}-i\right)\right)}, & \text{if } \frac{q+1}{2} \le j \le q-1. \end{cases}$$

(2) If $q \equiv 3 \bmod 4$, *we have*

$$-qC_{s+2(iq+j)} = C_{s+2(jq-i)}.$$

Proof By Lemma 3.1, we have $C_{s+2(iq+j)} = \{s+2(iq+j), s-2(iq+j)\}$.

(1) Assume that $q \equiv 1 \bmod 4$. If $0 \le j \le (q-1)/2$, we have

$$\begin{aligned} -q(s+2(iq+j)) &= -qs - 2iq^2 - 2jq = -qs - 2i(q^2+1) - 2jq + 2i \\ &\equiv s + 2\left(\left(\frac{q-1}{2}-j\right)q + \left(\frac{q+1}{2}+i\right)\right) \bmod 2n, \end{aligned}$$

which implies that $-qC_{s+2(iq+j)} = C_{s+2\left(\left(\frac{q-1}{2}-j\right)q+\left(\frac{q+1}{2}+i\right)\right)}$.
If $(q+1)2 \le j \le q-1$, we have

$$\begin{aligned} -q(s-2(iq+j)) &= -qs + 2iq^2 + 2jq = -qs + 2i(q^2+1) + 2jq - 2i \\ &\equiv s + 2\left(\left(j-\frac{q+1}{2}\right)q + \left(\frac{q-1}{2}-i\right)\right) \bmod 2n, \end{aligned}$$

which implies that $-qC_{s+2(iq+j)} = C_{s+2\left(\left(j-\frac{q+1}{2}\right)q+\left(\frac{q-1}{2}-i\right)\right)}$.

(2) Assume that $q \equiv 3 \bmod 4$, then we have

$$\begin{aligned} -q(s-2(iq+j)) &= -qs + 2iq^2 + 2jq = -qs + 2i(q^2+1) + 2jq - 2i \\ &\equiv s + 2(jq-i) \bmod 2n, \end{aligned}$$

which implies that $-qC_{s+(iq+j)r} = C_{s+(jq-i)r}$. The desired results follows. □

Lemma 3.3 *Let* $n = q^2+1$ *and* $q \ge 5$ *be an odd prime power. For a positive integer,* $2 \le m \le (q-1)/2$.

(1) If $q \equiv 1 \bmod 4$, *we define*

$$T_1 = \bigcup_{\substack{0 \le i \le m, \\ 0 \le j \le (q-2m-1)/2}} C_{s+2(iq+j)} \bigcup_{\substack{0 \le u \le m-1, \\ (q+2m+1)/2 \le v \le q-1}} C_{s+2(uq+v)}.$$

Then $T_1 \cap -qT_1 = \emptyset$.

(2) If $q \equiv 3 \bmod 4$, *we define*

$$T_2 = \bigcup_{\substack{0\le i\le m-1,\\ m+1\le j\le q-m-1}} C_{s+2(iq+j)} \bigcup_{\substack{i=m,\\ m+1\le j\le (q-2m-1)/2}} C_{s+2(iq+j)} \bigcup_{\substack{(q-1)/2-m\le u\le m-1,\\ v=q-m}} C_{s+2(uq+v)}.$$

Then $T_2 \bigcap -qT_2 = \emptyset$.

Proof (1) Assume that $q \equiv 1 \bmod 4$. Let

$$T_1 = \bigcup_{\substack{0\le i\le m,\\ 0\le j\le (q-2m-1)/2}} C_{s+2(iq+j)} \bigcup_{\substack{0\le u\le m-1,\\ (q+2m+1)/2\le v\le q-1}} C_{s+2(uq+v)}.$$

From the result of (1) in Lemma 3.2, we have

$$-qT_1 = \bigcup_{\substack{0\le i\le m,\\ 0\le j\le (q-2m-1)/2}} C_{s+2\left(\left(\frac{q-1}{2}-j\right)q+\left(\frac{q+1}{2}+i\right)\right)} \bigcup_{\substack{0\le u\le m-1,\\ (q+2m+1)/2\le v\le q-1}} C_{s+2\left(\left(v-\frac{q+1}{2}\right)q+\left(\frac{q-1}{2}-u\right)\right)}.$$

If $0 \le i \le m, 0 \le j \le (q-2m-1)/2$, then we have

$$\begin{aligned} &s+2(iq+j) \le s+2\left(mq+\frac{q-2m-1}{2}\right),\\ &s+2\left(\left(\frac{q-1}{2}-j\right)q+\left(\frac{q+1}{2}+i\right)\right)\\ &\ge s+2\left(mq+\frac{q+1}{2}\right). \end{aligned}$$

If $0 \le u \le m-1$, $(q+2m+1)/2 \le v \le q-1$, then we have

$$\begin{aligned} &s+2(uq+v) \le s+2((m-1)q+q-1),\\ &s+2\left(\left(v-\frac{q+1}{2}\right)q+\left(\frac{q-1}{2}-u\right)\right) \ge s+2\left(mq+\frac{q-2m+1}{2}\right). \end{aligned}$$

Therefore,

$$\begin{aligned} s+2(iq+j) &< s+2\left(\left(\frac{q-1}{2}-j\right)q+\left(\frac{q+1}{2}+i\right)\right),\\ s+2(iq+j) &< s+2\left(\left(v-\frac{q+1}{2}\right)q+\left(\frac{q-1}{2}-u\right)\right), \end{aligned}$$

$$s+2(uq+v)<s+2\left(\left(\frac{q-1}{2}-j\right)q+\left(\frac{q+1}{2}+i\right)\right),$$
$$s+2(uq+v)<s+2\left(\left(v-\frac{q+1}{2}\right)q+\left(\frac{q-1}{2}-u\right)\right).$$

For the range of i, j, u, v, the subscripts of $C_{s+2(iq+j)}$, $C_{s+2(uq+v)}$, $C_{s+2((\frac{q-1}{2}-j)q+(\frac{q+1}{2}+i))}$ and $C_{s+2((v-\frac{q-1}{2})q-(\frac{q+1}{2}+u))}$ are all belong to $[s, 3s]$. Then $T_1 \bigcap -qT_1 = \emptyset$.

(2) Assume that $q \equiv 3 \bmod 4$. If $2 \le m \le (q-3)/4$, then

$$T_2 = \bigcup_{\substack{0\le i\le m-1,\\ m+1\le j\le q-m-1}} C_{s+2(iq+j)} \bigcup_{\substack{i=m,\\ m+1\le j\le (q-2m-1)/2}} C_{s+2(iq+j)}.$$

From the result of (2) in Lemma 3.2, we have

$$-qT_2 = \bigcup_{\substack{0\le i\le m-1,\\ m+1\le j\le q-m-1}} C_{s+2(jq-i)} \bigcup_{\substack{i=m,\\ m+1\le j\le (q-2m-1)/2}} C_{s+2(jq-i)}.$$

If $(q+1)/4 \le m \le (q-1)/2$, then

$$T_2 = \bigcup_{\substack{0\le i\le m-1,\\ m+1\le j\le q-m-1}} C_{s+2(iq+j)} \bigcup_{\substack{(q-1)/2-m\le u\le m-1,\\ v=q-m}} C_{s+2(uq+v)}.$$

From the result of (2) in Lemma 3.2, we have

$$-qT_2 = \bigcup_{\substack{0\le i\le m-1,\\ m+1\le j\le q-m-1}} C_{s+2(jq-i)} \bigcup_{\substack{(q-1)/2-m\le u\le m-1,\\ v=q-m}} C_{s+2(vq-u)}.$$

Similar to the proof of (1), we have $T_2 \bigcap -qT_2 = \emptyset$. This completes the proof. □

Theorem 3.4 *Let $n = q^2+1$ and $q \ge 5$ be an odd prime power. For a positive integer, $2 \le m \le (q-1)/2$. Let $\mathcal{C}$ be a cyclic code with defining set T given as follows*

$$T = \bigcup_{\substack{0\le i\le m-1,\\ 0\le j\le q-1}} C_{s+2(iq+j)} \bigcup_{\substack{i=m,\\ 0\le j\le (q-2m-1)/2}} C_{s+2(iq+j)}.$$

(1) If $q \equiv 1 \bmod 4$, then $|T_{\mathrm{ss}}| = 4m^2$.
(2) If $q \equiv 3 \bmod 4$, then

$$|T_{\mathrm{ss}}| = \begin{cases} 4m(m+1)+1, & 2 \le m \le \frac{q-3}{4}, \\ 4m(m-1)+2q-1, & \frac{q+1}{4} \le m \le \frac{q-1}{2}. \end{cases}$$

Proof (1) Assume that $q \equiv 1 \bmod 4$. Define

$$T_1 = \bigcup_{\substack{0\le i\le m,\\ 0\le j\le (q-2m-1)/2}} C_{s+2(iq+j)} \bigcup_{\substack{0\le u\le m-1,\\ (q+2m+1)/2\le v\le q-1}} C_{s+2(uq+v)}$$

and

$$T_1' = \bigcup_{\substack{0\le i\le m-1,\\ (q-2m+1)/2\le j\le (q+2m-1)/2}} C_{s+2(iq+j)}.$$

From the result of (1) in Lemma 3.2 , we have

$$-qT_1' = \bigcup_{\substack{0\le i\le m-1,\\ (q-2m+1)/2\le j\le (q-1)/2}} C_{s+2\left(\left(\frac{q-1}{2}-j\right)q+\left(\frac{q+1}{2}+i\right)\right)} \bigcup_{\substack{0\le i\le m-1,\\ (q+1)/2\le j\le (q+2m-1)/2}} C_{s+2\left(\left(j-\frac{q+1}{2}\right)q+\left(\frac{q-1}{2}-i\right)\right)}.$$

For $0 \le i \le m-1$, $(q-2m+1)/2 \le j \le (q-1)/2$, it is easy to check that $0 \le (q-1)/2 - j \le m-1$ and $(q+1)/2 \le (q+1)/2 + i \le (q+2m-1)/2$. For $0 \le i \le m-1$, $(q+1)/2 \le j \le (q+2m-1)/2$, it is easy to check that $0 \le j-(q+1)/2 \le m-1$ and $(q-2m+1)/2 \le (q-1)/2 - i \le (q-1)/2$. Then we have $-qT_1' = T_1'$. From the definitions of T, T_1 and T_1', we have $T = T_1 \bigcup T_1'$. By Definition 2.3 and Lemma 3.3, then

$$\begin{aligned} T_{\mathrm{ss}} &= T \bigcap(-qT) = (T_1 \bigcup T_1') \bigcap(-qT_1 \cup T_1') \\ &= (T_1 \bigcap -qT_1) \bigcup(T_1 \bigcap -qT_1') \bigcup(T_1' \bigcap -qT_1) \bigcup(T_1' \bigcap -qT_1') \\ &= T_1'. \end{aligned}$$

Therefore, $|T_{\mathrm{ss}}| = |T_1'| = 4m^2$.

(2) Assume that $q \equiv 3 \bmod 4$. If $2 \le m \le (q-3)/4$, then define

$$T_2 = \bigcup_{\substack{0\le i\le m-1,\\ m+1\le j\le q-m-1}} C_{s+2(iq+j)} \bigcup_{\substack{i=m,\\ m+1\le j\le (q-2m-1)/2}} C_{s+2(iq+j)},$$

and

$$T_2' = \bigcup_{\substack{0\le i\le m-1, 0\le j\le m\\ q-m\le j\le q-1}} C_{s+2(iq+j)} \bigcup_{\substack{i=m,\\ 0\le j\le m}} C_{s+2(iq+j)}.$$

Similar to the proof of (1), we have $|T_{\mathrm{ss}}| = |T_2'| = 4m(m+1)+1$.

If $(q+1)/4 \leq m \leq (q-1)/2$, let

$$T_2 = \bigcup_{\substack{0 \leq i \leq m-1, \\ m+1 \leq j \leq q-m-1}} C_{s+2(iq+j)} \bigcup_{\substack{(q-1)/2-m \leq u \leq m-1, \\ v=q-m}} C_{s+2(uq+v)},$$

and

$$T_2' = \bigcup_{\substack{0 \leq i \leq (q-3)/2-m, \\ 0 \leq j \leq m, q-m \leq j \leq q-1}} C_{s+2(iq+j)} \bigcup_{\substack{i=m, \\ 0 \leq j \leq (q-2m-1)/2}} C_{s+2(iq+j)}$$
$$\bigcup_{\substack{(q-1)/2-m \leq u \leq m-1, \\ 0 \leq j \leq m, q-m+1 \leq j \leq q-1}} C_{s+2(uq+v)}.$$

Similar to the proof of (1), we can obtain $|T_{\mathrm{ss}}| = |T_2'| = 4m(m-1)+2q-1$. The desired results follow. □

Theorem 3.5 *Let* $n = q^2+1$ *and* $q \geq 5$ *be an odd prime power.*

(1) If $q \equiv 1 \bmod 4$*, then there are the following EAQMDS codes with parameters*

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

where $2 \leq m \leq (q-1)/2$.

(2) If $q \equiv 3 \bmod 4$

(i) $2 \leq m \leq (q-3)/4$*, then there are the following EAQMDS codes with parameters*

$$\begin{aligned}&[[n, n-(4m+2)q+4m(m+2)+1,\\ &(2m+1)q-2m+1; 4m(m+1)+1]]_q.\end{aligned}$$

(ii) $(q+1)/4 \leq m \leq (q-1)/2$*, then there are the following EAQMDS codes with parameters*

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

Proof Suppose that $\mathcal{C}$ is a cyclic code with defining set T, which is given in Theorem 3.4.

(1) When $q \equiv 1 \bmod 4$, note that the cyclic code $\mathcal{C}$ have $(2m+1)q-2m$ consecutive roots. From Lemma 2.1, the minimum distance of $\mathcal{C}$ is at least $(2m+1)q-2m+1$. Then $\mathcal{C}$ is an MDS code with parameter $[n, n-(2m+1)q+2m, (2m+1)q-2m+1]_{q^2}$ by Singleton bound. From Lemma 3.3, we have $|T_{\mathrm{ss}}| = 4m^2$. From Lemmas 2.2 and 2.4, there are the following EAQECCs with parameters

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

Table 1 Some new EAQMDS codes with length $n = q^2 + 1$

Length	Parameters	Condition	Distance	References
n	$[[n, n-4q+3, d; 5]]_q$	$q \geq 5$	$2q+2$	[27]
n	$[[n, n-8q+15, d; 9]]_q$	$q \geq 7$	$4q-2$	[27]
n	$[[n, n-8q+15, d; 13]]_q$	$q \geq 7$	$4q$	[27]
n	$[[n, n-8q+15, d; 17]]_q$	$q \geq 7$	$4q+2$	[27]
n	$[[n, n-12q+35, d; 25]]_q$	$q \geq 9$	$6q-4$	[27]
n	$[[n, n-12q+35, d; 29]]_q$	$q \geq 9$	$6q-2$	[27]
n	$[[n, n-10q+24, d; 16]]_q$	$q \geq 5, q \equiv 1 \bmod 4$	$5q-3$	Th.3.5 (1)
n	$[[n, n-14q+48, d; 36]]_q$	$q \geq 9, q \equiv 1 \bmod 4$	$7q-5$	Th.3.5 (1)
n	$[[n, n-12q+35, d; 2q+23]]_q$	$q \geq 7, q \equiv 3 \bmod 4$	$7q-5$	Th.3.5 (2)
n	$[[n, n-20q+99, d; 2q+79]]_q$	$q \geq 11, q \equiv 3 \bmod 4$	$11q-9$	Th.3.5 (2)

Notice that

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

which implies that the EAQECCs are EAQMDS codes.

(2) When $q \equiv 3 \bmod 4$, we can construct EAQMDS codes with the following parameters

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

Its proof is similar to (1), so we omit it here. □

Next, we list some new EAQMDS codes and compare these codes with previously all known EAQMDS codes of length $n = q^2 + 1$ in Table 1.

Furthermore, we compare these codes with EAQMDS codes constructed in [30], where q is an odd prime power. For convenience, we write their parameters in a unified form.

We obtain EAQMDS codes with the following parameters.

1 For $2 \leq m \leq \frac{q-1}{2}$, let $d = 2 + (2m+1)(q-1)$ and $q \equiv 1 \bmod 4$, $[[n, n - 2d + 4m^2 + 2, d; 4m^2]]_q$;

2.1 For $3 \leq m \leq \frac{q+1}{4}$, let $d = 2m(q-1) - q + 3$ and $q \equiv 3 \bmod 4$, $[[n, n - 2d + 4m^2 - 4m + 3, d; 1 + 4m^2 - 4m]]_q$;

2.2 For $\frac{q+1}{4} \leq m \leq \frac{q-1}{2}$, let $d = 2 + (2m+1)(q-1)$ and $q \equiv 3 \bmod 4$, $[[n, n - 2d + 4m^2 - 4m + 2q + 1, d; 4m(m-1) + 2q - 1]]_q$.

Wang et al. [30] constructed two classes of EAQMDS codes below.

1′ For $1 \leq m \leq \frac{q-1}{4}$, let $2 + (2m-1)(q+1) \leq d \leq 2 + (2m+1)(q-1)$ and d be even, $[[n, n - 2d + 4m^2 + 2, d; 4m^2]]_q$;

2′ For $1 \leq m \leq \frac{q+1}{4}$, let $2 + (2m-1)(q+1) \leq d \leq 2 + 2m(q-1)$ and d be even, $[[n, n - 2d + 4m^2 - 4m + 3, d; 1 + 4m^2 - 4m]]_q$.

Compared with the codes in [30], our parameters are new in the following three cases.

(a) The EAQMDS codes are new for $\frac{q+3}{4} \leq m \leq \frac{q-1}{2}$ in case 1;
(b) The EAQMDS codes are new for $3 \leq m \leq \frac{q+1}{4}$ in case 2.1;
(c) The EAQMDS codes are new for $\frac{q+1}{4} \leq m \leq \frac{q-1}{2}$ in case 2.2.

4 New EAQMDS codes of length $\frac{q^2+1}{2}$

In this section, we construct new EAQMDS codes from η-constacyclic codes of length $n = (q^2+1)/2$ over $\mathbb{F}_{q^2}$. Throughout this section, let $r \mid q+1$.

Lemma 4.1 *Let $n = (q^2+1)/2$, $r < q+1$ and $r \mid q+1$, where q is an odd prime power. Then the q^2-cyclotomic coset modulo rn containing integers in Ω_{rn} are $C_n = \{n\}$ and $C_{n+ir} = \{n+ir, n-ir\}$ with $1 \leq i \leq (n-1)/2$.*

Proof Note that the size of C_{n+ir} at most two since $\mathrm{ord}_{rn}(q^2) = 2$. It is clear that $C_n = \{n\}$ since $q^2 n \equiv n \bmod rn$. Notice that $q^2(n+ir) \equiv n - ir \bmod rn$. This completes the proof. □

In Lemma 4.1, an expression of the q^2-cyclotomic coset modulo rn containing integers in Ω_{rn} is given. Next, we will give another expression of the q^2-cyclotomic cosets. The definitions of n, r, q are the same as in Lemma 4.1; then,

$$C_{n+(iq+j)r} = \{n + (iq+j)r, n - (iq+j)r\},$$

where i and j have inner connection listed below. Assume that $q \equiv 1 \bmod 4$, then

$$\begin{cases} 0 \leq j \leq q-1, \ 0 \leq i \leq \frac{q-5}{4}, \\ 0 \leq j \leq \frac{q-1}{4}, \quad i = \frac{q-1}{4}. \end{cases}$$

Assume that $q \equiv 3 \bmod 4$, then

$$\begin{cases} 0 \leq j \leq q-1, \ 0 \leq i \leq \frac{q-7}{4}, \\ 0 \leq j \leq \frac{3q-1}{4}, \ \ i = \frac{q-3}{4}. \end{cases}$$

From this expression, we have the following lemma, which is vital for the construction of EAQMDS codes.

Lemma 4.2 *Let $n = (q^2+1)/2$ and q be an odd prime power. For i, j defined as above, then we have*

$$-qC_{n+(iq+j)r} = C_{n+(jq-i)r}.$$

Proof By Lemma 4.1, we have $C_{n+(iq+j)r}=\{n+(iq+j)r,n-(iq+j)r\}$.

$$\begin{aligned}-q(n-(iq+j)r)&=irq^2+jrq-qn=ir(q^2+1)-qn+jrq-ir\\&\equiv n+(jq-i)r \bmod rn,\end{aligned}$$

which implies that $-qC_{n+(iq+j)r}=C_{n+(jq-i)r}$. □

Lemma 4.3 *Let $n=(q^2+1)/2$, $t=(q-1)/2$ and q be an odd prime power. For a positive integer, $2\le m\le(q+1)/2$.*

(1) If m is even, we define

$$T_1=\bigcup_{\substack{0\le i\le(m-4)/2,i+1\le j\le t-i,\\ \text{or } t+2+i\le j\le 2t-i}}C_{n+(iq+j)r}\quad\bigcup_{\substack{i=(m-2)/2,i+1\le j\le t-i,\\ \text{or } t+2+i\le j\le q-m/2}}C_{n+(iq+j)r}.$$

Then $T_1\cap -qT_1=\emptyset$.

(2) If m is odd, we define

$$T_2=\bigcup_{\substack{0\le i\le(m-3)/2,i+1\le j\le t-i,\\ \text{or } t+2+i\le j\le 2t-i}}C_{n+(iq+j)r}\quad\bigcup_{i=(m-1)/2,1+i\le j\le t-i}C_{n+(iq+j)r}.$$

Then $T_2\cap -qT_2=\emptyset$.

Proof As for the case of $q\equiv 1 \bmod 4$, let $\widetilde{T_2}=T_2$, where $m=(q+1)/2$ and m is odd. It is easy to check that $T_1\subseteq\widetilde{T_2}$ and $T_2\subseteq\widetilde{T_2}$ for any $2\le m<(q+1)/2$. Then we only need to prove $\widetilde{T_2}\cap -q\widetilde{T_2}=\emptyset$. Since $m=(q+1)/2$ is an odd integer, then we can get the following result from (2)

$$\widetilde{T_2}=\bigcup_{\substack{0\le i\le(q-5)/4,i+1\le j\le t-i,\\ \text{or } t+2+i\le j\le 2t-i}}C_{n+(iq+j)r}.$$

From Lemma 4.2, we have

$$-q\widetilde{T_2}=\bigcup_{\substack{0\le i\le(q-5)/4,i+1\le j\le t-i,\\ \text{or } t+2+i\le j\le 2t-i}}C_{n+(jq-i)r}.$$

Note that $n=(q-1)q/2+(q+1)/2$. For $0\le i\le(q-5)/4$, $i+1\le j\le t-i$, or $t+2+i\le j\le 2t-i$. We have $C_{n+(iq+j)r}=\{n+(iq+j)r,n-(iq+j)r\}$. For $(q+1)/2\le j\le q-1$, $C_{n+(jq-i)r}=C_{n+((j-\frac{q-1}{2})q-(i-\frac{q+1}{2}))r}$. Thus, we only need to consider $1\le j\le(q-1)/2$. We divide our discussions into two subcases as to j.

(1) If $1\le j\le(q-1)(r-1)/2r$, then we have

$$C_{n+(jq-i)r}=\{n+(jq-i)r,(r+1)n+(jq-i)r,\}$$

where $n \leq (jq-i)r$, and

$$C_{n+(jq-i)r} = \{n+(jq-i)r, n-(jq-i)r, \}$$

where $n > (jq-i)r$.

Assume that $\widetilde{T_2} \cap -q\widetilde{T_2} \neq \emptyset$, then there are some of the following equations hold.

If $iq+j \leq \lfloor n/r \rfloor$, then we have $n+(iq+j)r = n+(jq-i)r, n+(iq+j)r = n-(jq-i)r, n+(iq+j)r = (r+1)n-(jq-i)r, n-(iq+j)r = n+(jq-i)r$, $n-(iq+j)r = n-(jq-i)r$ or $n-(iq+j)r = (r+1)n-(jq-i)r$ hold, but it is easy to check that it is impossible.

If $iq+j > \lfloor n/r \rfloor$, then we have $(r+1)n-(iq+j)r = n+(jq-i)r$, $(r+1)n-(iq+j)r = n-(jq-i)r$ or $(r+1)n-(iq+j)r = (r+1)n-(jq-i)r$ hold, which is equivalent to one of the cases in $iq+j \leq \lfloor n/r \rfloor$, so it is also impossible.

(2) If $(q-1)(r-1)/2r < j \leq (q-1)/2$, then we have

$$C_{n+(jq-i)r} = \{n+(jq-i-n)r, n-(jq-i-n)r, \}$$

where $n > (jq-i-n)r$, and

$$C_{n+(jq-i)r} = \{n+(jq-i-n)r, (r+1)n-(jq-i-n)r, \}$$

where $n \leq (jq-i-n)r$.

Assume that $\widetilde{T_2} \cap -q\widetilde{T_2} \neq \emptyset$, then there are some of the following equations hold.

If $iq+j \leq \lfloor n/r \rfloor$, then we have $n+(iq+j)r = n+(jq-i-n)r, n+(iq+j)r = n-(jq-i-n)r, n+(iq+j)r = (r+1)n-(jq-i-n)r$,$n-(iq+j)r = n+(jq-i-n)r$, $n-(iq+j)r = n-(jq-i-n)r$ or $n-(iq+j)r = (r+1)n-(jq-i-n)r$ hold, but it is easy to check that it is impossible.

If $iq+j > \lfloor n/r \rfloor$, then we have $(r+1)n-(iq+j)r = n+(jq-i-n)r$, $(r+1)n-(iq+j)r = n-(jq-i-n)r$, or $(r+1)n-(iq+j)r = (r+1)n-(jq-i-n)r$ hold, which is equivalent to one of case in $iq+j \leq \lfloor n/r \rfloor$, so it is also impossible.

As for the case of $q \equiv 3 \bmod 4$, we can get the same results similarly. Till now, we complete the proof. □

Theorem 4.4 *Let $n = (q^2+1)/2$ and q be an odd prime power. For a positive integer, $2 \leq m \leq (q+1)/2$.*

(1) If m is even, we define

$$T = \bigcup_{\substack{0\leq i\leq (m-4)/2,\\ 0\leq j\leq q-1}} C_{n+(iq+j)r} \bigcup_{\substack{i=(m-2)/2,\\ 0\leq j\leq q-m/2}} C_{n+(iq+j)r}.$$

(2) If m is odd, we define

$$T = \bigcup_{\substack{0\leq i\leq (m-3)/2,\\ 0\leq j\leq q-1}} C_{n+(iq+j)r} \bigcup_{\substack{i=(m-1)/2,\\ 0\leq j\leq (q-m)/2}} C_{n+(iq+j)r}.$$

Then we have $T_{\mathrm{ss}} = 2m(m-1) + 1$ *for any integer* $2 \leq m \leq (q+1)/2$.

Proof (1) If m is even, let

$$T_1 = \bigcup_{\substack{0\leq i\leq (m-4)/2, i+1\leq j\leq t-i,\\ \text{or } t+2+i\leq j\leq 2t-i}} C_{n+(iq+j)r} \quad \bigcup_{\substack{i=(m-2)/2, i+1\leq j\leq t-i,\\ \text{or } t+2+i\leq j\leq q-m/2}} C_{n+(iq+j)r},$$

and

$$T_1' = \bigcup_{\substack{1\leq u\leq (m-4)/2,\\ q-u\leq v\leq 2t}} C_{n+(uq+v)r} \quad \bigcup_{\substack{0\leq u\leq (m-2)/2, 0\leq v\leq u,\\ \text{or } t+1-u\leq v\leq t+1+u}} C_{n+(uq+v)r}.$$

By Lemma 4.2, we have

$$-qT_1' = \bigcup_{\substack{1\leq u\leq (m-4)/2,\\ q-u\leq v\leq 2t}} C_{n+(vq-u)r} \quad \bigcup_{\substack{0\leq u\leq (m-2)/2, 0\leq v\leq u,\\ \text{or } t+1-u\leq v\leq t+1+u}} C_{n+(vq-u)r}.$$

From the proof of Lemma 4.3, we have $T_1' \bigcap -qT_1' = C_n$. By the definitions of T, T_1 and T_1', we know $T = T_1 \bigcup T_1'$. Then we have

$$\begin{aligned} T_{\mathrm{ss}} &= T \bigcap -qT = \left(T_1 \bigcup T_1'\right) \bigcap -q\left(T_1 \bigcup T_1'\right) \\ &= \left(T_1 \bigcap -qT_1\right) \bigcup \left(T_1 \bigcap -qT_1'\right) \bigcup \left(T_1' \bigcap -qT_1\right) \bigcup (T_1' \bigcap -qT_1') \\ &= C_n \bigcup \left(T_1 \bigcap -qT_1'\right) \bigcap \left(T_1' \bigcap -qT_1\right). \end{aligned}$$

Next, we show that $T \bigcap -qT_1' = -qT_1'$. Let $S = S_1 \bigcup S_2$, $S_1 = \{(u,v) \mid 1 \leq u \leq (m-4)/2, q-u \leq v \leq 2t\}$, $S_2 = \{(u,v) \mid 0 \leq u \leq (m-2)/2, 0 \leq v \leq u \text{ or } t+1-u \leq v \leq t+1+u\}$ and $(v'q-u')r \equiv (vq-u)r \pmod{(r-1)n} \geq 0$. We only need to prove $uq+v-(v'q-u') \geq 0$ for any $(u,v) \in S$. We divide our discussions into three subcases.

(1.1) If $0 \leq (vq-u)r < (r-1)n$, it is easy to check that

$$uq + v - (v'q - u') = uq + v - (vq - u) \geq 0$$

for the range of (u,v).

(1.2) If $(r-1)n \leq (vq-u)r < 2(r-1)n$, we can easy prove that

$$\begin{aligned} uq + v - (v'q - u') = uq + v - ((v - (r-1)(q-1)/2r)q \\ -(u + (r-1)(q+1)/2r)) \geq 0 \end{aligned}$$

by considering the range of $(vq-u)r$ in the following three cases.

(i) If $v = (r-1)(q-1)/2r + 1$, then $q - u \geq (r-1)(q+1)/2r$. Thus, the above result follows.

(ii) If $(r-1)(q-1)/2r+1 < v < (r-1)(q-1)/r+1$, then the above result is apparent.

(iii) If $v=(r-1)(q-1)/r+1$, then $q-u < (r-1)(q+1)/r$. Thus, the above result follows.

(1.3) If $(vq-u)r \geq 2(r-1)n$, we can easy prove that

$$\begin{aligned} uq+v-(v'q-u') &= q+v-((v-(r-1)(q-1)/r)q \\ &\quad -(u+(r-1)(q+1)/r)) \geq 0 \end{aligned}$$

by considering the range of $(vq-u)r$ in the following two cases, where $v=(r-1)(q-1)/r+1$ or $v>(r-1)(q-1)/r+1$.

Then we have $T\bigcap -qT_1' = -qT_1'$ and $T_1'\bigcap -qT_1' = C_n$. Hence, $T_1\bigcap -qT_1' = -qT_1' \setminus C_n$. Notice that $-qT_1\bigcap T_1' = -q(T_1\bigcap -qT_1') = T_1' \setminus C_n$. Therefore, we have $T_{\text{ss}} = C_n\bigcup(T_1'\setminus C_n)\bigcup(-qT_1'\setminus C_n) = T_1'\bigcup -qT_1'$. Furthermore, we determine the size of T_{ss}. From Lemma 4.1, we have $|C_n|=1$ and $|C_{n+(iq+j)r}|=2$ with $(i,j)\neq(0,0)$. From the definition of T_1', we have $|T_{\text{ss}}| = |T_1'|+|-qT_1'|-|T_1'\bigcap -qT_1'| = 2|T_1'|-1 = 2m(m-1)+1$.

(2) If m is odd, let

$$T_2 = \bigcup_{\substack{0\le i\le (m-3)/2,\, i+1\le j\le t-i,\\ \text{or } t+2+i\le j\le 2t-i}} C_{n+(iq+j)r} \bigcup_{i=(m-1)/2,\, 1+i\le j\le t-i} C_{n+(iq+j)r},$$

and

$$T_2' = \bigcup_{\substack{0\le u\le (m-3)/2,\, q-u\le v\le 2t\\ \text{or } t+1-u\le v\le t+1+u}} C_{n+(uq+v)r} \bigcup_{\substack{0\le u\le (m-1)/2,\\ 0\le v\le u}} C_{n+(uq+v)r}.$$

By Lemma 4.2, we have

$$-qT_2' = \bigcup_{\substack{0\le u\le (m-3)/2,\, q-u\le v\le 2t\\ \text{or } t+1-u\le v\le t+1+u}} C_{n+(vq-u)r} \bigcup_{\substack{0\le u\le (m-1)/2,\\ 0\le v\le u}} C_{n+(vq-u)r}.$$

It is similar to (1). We have $T_{\text{ss}} = T_2'\bigcup -qT_2'$ and $|T_{\text{ss}}| = 2|T_2'|-1 = 2m(m-1)+1$. This completes the proof. □

Theorem 4.5 *Let $n=(q^2+1)/2$, $r|q+1$ and q be an odd prime power. For a positive integer, $2\le m\le (q+1)/2$. Then there are EAQMDS codes with parameters*

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

Proof Assume that the definitions of T, T_1, T_1', T_2 and T_2' are defined as in Theorem 4.4 and m a positive integer, where $2\le m\le (q+1)/2$. Suppose that $\mathcal{C}$ is a cyclic code of length $n=(q^2+1)/2$ with defining set T. Note that $\mathcal{C}$ has $m(q-1)$ consecutive

Table 2 Some new EAQMDS codes with length $n = \frac{q^2+1}{2}$

Length	Parameters	Condition	Distance	References
n	$[[n, n-5, d; 5]]_q$	$q > 3$	$d \geq 3$	[2]
n	$[[n, n-2d+7, d; 5]]_q$	$q > 7$	$q+5 \leq d \leq 2q$	[2]
n	$[[n, n-2d+3, d; 1]]_q$	–	$2 \leq d \leq 2\lfloor \frac{n}{q+1} \rfloor$ even	[5]
n	$[[n, n-2d+15, d; 13]]_q$	$q \geq 5$	$d = 3q-1$	New
n	$[[n, n-2d+27, d; 25]]_q$	$q \geq 7$	$d = 4q-2$	New
n	$[[n, n-2d+63, d; 61]]_q$	$q \geq 11$	$d = 6q-4$	New
n	$[[n, n-2d+87, d; 85]]_q$	$q \geq 13$	$d = 7q-5$	New

roots. It is easy to check that the dimension of $\mathcal{C}$ is $n-m(q-1)-1$. From Lemma 2.1, then we have $\mathcal{C}$ is an MDS code with parameters $[n, n-m(q-1)-1, m(q-1)+2]_{q^2}$. From Lemmas 2.2 and 2.4, Theorem 4.4, there are EAQECCs with parameters

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

Notice that

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

which implies that its parameters achieve the EA-quantum Singleton bound. Thus, the EAQECCs we constructed are EAQMDS codes. □

Next, we list some new EAQMDS codes and compare these codes with previously all known EAQMDS codes of length $n = (q^2+1)/2$ in Table 2.

5 Conclusion

In this paper, we investigate the q^2-cyclotomic coset modulo rn, where $n = q^2+1$ and $n = (q^2+1)/2$. Then series of entanglement-assisted quantum MDS codes with length $n = q^2+1$ and $n = (q^2+1)/2$ are constructed from negacyclic MDS codes and constacyclic codes, respectively. From those two tables, we know that EAQMDS codes constructed in the paper have larger minimum distance than those in the previous literature. It is an interesting problem to construct more EAQMDS codes with different lengths.

References

1. Brun, T., Devetak, I., Hsieh, M.: Correcting quantum errors with entanglement. Science **314**(5798), 436–439 (2006)
2. Chen, J., Huang, Y., Feng, C., Chen, R.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. Quantum Inf. Process. **16**(303), 1–22 (2017)

3. Chen, X., Zhu, S., Kai, X.: Entanglement-assisted quantum MDS codes constructed from constacyclic codes. Quantum Inf. Process. **17**, 273 (2018). https://doi.org/10.1007/s11128-018-2044-1
4. Fujiwara, Y., Clark, D., Vandendriessche, P., Boeck, M.D., Tonchev, V.D.: Entanglement-assisted quantum low-density parity-check codes. Phys. Rev. A **82**, 042338 (2010)
5. Fan, J., Chen, H., Xu, J.: Construction of q-ary entanglement-assisted quantum MDS codes with minimum distance greater than $q + 1$. Quantum Inf. Comput. **16**(5&6), 0423–0434 (2016)
6. Guenda, K., Jitman, S., Gulliver, T.A.: Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr. **86**(1), 121–136 (2018)
7. Guo, L., Li, R.: Linear Plotkin bound for entanglement-assisted quantum codes. Phys. Rev. A **87**, 032309 (2013)
8. Hsieh, M.H., Devetak, I., Brun, T.A.: General entanglement-assisted quantum error-correcting codes. Phys. Rev. A **76**, 062313 (2007)
9. Hsieh, M.H., Brun, T.A., Devetak, I.: Entanglement-assisted quantum quasi-cyclic low-density parity-check codes. Phys. Rev. A **79**, 032340 (2009)
10. Hsieh, M.H., Yen, W.T., Hsu, L.Y.: High performance entanglement-assisted quantum LDPC codes need little entanglement. IEEE Trans. Inf. Theory **57**(3), 1761–1769 (2011)
11. Krishna, A., Sarwate, D.V.: Pseudo-cyclic maximum-distance separable codes. IEEE Trans. Inf. Theory **36**(4), 880–884 (1990)
12. Koroglu, M.E.: New entanglement-assisted MDS quantum codes from constacyclic codes. Quantum Inf. Process. **18**, 44 (2019). https://doi.org/10.1007/s11128-018-2155-8
13. Kai, X., Zhu, S.: New quantum MDS codes from negacyclic codes. IEEE Trans. Inf. Theory **59**(2), 1193–1197 (2013)
14. Lu, L., Li, R.: Entanglement-assisted quantum codes constructed from primitive quaternary BCH codes. Int. J. Quantum Inf. **12**(03), 1450015 (2014)
15. Liu, Y., Li, R., Lu, L., Ma, Y.: Application of constacyclic codes to entanglement-assisted quantum maximum distance separable codes. Quantum Inf. Process. **17**(210), 1–19 (2018)
16. Lai, C.Y., Brun, T.A.: Entanglement-assisted quantum error-correcting codes with imperfect ebits. Phys. Rev. A **86**, 032319 (2012)
17. Lai, C.Y., Brun, T.A., Wilde, M.M.: Duality in entanglement-assisted quantum error correction. IEEE Trans. Inf. Theory **59**(6), 4020–4024 (2013)
18. Li, R., Li, X., Guo, L.: On entanglement-assisted quantum codes achieving the entanglement-assisted Griesmer bound. Quantum Inf. Process. **14**(12), 4427–4447 (2015)
19. Liu, X., Yu, L., Hu, P.: New entanglement-assisted quantum codes from k-Galois dual codes. Finite Fields Appl. **55**, 21–32 (2019)
20. 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)
21. Lu, L., Li, R., Guo, L., Ma, Y., Liu, Y.: Entanglement-assisted quantum MDS codes from negacyclic codes. Quantum Inf. Process. **17**, 69 (2018). https://doi.org/10.1007/s11128-018-1838-5
22. Liu, Y., Li, R., Lu, L., Ma, Y.: Application of constacyclic codes to entanglement-assisted quantum maximum distance separable codes. Quantum Inf. Process. **17**, 210 (2018). https://doi.org/10.1007/s11128-018-1978-7
23. Luo, G., Cao, X., Chen, X.: MDS codes with arbitrary dimensional hull and their applications. IEEE Trans. Inf. Theory **65**(5), 2944–2952 (2019)
24. Mustafa, S., Emre, K.: An application of constacyclic codes to entanglement-assisted quantum MDS codes. Comput. Appl. Math. **38**(75), 1–13 (2019)
25. Qian, J., Zhang, L.: Entanglement-assisted quantum codes from arbitrary binary linear codes. Des. Codes Cryptogr. **77**(1), 193–202 (2015)
26. Qian, J., Zhang, L.: On MDS linear complementary dual codes and entanglement-assisted quantum codes. Des. Codes Cryptogr. **86**(7), 1565–1572 (2018)
27. Qian, J., Zhang, L.: Constructions of new entanglement-assisted quantum MDS and almost MDS codes. Quantum Inf. Process. **18**, 71 (2019). https://doi.org/10.1007/s11128-019-2197-6
28. Shin, J., Heo, J., Brun, T.A.: Entanglement-assisted codeword stabilized quantum codes. Phys. Rev. A **84**, 062321 (2011)
29. Wilde, M.M., Brun, T.A.: Optimal entanglement formulas for entanglement-assisted quantum coding. Phys. Rev. A **77**, 064302 (2008)

30. Wang, J., Li, R., Lv, J., Guo, G., Liu, Y.: Entanglement-assisted quantum error correction codes with length $n = q^2 + 1$. Quantum Inf. Process. **18**, 292 (2019). https://doi.org/10.1007/s11128-019-2409-0

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