Quantum Information Processing (2018) 17:210
https://doi.org/10.1007/s11128-018-1978-7

Application of constacyclic codes to entanglement-assisted quantum maximum distance separable codes

Yang Liu[1] · Ruihu Li[1] · Liangdong Lv[1] · Yuena Ma[1]

Received: 8 February 2018 / Accepted: 7 July 2018 / Published online: 14 July 2018

Abstract

The entanglement-assisted stabilizer formalism overcomes the dual-containing constraint of standard stabilizer formalism for constructing quantum codes. This allows ones to construct entanglement-assisted quantum error-correcting codes (EAQECCs) from arbitrary linear codes by pre-shared entanglement between the sender and the receiver. However, it is not easy to determine the number c of pre-shared entanglement pairs required to construct an EAQECC from arbitrary linear codes. In this paper, let q be a prime power, we aim to construct new q-ary EAQECCs from constacyclic codes. Firstly, we define the decomposition of the defining set of constacyclic codes, which transforms the problem of determining the number c into determining a subset of the defining set of underlying constacyclic codes. Secondly, five families of non-Hermitian dual-containing constacyclic codes are discussed. Hence, many entanglement-assisted quantum maximum distance separable codes with $c \leq 7$ are constructed from them, including ones with minimum distance $d \geq q + 1$. Most of these codes are new, and some of them have better performance than ones obtained in the literature.

Keywords Entanglement-assisted quantum code · Constacyclic code · Defining set · Quantum MDS code

This work is supported by the National Natural Science Foundation of China under Grant No. 11471011 and Natural Science Foundation of Shaanxi province under Grant No. 2017JQ1032..

✉ Ruihu Li
llzsy2015@163.com

Yang Liu
liu_yang10@163.com

Liangdong Lv
lvliangdong_kgd@163.com

Yuena Ma
mayuena2013@163.com

1 Department of Basic Sciences, Air Force Engineering University, Xi'an 710051, Shaanxi, People's Republic of China

1 Introduction

Quantum codes are applied to reduce decoherence in quantum computation and quantum communication. The quantum stabilizer formalism allows constructing quantum codes from "dual-containing" or "self-orthogonal" classical linear codes, see [1–4]. Then, a great deal of good quantum codes have been obtained. However, owing to the limitation of the dual-containing condition for underlying classical codes, many classical codes with good performance cannot be used to construct quantum stabilizer codes.

Bowen found that pre-shared entangled states between the sender and the receiver can increase both quantum and classical capacity for communication [5]. Based on this, Brun et al. [6] proposed an entanglement-assisted stabilizer formalism, which avoids the dual-containing constraint and allows ones to construct EAQECCs from arbitrary classical linear codes. Here, an EAQECC can be denoted by $[[n, k, d; c]]_q$, which encodes k information qubits into n channel qubits with the help of c pairs of maximally entangled states and corrects up to $\lfloor \frac{d-1}{2} \rfloor$ errors, where d is the minimum distance of the code.

EA-quantum Singleton bound of EAQECCs was proposed at first in [6]. Recently, it was pointed to be incomplete and some examples of EAQECCs beating the bound were presented [7]. In fact, this bound holds if $d \leq \frac{n+2}{2}$ [8], which can be specifically given below.

Proposition 1 *([6–8] EA-quantum Singleton bound) Suppose that* $d \leq \frac{n+2}{2}$. *An EAQECC* $[[n, k, d; c]]_q$ *satisfies* $n + c - k \geq 2(d - 1)$. *Particularly, if* $c = 0$, *then* $n - k \geq 2(d - 1)$.

When $d \leq \frac{n+2}{2}$, an $[[n, k, d; c]]_q$ EAQECC achieving $n + c - k = 2(d - 1)$ is called an EAQMDS code. It is called a standard QMDS code when $c = 0$.

There have been many papers on the construction of quantum MDS codes (see Refs. [9–22] and the references therein). However, it is not an easy task to construct QMDS codes with large distance. For $n = q^2 + 1$, q^2, $q^2 - 1$, $(q^2 + 1)/2$ and $(q^2 - 1)/2$, there are QMDS codes with $d \geq q$. Except for these five classes of code lengths, it is very hard to construct QMDS codes with $d \geq q/2$, see [15,17,18,21]. Since the entanglement can increase the error-correcting ability of quantum codes [23], it is natural to consider constructing EAQMDS codes with large distance. In the latest years, some EAQMDS codes of minimum distance greater than $q+1$ were increasingly obtained. Lai and Brun presented EAQMDS codes $[[7, 1, 5; 2]]_2$, $[[9, 1, 7; 4]]_2$ and $[[n, 1, n; n-1]]_2$ with n odd in [23,24]. An infinite class of EAQMDS codes based on quaternary linear codes were constructed by Li et al. [25]. Applying Reed–Solomon codes and constacyclic codes, Fan et al. [26] obtained five classes of EAQMDS codes with the help of a few shared entanglement states. Chen et al. [27] derived four families of EAQMDS codes from negacyclic codes by 4 or 5 pre-shared entanglement states. Guenda et al. [28] provided the construction of EAQMDS codes based on the dimension of the Hermitian hull of generalized Reed–Solomon codes.

Motivated by these previous results, we construct some new EAQMDS codes from constacyclic codes of lengths $n = \frac{q+1}{r}(q - 1)$ for $r = 3, 4, 5, 6, 7$ and $q \equiv -1 \bmod r$. The paper is organized as follows. In Sect. 2, basic concepts on η-constacyclic codes, q^2-cyclotomic cosets and EAQMDS codes are reviewed. We will generalize the decomposition of the defining set of cyclic codes in [29] and negacyclic codes in [27] to η-constacyclic codes. In Sects. 3 and 4, five families of EAQMDS codes are obtained. In Sect. 5, we conclude the paper.

2 Preliminaries

In this section, we will review some relevant concepts on η-constacyclic codes, q^2-cyclotomic cosets, EAQECCs and EAQMDS codes. For more details, one can refer to Refs. [6,25,30–32].

2.1 A review of η-constacyclic codes

For a given prime power q, let $\mathbb{F}_{q^2}$ be the finite field with q^2 elements and $\mathbb{F}_{q^2}^n$ be the n-dimensional vector space over $\mathbb{F}_{q^2}$. Denote $\mathbb{F}_{q^2}^*$ as the multiplicative group of nonzero elements of $\mathbb{F}_{q^2}$. Suppose that e is the identity of $\mathbb{F}_{q^2}^*$ and $\alpha \in \mathbb{F}_{q^2}^*$. The order of α is defined by the smallest positive integer r such that $\alpha^r = e$. Here, α is called a primitive r-th root of unity in $\mathbb{F}_{q^2}^*$ and a conjugation of α is denoted by $\overline{\alpha} = \alpha^q$.

Given two vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_{q^2}^n$, their Hermitian inner product is defined as

$$(\mathbf{x}, \mathbf{y})_h = \sum_{i=1}^{n} \overline{x_i} y_i = \overline{x_1} y_1 + \overline{x_2} y_2 + \cdots + \overline{x_n} y_n.$$

For a linear code $\mathcal{C}$ over $\mathbb{F}_{q^2}$ of length n, the Hermitian dual code of $\mathcal{C}$ is denoted by $\mathcal{C}^{\perp_h}$, where

$$\mathcal{C}^{\perp_h} = \{\mathbf{x} \in \mathbb{F}_{q^2}^n \mid (\mathbf{x}, \mathbf{y})_h = 0, \forall \mathbf{y} \in \mathcal{C}\}.$$

If $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$, then $\mathcal{C}$ is called a Hermitian dual-containing code, while $\mathcal{C}^{\perp_h}$ is called a Hermitian self-orthogonal code.

Let η be a primitive r-th root of unity in $\mathbb{F}_{q^2}^*$. A q^2-ary linear code $\mathcal{C}$ of length n is called η-**constacyclic** if $(\eta c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$ whenever $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$. If $\eta = 1$, then $\mathcal{C}$ is a cyclic code; $\mathcal{C}$ is a negacyclic code when $\eta = -1$. For an η-constacyclic code $\mathcal{C}$, each codeword $c = (c_0, c_1, \ldots, c_{n-1})$ is customarily represented in its polynomial form: $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$, and the code $\mathcal{C}$ is in turn identified with an ideal of the quotient ring $\mathcal{R}_n = \mathbb{F}_q[x]/(x^n - \eta)$. It follows that $\mathcal{C}$ is generated by a monic factor of $x^n - \eta$, i.e., $\mathcal{C} = \langle g(x) \rangle$ with $g(x)|(x^n - \eta)$. The polynomial $g(x)$ is called the generator polynomial of $\mathcal{C}$.

Let $\gcd(n, q) = 1$ and η be a primitive r-th root of unity. Then, there exists a primitive rn-th root ζ of unity in some extension field of $\mathbb{F}_{q^2}$ such that $\zeta^n = \eta$. Let $\xi = \zeta^r$. Then, ξ is a primitive n-th root of unity. It follows that the roots of $x^n - \eta$ are $\zeta \xi^j = \zeta^{1+jr}$ for $0 \le j \le n-1$.

For convenience, we denote a set Ω by

$$\Omega=\Omega_{r,n}=\{i=1+jr|0\leq j\leq n-1\}.$$

The defining set of an η-constacyclic code $\mathcal{C}=\langle g(x)\rangle$ of length n is defined by

$$T=\{i\in\Omega\mid g(\zeta^i)=0\}.$$

It is well known that there is a close relation between cyclotomic cosets and constacyclic codes [14,17,30,33–35].

The q^2-*cyclotomic coset* modulo rn containing i is defined by

$$C_i=\{i,iq^2,i(q^2)^2,...,i(q^2)^{k-1}\} \bmod rn,$$

where $i\in\Omega$ and k is the smallest positive integer such that $(q^2)^k i\equiv i \bmod rn$. It is easy to know that the defining set T of an η-constacyclic code is a union of some q^2-cyclotomic cosets modulo rn (see [14,17]).

To study the properties of q^2-ary cyclotomic cosets modulo rn, we first give some useful definitions introduced in [33,35]. For each $i\in\Omega$, C_i is called *skew symmetric* if $-qi \pmod{rn}\in C_i$, and **skew asymmetric**, otherwise. Skew asymmetric cosets C_i and C_{-qi} come in pair, and we use (C_i, C_{-qi}) to denote such a *skew asymmetric pair* (SAP, for short).

For an η-constacyclic code $\mathcal{C}$ and its Hermitian dual $\mathcal{C}^{\perp_h}$, some known results about the generator polynomial and the defining set are summarized in the following Lemmas 1 and 2 (see [14,17,33]).

Lemma 1 *Let $\mathcal{C}=\langle g(x)\rangle$ be an η-constacyclic code of length n over $\mathbb{F}_{q^2}$ and T be its defining set. Suppose that $h(x)=\frac{x^n-\eta}{g(x)}=h_0+h_1x+\cdots+h_kx^k$, then*

(1) $\mathcal{C}^{\perp_h}=\langle u(x)\rangle$ is an $\overline{\eta}^{-1}$-constacyclic code with

$$u(x)=h_0^{-q}\sum_{i=0}^{k}h_i^q x^{k-i}=h_0^{-q}x^k\sum_{i=0}^{k}h_i^q x^{-i}=h_0^{-q}\overline{\widetilde{h(x)}},$$

where $\widetilde{h(x)}=x^kh(\frac{1}{x})$ is the polynomial $h(x)$ with reversed coefficients and $\overline{f(x)}=\sum f_i^q x^i$ for $f(x)=\sum f_ix^i$.

(2) If $r|q+1$, then $\mathcal{C}^{\perp_h}$ is also η-constacyclic. Moreover, $\mathcal{C}^{\perp_h}$ has defining set $T^{\perp_h}=\Omega\backslash T^{-q}$, where $T^{-q}=-qT=\{-jq\in\Omega|j\in T\}$.

For convenience to give our discussions in the sequel, it is necessary to first present Notation 1 below.

Notation 1 Let q be a prime power. To make sure the Hermitian dual code of an η-constacyclic code is also η-constacyclic, i.e., $\eta=\overline{\eta}^{-1}$, the order r of η in $\mathbb{F}_{q^2}^*$ will be always chosen to be a divisor of $q+1$ by Lemma 1. Hence, we can set $q=rl-1$, where l is a proper integer such that q is a prime power. According to Proposition 1, we always set $d\leq\frac{n+2}{2}$ when constructing EAQMDS codes with parameters $[[n,k,d;c]]_q$.

Lemma 2 *If $\mathcal{C}$ is an η-constacyclic code of length n with defining set T, then $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$ if and only if one of the following idems holds:*

(1) $T \cap T^{-q} = \emptyset$;
(2) each C_i in T is skew asymmetric and any two cosets in T cannot form a SAP.

Similar to cyclic codes, there also exists the BCH bound for η-constacyclic codes as follows.

Lemma 3 *(The BCH bound for constacyclic codes [9,36]) Suppose that $\mathcal{C}$ is an η-constacyclic code with the generator polynomial $g(x)$ of length n over $\mathbb{F}_{q^2}$, where η is a primitive r-th root of unity. Let ζ be an rn-th primitive root of unity in an extension field of $\mathbb{F}_{q^2}$. If the roots of $g(x)$ include the set $\{\zeta^{1+ri} | i_1 \leq i \leq i_1 + \delta - 2, i_1$ is an arbitrary integer$\}$, then the minimum distance of $\mathcal{C}$ is at least δ.*

2.2 The decomposition of the defining set of η-constacyclic codes

According to [37,38], EAQECCs can be constructed from arbitrary linear codes over $\mathbb{F}_{q^2}$, which can be given by the following proposition.

Proposition 2 *Let $\mathcal{C}$ be an $[n, k, d]_{q^2}$ linear code with parity check matrix H. If $c = rank(HH^\dagger)$ where $H^\dagger$ is the conjugate transpose of H, then there exists an $[[n, 2k - n + c, d; c]]$ EAQECC.*

For general linear codes $\mathcal{C}$, it is not easy to calculate c in Proposition 2. However, c can be easily determined for some special classes of linear codes [27,29,39]. In [29], the decomposition of the defining set of cyclic codes was initially introduced. Using the technique, the problem of determining c can be reduced to determine some special subset of T, where T is the defining set of a cyclic code $\mathcal{C}$.

For constructing more EAQMDS codes, the decomposition of the defining set of negacyclic codes was further developed by [27]. Notice that some EAQECCs with good parameters cannot be constructed from cyclic codes or negacyclic codes. Below we generalize the decomposition of the defining set of cyclic (negacyclic) codes to η-constacyclic codes.

Definition 1 Let T be the defining set of an η-constacyclic code $\mathcal{C}$ over $\mathbb{F}_{q^2}$. Denote $T_{ss} = T \bigcap T^{-q}$ and $T_{sas} = T \backslash T_{ss}$. Then, $T = T_{ss} \bigcup T_{sas}$ is called the decomposition of the defining set T.

Remark 1 From the following lemma, it is easy to know that $T \bigcap T^{-q}$ contains all the skew symmetric (for short, "**ss**") cosets and SAPs. Whereas the cyclotomic cosets in $T \backslash (T \bigcap T^{-q})$ are all skew asymmetric (for short,"**sas**"). Moreover, there is no SAP in $T \backslash (T \bigcap T^{-q})$. Hence, "$T_{ss}$" and "$T_{sas}$" are adopted to denote $T \bigcap T^{-q}$ and $T \backslash (T \bigcap T^{-q})$ in Definition 1, respectively.

Lemma 4 *Let $\mathcal{C}$ be an η-constacyclic code over $\mathbb{F}_{q^2}$ with defining set T. Suppose that $T = T_{ss} \bigcup T_{sas}$ is the decomposition of the defining set T.*

(1) If $i \in T$, then $i \in T_{sas}$ if and only if C_i is skew asymmetric and there is no integer $j \in T$ such that (C_i, C_j) is a SAP.

$$T_{ss} = \bigcup_{i, j_1, j_2 \in T} C_i \bigcup \left(C_{j_1} \bigcup C_{j_2}\right),$$

where C_i is skew symmetric and (C_{j_1}, C_{j_2}) is a SAP.

(2) $T_{sas} \bigcap T_{sas}^{-q} = \emptyset$ and $T_{ss} = T_{ss}^{-q} = T_{ss} \bigcap T_{ss}^{-q}$.

(3) Let the defining sets of two η-constacyclic codes $\mathcal{C}_1$ and $\mathcal{C}_2$ be T_{sas} and T_{ss}, respectively. Then $\mathcal{C}_1^{\perp_h} \subseteq \mathcal{C}_1$, $\mathcal{C}_2^{\perp_h} \bigcap \mathcal{C}_2 = \{\mathbf{0}\}$, $\mathcal{C}_1 \bigcap \mathcal{C}_2 = \mathcal{C}$ and $\mathcal{C}_1^{\perp_h} + \mathcal{C}_2^{\perp_h} = \mathcal{C}^{\perp_h}$.

Proof(1): From Definition 1, we split into two cases as follows.

Case 1: When $C_x \subseteq T$ is skew symmetric. Let $i = x$ and $C_i \subseteq T$.
In this case, by the definition of skew symmetric cyclotomic cosets, we know that $C_{-qi} = C_i$. It immediately follows that $C_i \subseteq T^{-q}$, then we have $C_i \subseteq T \bigcap T^{-q} = T_{ss}$.

Case 2: When $C_x \subseteq T$ is skew asymmetric. Let $j_1 = x$ and $C_{j_1} \subseteq T$.

Subcase 2.1: There exists $j_2 \in T$ such that (C_{j_1}, C_{j_2}) is a SAP.
In this subcase, , we have $C_{-qj_1} = C_{j_2}$ by the definition of a SAP, then $C_{j_2} \subseteq T^{-q}$. From $j_2 \subseteq T$, we can similarly derive that $C_{j_2} \subseteq T$ and $C_{j_1} \subseteq T^{-q}$. As thus, we can easily infer that $C_{j_1} \bigcup C_{j_2} \subseteq T \bigcap T^{-q} = T_{ss}$.

Subcase 2.2: There is no integer $j_2 \in T$ such that (C_{j_1}, C_{j_2}) is a SAP.
In this subcase, $C_{j_1} \nsubseteq T^{-q}$. Hence we have $C_{j_1} \subseteq T_{sas}$.
Concluding the above two cases, then (1) follows.

(2): Assume that $T_{sas} \bigcap T_{sas}^{-q} \neq \emptyset$. Let $i \in T_{sas} \bigcap T_{sas}^{-q}$, then $i \in T \bigcap T^{-q} = T_{ss}$. This yields a contradiction, which implies $T_{sas} \bigcap T_{sas}^{-q} = \emptyset$. We then proceed to verify the rest of (2).
$T_{ss} \bigcap T_{ss}^{-q} = (T \bigcap T^{-q}) \bigcap (T^{-q} \bigcap T) = T \bigcap T^{-q} = T_{ss} = T_{ss}^{-q}$.

(3): (3.1). According to (2), we know that $T_{sas} \bigcap T_{sas}^{-q} = \emptyset$. It naturally follows from Lemma 2 that $\mathcal{C}_1^{\perp_h} \subseteq \mathcal{C}_1$.

(3.2). From (2), we know that $T_{ss} = T_{ss}^{-q}$, then the defining set of $\mathcal{C}_2^{\perp_h} \bigcap \mathcal{C}_2$ is

$$T_{ss}^{\perp h} \cup T_{ss} = (\Omega \backslash T_{ss}^{-q}) \bigcup T_{ss} = \Omega,$$

which implies that $\mathcal{C}_2^{\perp_h} \bigcap \mathcal{C}_2 = \{\mathbf{0}\}$.

(3.3). Since the defining set of $\mathcal{C}_1 \bigcap \mathcal{C}_2$ is $T_{sas} \bigcup T_{ss} = T$, we have $\mathcal{C}_1 \bigcap \mathcal{C}_2 = \mathcal{C}$.

(3.4). Notice that the defining set of $\mathcal{C}_1^{\perp_h} + \mathcal{C}_2^{\perp_h}$ is

$$T_{sas}^{\perp h} \bigcap T_{ss}^{\perp h} = (\Omega \backslash T_{sas}^{-q}) \bigcap (\Omega \backslash T_{ss}^{-q}) = \Omega \backslash \left(T_{sas}^{-q} \bigcup T_{ss}^{-q}\right) = \Omega \backslash T^{-q} = T^{\perp_h}.$$

We then get $\mathcal{C}_1^{\perp_h} + \mathcal{C}_2^{\perp_h} = \mathcal{C}^{\perp_h}$ since $T^{\perp_h}$ is the defining set of $\mathcal{C}^{\perp_h}$.
Concluding the above discussions, (3) follows.

□

According to Lemma 4, the following theorem can be proved.

Theorem 1 *Let $\mathcal{C}$ be an η-constacyclic code over $\mathbb{F}_{q^2}$ with defining set T. Suppose that $T = T_{ss} \bigcup T_{sas}$ is the decomposition of the defining set T. If $\mathcal{C}$ has parameters $[n, k = n - |T|, d]_{q^2}$, then there exist EAQECCs with parameters $[[n, n - 2|T| + |T_{ss}|, d; |T_{ss}|]]_q$.*

Proof Let T_{sas} and T_{ss} be the defining sets of two η-constacyclic codes $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Suppose that their parity check matrices are H_1 and H_2, respectively. From (3) in Lemma 4, one can deduce that a parity check matrix H of $\mathcal{C}$ can be given by

$$H = \begin{pmatrix} H_1 \\ H_2 \end{pmatrix}.$$

Since $T_{ss} \bigcap T_{sas} = \emptyset$, we can easily check that $T_{ss}^{\perp_h} \supseteq T_{sas}$. Hence, $\mathcal{C}_2^{\perp_h} \subseteq \mathcal{C}_1$ and $H_1 H_2^\dagger = \mathbf{0}$, $H_2 H_1^\dagger = \mathbf{0}$. According to $\mathcal{C}_1^{\perp_h} \subseteq \mathcal{C}_1$, we have $H_1 H_1^\dagger = \mathbf{0}$. Thus, we can obtain that

$$HH^\dagger = \begin{pmatrix} H_1 \\ H_2 \end{pmatrix} (H_1^\dagger H_2^\dagger) = \begin{pmatrix} H_1 H_1^\dagger & H_1 H_2^\dagger \\ H_2 H_1^\dagger & H_2 H_2^\dagger \end{pmatrix} = \begin{pmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & H_2 H_2^\dagger \end{pmatrix}$$

Then, we have $\text{rank}(HH^\dagger) = \text{rank}(H_2 H_2^\dagger)$. From $\mathcal{C}_2^{\perp_h} \bigcap \mathcal{C}_2 = \{0\}$, it follows that $\text{rank}(H_2 H_2^\dagger) = |T_{ss}|$. Combining Proposition 2, the desired conclusion can be derived.

□

Compared with Refs. [27,29], the research scope is extended from cyclic and negacyclic codes to general η-constacyclic codes. In addition, in (1) of Lemma 4, we deeply study which cyclotomic cosets modulo rn are contained in T_{ss} and T_{sas}, respectively. It makes it relatively easy to determine $|T_{ss}|$. We also detailedly prove the Hermitian dual properties of $\mathcal{C}$, $\mathcal{C}_1$ and $\mathcal{C}_2$ and investigate the relationships among them in (3) of Lemma 4. This is the key step to show Theorem 1.

The following theorem is much useful to discuss the decomposition of the definition set of η-constacyclic codes with length $n = \frac{q+1}{r}(q-1)$ in the following sections.

Theorem 2 *Suppose that $\mathcal{C}$ is an η-constacyclic code of length $n = \frac{q+1}{r}(q-1)$. Let C_i be the q^2-cyclotomic coset modulo rn containing i and $\Omega = \{1 + jr | 0 \leq j \leq n-1\}$, then the following holds.*

(1) For each $i \in \Omega$, $C_i = \{i\}$.
(2) If $i \in \Omega$, then C_i is skew symmetric if and only if $1 + jr \equiv 0 \bmod q-1$.
(3) For a given integer $i_2 \in \Omega$, i_2 can be denoted by $i_2 = \alpha q - \beta$ for two proper integers $1 \leq \alpha, \beta \leq q$. Then, there exists an integer $i_1 \in \Omega$ such that (C_{i_1}, C_{i_2}) is a SAP if and only if $i_1 = \beta q - \alpha$.

Proof (1) From $rn = q^2 - 1$, we know that $iq^2 \equiv i \bmod rn$. It follows directly that $C_i = \{i\}$.

(2) According to the skew symmetric properties of cyclotomic cosets modulo rn, $C_{i=1+jr}$ is skew symmetric if and only if $(1 + rj)(q + 1) \equiv 0 \bmod rn$, which is equivalent to $1 + rj \equiv 0 \bmod q - 1$. Hence, (2) holds.

(3) Note that $\Omega = \{i = 1 + jr | 0 \leq j \leq n - 1\}$. For a given integer $i_2 \in \Omega$, we have $1 \leq i_2 \leq q^2 - r$. If $1 \leq \alpha, \beta \leq q$, then there exists a unique integers pair (α, β) such that $i_2 = \alpha q - \beta$ since $\alpha q - \beta$ runs through all the integers in the set $\{0, 1, 2, \ldots, q^2 - 1\}$. For simplifying the following discussions, here we adopt the representation $i_2 = \alpha q - \beta$.

Since $C_i = \{i\}$ and $C_{-iq} = \{-iq \bmod rn\}$ form a SAP, (C_{i_1}, C_{i_2}) is a SAP if and only if $i_1 + i_2 q \equiv 0 \bmod q^2 - 1$. When i_2 is denoted by $i_2 = \alpha q - \beta$ $(1 \leq \alpha, \beta \leq q)$, then $i_1 + i_2 q \equiv 0 \bmod q^2 - 1 \Leftrightarrow i_1 + (\alpha q - \beta)q \equiv i_1 + \alpha - \beta q \equiv 0 \bmod q^2 - 1$, i.e.,

$$i_1 + \alpha - \beta q \equiv 0 \bmod q^2 - 1. \tag{1}$$

Moreover, by $i_2 \in \Omega$, we have $\alpha q - \beta \equiv 1 \bmod r$. It follows from $r | q + 1$ that $(\alpha q - \beta) - (\alpha - \beta)(q + 1) = \beta q - \alpha \equiv 1 \bmod r$, then

$$\beta q - \alpha \in \Omega. \tag{2}$$

Notice that

$$i_1 < q^2 - 1. \tag{3}$$

Combining the above expressions (1)–(3), it is easy to derive that there exists an integer $i_1 \in \Omega$ such that (C_{i_1}, C_{i_2}) is a SAP if and only if $i_1 = \beta q - \alpha$. □

3 New EAQMDS codes of length $n = \frac{q+1}{r}(q - 1)$ with $r = 3, 5, 7$

For a given $r = 3, 5$ or 7, let $n = \frac{q+1}{r}(q - 1)$. It was shown in [16,17] that there are $[[n, n - 2d + 2, d]]_q$ standard QMDS codes for $2 \leq d \leq \frac{(q+1)(r+1)}{2r} - 1$. Ref. [26] obtained $[[n, n - 2d + 2 + r, d; r]]_q$ EAQMDS codes for $\frac{(q+1)(r-1)}{r} + 2 \leq d \leq \frac{(q+1)(r+1)}{r} - 2$. In this section, we will discuss constructions of new $[[n, n - 2d + 2 + c, d; c]]_q$ EAQMDS codes with $1 \leq c \leq r$ and $d > \frac{(q+1)(r+1)}{2r} - 1$. Our results are presented in three subsections according to different $r = 3, 5, 7$, respectively.

3.1 New EAQMDS codes of length $n = \frac{q+1}{3}(q - 1)$

In this subsection, let $r = 3$, $q = 3l - 1 \geq 8$ and $n = \frac{q+1}{3}(q - 1)$.

Lemma 5 *Let* $T = \{i = 1 + 3j \mid 0 \leq j \leq \frac{4(q-2)}{3}\}$. *Then*

(1) C_{q-1} *is skew symmetric and* C_i *is skew asymmetric if* $i \in T \backslash \{q - 1\}$.

(2) There is only one SAP (C_{3q-2}, C_{2q-3}) in T.

Proof(1): According to Theorem 2, C_i is skew symmetric if and only if $1+3j \equiv 0 \bmod q-1$, i.e., $j \equiv \frac{q-2}{3} \bmod q-1$. From $j \in [0, \frac{4(q-2)}{3}]$, it naturally follows that $j = \frac{q-2}{3}$, which implies that there is only one skew symmetric coset C_{q-1} in T. Hence, (1) holds.

(2): Given two integers $i_1 < i_2 \in T$, we have $1 \leq i_1 < i_2 \leq 4q-7$. Let $i_2 = \alpha q - \beta$ for two proper integers $1 \leq \alpha, \beta \leq q$. Applying Theorem 2, (C_{i_1}, C_{i_2}) is a SAP if and only if $i_1 = \beta q - \alpha$.

Since $q \geq 8$, $1 \leq i_2 \leq 4q-7$ and $i_2 = \alpha q - \beta$, we can infer that

$$1 \leq \alpha \leq 4. \tag{4}$$

From $i_1 = \beta q - \alpha < \alpha q - \beta = i_2$, we derive that

$$1 \leq \beta < \alpha. \tag{5}$$

Combining the above inequations (4) and (5), we can easily derive that $1 \leq \beta < \alpha \leq 4$. Assume that $\alpha = 4$ and $\beta < \alpha$, then $\alpha q - \beta = 4q - \beta > 4q - 4 \notin T$. As thus, we can further get that

$$1 \leq \beta < \alpha \leq 3. \tag{6}$$

Solving the inequation (6), then $(\alpha, \beta) = (2, 1), (3, 1)$ or $(3, 2)$, i.e., $i_2 = 2q-1, 3q-1$ or $3q-2$. From $q = 3l-1$, it can be obtained that there is only $i_2 = 3q-2$ such that $i_2 \equiv 1 \bmod 3 \in T$, which implies that there is only one SAP (C_{3q-2}, C_{2q-3}) in T. This completes the proof. □

Consider the following sets:
$T_0(\delta) = \{i = 1+3j | q-\delta \leq j \leq q-2\}$ for $2 \leq \delta \leq \frac{2(q+1)}{3} - 1$,
$T_1(\delta) = \{i = 1+3j | q-\delta \leq j \leq q-2\}$ for $\frac{2(q+1)}{3} \leq \delta \leq q$,
$T_3(\delta) = \{i = 1+3j | 0 \leq j \leq \delta-2\}$ for $q+1 \leq \delta \leq \frac{4(q+1)}{3} - 2$.
From Lemma 5, we can derive the following corollary.

Corollary 3 *Let $T_i(\delta)$ for $i = 0, 1, 3$ be given as above.*

(1) If $2 \leq \delta \leq \frac{2(q+1)}{3} - 1$, then $T_0(\delta)_{ss} = T_0(\delta) \bigcap T_0(\delta)^{-q} = \emptyset$;
(2) If $\frac{2(q+1)}{3} \leq \delta \leq q$, then $T_1(\delta)_{ss} = T_1(\delta) \bigcap T_1(\delta)^{-q} = \{q-1\}$;
(3) If $q+1 \leq \delta \leq \frac{4(q+1)}{3} - 2$, then $T_3(\delta)_{ss} = T_3(\delta) \bigcap T_3(\delta)^{-q} = \{q-1, 2q-3, 3q-2\}$.

Proof According to Lemmas 4 and 5, to determine $T_i(\delta)$, we only need to analyze which ones of C_{q-1}, C_{2q-3} and C_{3q-2} are contained in $T_i(\delta)$ for $i = 0, 1, 3$.

(1): When $2 \leq \delta \leq \frac{2(q+1)}{3} - 1$, it is easy to know that $C_{q-1} \nsubseteq T_0(\delta)$, $C_{2q-3} \subseteq T_0(\delta)$ and $C_{3q-2} \nsubseteq T_0(\delta)$. From (1) of Lemma 4, we get that $T_0(\delta) \bigcap T_0(\delta)^{-q} = \emptyset$.

(2): When $\frac{2(q+1)}{3} \le \delta \le q$, we derive that $C_{q-1} \subseteq T_1(\delta)$, $C_{2q-3} \subseteq T_1(\delta)$ and $C_{3q-2} \nsubseteq T_1(\delta)$. It follows from (1) of Lemma 4 that $T_1(\delta) \bigcap T_1(\delta)^{-q} = \{q-1\}$.

(3): When $q+1 \le \delta \le \frac{4(q+1)}{3} - 2$, we have $C_{q-1} \subseteq T_3(\delta)$, $C_{2q-3} \subseteq T_3(\delta)$ and $C_{3q-2} \subseteq T_3(\delta)$. We shall similarly verify that $T_3(\delta) \bigcap T_3(\delta)^{-q} = \{q-1, 2q-3, 3q-2\}$. □

Theorem 4 *Suppose that* $n = \frac{q+1}{3}(q-1)$. *Set* $\delta \le \frac{n+2}{2}$, *then there exist EAQMDS codes with parameters*

$$\begin{cases} [[n, n-2\delta+3, \delta; 1]]_q & \text{if } \frac{2(q+1)}{3} \le \delta \le q; \\ [[n, n-2\delta+5, \delta; 3]]_q & \text{if } q+1 \le \delta \le \frac{4(q+1)}{3} - 2. \end{cases}$$

Proof (1) If $\frac{2(q+1)}{3} \le \delta \le q$, let $\mathcal{C}$ be an η-constacyclic code over $\mathbb{F}_{q^2}$ with defining set $T_1(\delta)$, where $T_1(\delta)$ is given as above. We can easily know that there are $\delta - 1$ consecutive integers in $T_1(\delta)$. According to Lemma 3, the minimum distance of $\mathcal{C}$ is at least δ. Since $C_i = \{i\}$ by Theorem 2, we have $|T_1(\delta)| = \delta - 1$. Notice that $|T_1(\delta)_{ss}| = 1$ from Corollary 3. Applying Theorem 1 and Proposition 1, if follows immediately that there exist EAQMDS codes with parameters $[[n, n-2\delta+3, \delta; 1]]_q$.

(2) When $q+1 \le \delta \le \frac{4(q-2)}{3} - 2$, let the defining set of $\mathcal{C}$ be $T_3(\delta)$. Similar to (1), applying Theorem 1 to $\mathcal{C}$, we shall derive that there exist EAQMDS codes with parameters $[[n, n-2\delta+5, \delta; 3]]_q$.

In the following two subsections and Sect. 4, the similar conclusions can be derived by the corresponding results in Sect. 3.1 combining Theorems 1 and 2. For conciseness and clarity, we only present main results and omit some similar proofs.

3.2 New EAQMDS codes of length $n = \frac{q+1}{5}(q-1)$

In this subsection, let $r = 5$, $q = 5l - 1 \ge 9$ and $n = \frac{q+1}{5}(q-1)$.

Lemma 6 *Let* $T = \{i = 1 + 5j \mid 0 \le j \le \frac{6(q+1)}{5} - 3\}$. *Then:*

(1) $C_{2(q-1)}$ *is skew symmetric and* C_i *is skew asymmetric if* $i \in T \backslash \{2(q-1)\}$.
(2) There are only two SAPs (C_{3q-1}, C_{q-3}) *and* (C_{4q-5}, C_{5q-4}) *in* T.

Proof According to Theorem 2, we can obtain the desired conclusion in a similar way to the proof of Lemma 5. □

Consider the following sets:
$T_0(\delta) = \{i = 1 + 5j | q - \delta \le j \le q - 2\}$ for $2 \le \delta \le \frac{3(q+1)}{5} - 1$,
$T_1(\delta) = \{i = 1 + 5j | q - \delta \le j \le q - 2\}$ for $\frac{3(q+1)}{5} \le \delta \le \frac{4(q+1)}{5} - 1$,
$T_3(\delta) = \{i = 1 + 5j | q - \delta \le j \le q - 2\}$ for $\frac{4(q+1)}{5} \le \delta \le q$,
$T_5(\delta) = \{i = 1 + 5j | 0 \le j \le \delta - 2\}$ for $q + 1 \le \delta \le \frac{6(q+1)}{5} - 1$.
From Lemma 6, we can get the following corollary.

Corollary 5 *Let $T_i(\delta)$ for $i = 0, 1, 3, 5$ be given as above.*

(1) If $2 \leq \delta \leq \frac{3(q+1)}{5} - 1$, then $T_0(\delta)_{ss} = T_0(\delta) \bigcap T_0(\delta)^{-q} = \emptyset$.
(2) If $\frac{3(q+1)}{5} \leq \delta \leq \frac{4(q+1)}{5} - 1$, then $T_1(\delta)_{ss} = T_1(\delta) \bigcap T_1(\delta)^{-q} = \{2q-2\}$.
(3) If $\frac{4(q+1)}{5} \leq \delta \leq q$, then $T_3(\delta)_{ss} = T_3(\delta) \bigcap T_3(\delta)^{-q} = \{q-3, 2(q-1), 3q-1\}$.
(4) If $q+1 \leq \delta \leq \frac{6(q+1)}{5} - 1$, then $T_5(\delta)_{ss} = \{q-3, 2(q-1), 3q-1, 4q-5, 5q-4\}$.

By Corollary 5, the following theorem can be derived in a similar way to the proof of Theorem 4.

Theorem 6 *Suppose that $n = \frac{q+1}{5}(q-1)$. Set $\delta \leq \frac{n+2}{2}$, then there exist EAQMDS codes with parameters*

$$\begin{cases} [[n, n-2\delta+3, \delta; 1]]_q & \text{if} \quad \frac{3(q+1)}{5} \leq \delta \leq \frac{4(q+1)}{5} - 1; \\ [[n, n-2\delta+5, \delta; 3]]_q & \text{if} \quad \frac{4(q+1)}{5} \leq \delta \leq q; \\ [[n, n-2\delta+7, \delta; 5]]_q & \text{if} \quad q+1 \leq \delta \leq \frac{6(q+1)}{5} - 1. \end{cases}$$

3.3 New EAQMDS codes of length $n = \frac{q+1}{7}(q-1)$

In this subsection, let $r = 7$, $q = 7l - 1 \geq 13$ and $n = \frac{q+1}{7}(q-1)$.

Lemma 7 *Let $T = \{i = 1 + 7j, 0 \leq j \leq \frac{8(q+1)}{7} - 3\}$. Then*

(1) $C_{3(q-1)}$ is skew symmetric and C_i is skew asymmetric if $i \in T \backslash \{3(q-1)\}$.
(2) There is only three SAPs (C_{q-5}, C_{5q-1}), (C_{2q-4}, C_{4q-2}) and (C_{6q-7}, C_{7q-6}) in T.

Consider the following sets:
$T_0(\delta) = \{i = 1 + 7j | q - \delta \leq j \leq q - 2\}$ for $2 \leq \delta \leq \frac{4(q+1)}{7} - 1$,
$T_1(\delta) = \{i = 1 + 7j | q - \delta \leq j \leq q - 2\}$ for $\frac{4(q+1)}{7} \leq \delta \leq \frac{5(q+1)}{7} - 1$,
$T_3(\delta) = \{i = 1 + 7j | q - \delta \leq j \leq q - 2\}$ for $\frac{5(q+1)}{7} \leq \delta \leq \frac{6(q+1)}{7} - 1$,
$T_5(\delta) = \{i = 1 + 7j | q - \delta \leq j \leq q - 2\}$ for $\frac{6(q+1)}{7} \leq \delta \leq q$,
$T_7(\delta) = \{i = 1 + 7j | 0 \leq j \leq \delta - 2\}$ for $q + 1 \leq \delta \leq \frac{8(q+1)}{7} - 1$.
From Lemma 7, we can derive the following corollary.

Corollary 7 *Let $T_i(\delta)$ for $i = 0, 1, 3, 5, 7$ be given as above.*

(1) If $2 \leq \delta \leq \frac{4(q+1)}{7} - 1$, then $T_0(\delta)_{ss} = T_0(\delta) \bigcap T_0(\delta)^{-q} = \varnothing$.
(2) If $\frac{4(q+1)}{7} \leq \delta \leq \frac{5(q+1)}{7} - 1$, then $T_1(\delta)_{ss} = T_1(\delta) \bigcap T_1(\delta)^{-q} = \{3q-3\}$.
(3) If $\frac{5(q+1)}{7} \leq \delta \leq \frac{6(q+1)}{7} - 1$, then $T_3(\delta)_{ss} = T_3(\delta) \bigcap T_3(\delta)^{-q} = \{3q-3, 2q-4, 4q-2\}$
(4) If $\frac{6(q+1)}{7} \leq \delta \leq q$, then $T_5(\delta)_{ss} = \{3q-3, 2q-4, 4q-2, q-5, 5q-1\}$.
(5) If $\frac{6(q+1)}{7} \leq \delta \leq q$, then $T_7(\delta)_{ss} = T_7(\delta) \bigcap T_7(\delta)^{-q} = \{3q-3, 2q-4, 4q-2, q-5, 5q-1, 6q-7, 7q-6\}$.

Applying Corollary 7, in a similar way to the proof of Theorem 4, we shall present the following theorem.

Theorem 8 *Suppose that* $n=\frac{q+1}{7}(q-1)$. *Set* $\delta\leq\frac{n+2}{2}$, *then there exist EAQMDS codes with parameters*

$$\begin{cases}[[n,n-2\delta+3,\delta;1]]_q & \text{if}\quad \frac{4(q+1)}{7}\leq\delta\leq\frac{5(q+1)}{7}-1;\\ [[n,n-2\delta+5,\delta;3]]_q & \text{if}\quad \frac{5(q+1)}{7}\leq\delta\leq\frac{6(q+1)}{7}-1;\\ [[n,n-2\delta+7,\delta;5]]_q & \text{if}\quad \frac{6(q+1)}{7}\leq\delta\leq q;\\ [[n,n-2\delta+9,\delta;7]]_q & \text{if}\quad q+1\leq\delta\leq\frac{8(q+1)}{7}-1.\end{cases}$$

In this section, we have constructed three classes of EAQMDS codes from η-constacyclic codes of lengths $\frac{q+1}{r}(q-1)$ $(r=3,5,7)$. Actually, similar to the above procedures, the same conclusions shall be obtained applying cyclic codes of responding lengths. For convenience to present all results of the whole paper, alternatively, we employ constacyclic codes here (cyclic codes are not able to work well in next section).

However, one cannot construct EAQMDS codes from underlying negacyclic codes like above subsections. There are two reasons. On the one hand, all cyclotomic cosets C_{1+2j} modulo $2n$ have the cardinality 2 since $(1+2j)(q^2-1)\not\equiv 0 \bmod \frac{2(q^2-1)}{r}$. Thus, it is impossible to construct underlying negacyclic MDS codes. On the other hand, 2 is not a factor of $q+1$ with q even. Hence, the Hermitian dual code of a q-ary negacyclic code is no longer negacyclic according to Lemma 2.

4 New EAQMDS codes of length $n=\frac{q+1}{r}(q-1)$ with $r=4,6$

It is shown in [16] that: If $r=4,6$, for $n=\frac{q+1}{r}(q-1)$, there are $[[n,n-2d+2,d]]_q$ QMDS code for $2\leq d\leq\frac{q+1}{2}+\frac{q+1}{r}-1$. In this section, we will discuss constructions of new $[[n,n-2d+2+c,d;c]]_q$ QMDS codes with $1\leq c\leq r$ and $d\geq\frac{q+1}{2}+\frac{q+1}{r}$, our results are presented in two subsections according to different $r=4,6$, respectively.

4.1 New EAQMDS codes of length $n=\frac{q+1}{4}(q-1)$

In this subsection, let $r=4$, $q=4l-1\geq 7$ and $n=\frac{q+1}{4}(q-1)$.

Lemma 8 *Let* $T=\{i=1+4j|0\leq j\leq\frac{5(q+1)}{4}-3\}$. *Then:*

(1) Each C_i *is skew asymmetric for* $i\in T$.
(2) There are only two SAPs (C_{q-2},C_{2q-1}) *and* (C_{3q-4},C_{4q-3}) *in* T.

Proof(1): According to Theorem 2, C_i is skew symmetric if and only if $1+4j\equiv 0 \bmod q-1$, i.e., $4j\equiv q-2 \bmod q-1$. Since $q=4l-1$ and $4j\leq 5q-5$, we have $4\nmid(q-2)+\alpha(q-1)$ if $\alpha=0,1,2,3,4$. This implies that $i(q+1)\not\equiv 0 \bmod q^2-1$ for $i\in T$, i.e., each C_i is skew asymmetric. Hence, (1) holds.

(2): Applying Theorem 2, in a similar way to the proof of Lemma 5, we can derive that there are only two SAPs (C_{q-2},C_{2q-1}) and (C_{3q-4},C_{4q-3}) in T. □

Consider the following sets:

$T_0(\delta)=\{i=1+4j|q-\delta\leq j\leq q-2\}$ for $2\leq\delta\leq\frac{3(q+1)}{4}-1$,

$T_2(\delta)=\{i=1+4j|q-\delta\leq j\leq q-2\}$ for $\frac{3(q+1)}{4}\leq\delta\leq q$,

$T_4(\delta)=\{i=1+4j|0\leq j\leq\delta-2\}$ for $q+1\leq\delta\leq\frac{5(q+1)}{4}-1$.

One can deduce the following results from Lemma 8.

Corollary 9 *Let $T_i(\delta)$ for $i=0,2,4$ be given as above.*

(1) If $2\leq\delta\leq\frac{3(q+1)}{4}-1$, then $T_0(\delta)_{ss}=T_0(\delta)\bigcap T_0(\delta)^{-q}=\emptyset$.
(2) If $\frac{3(q+1)}{4}\leq\delta\leq q$, then $T_2(\delta)_{ss}=T_2(\delta)\bigcap T_2(\delta)^{-q}=\{q-2,2q-1\}$.
(3) If $q+1\leq\delta\leq\frac{5(q+1)}{4}-1$, then $T_4(\delta)_{ss}=T_4(\delta)\bigcap T_4(\delta)^{-q}=\{q-2,2q-1,3q-4,4q-3\}$.

Applying Corollary 9, the following theorem can be obtained in a similar way to the proof of Theorem 4.

Theorem 10 *Suppose that $n=\frac{q+1}{4}(q-1)$. Set $\delta\leq\frac{n+2}{2}$, then there exist EAQMDS codes with parameters*

$$\begin{cases}[[n,n-2\delta+4,\delta;2]]_q \text{ if } & \frac{3(q+1)}{4}\leq\delta\leq q;\\ [[n,n-2\delta+6,\delta;4]]_q \text{ if } & q+1\leq\delta\leq\frac{5(q+1)}{4}-1.\end{cases}$$

4.2 New EAQMDS codes of length $n=\frac{q+1}{6}(q-1)$

In this subsection, let $r=6$, $q=6l-1\geq 11$ and $n=\frac{q+1}{6}(q-1)$. Similar to the last subsection, we can derive the following results.

Lemma 9 *Let $T=\{i=1+6j,0\leq j\leq\frac{7(q+1)}{6}-3\}$. Then:*

(1) each C_i is skew asymmetric for $i\in T$.
(2) there are only three SAPs (C_{q-4},C_{4q-1}), (C_{2q-3},C_{3q-2}) and (C_{6q-5},C_{5q-6}) in T.

Consider the following sets:

$T_0(\delta)=\{i=1+6j|q-\delta\leq j\leq q-2\}$ for $2\leq\delta\leq\frac{4(q+1)}{6}-1$,

$T_2(\delta)=\{i=1+6j|q-\delta\leq j\leq q-2\}$ for $\frac{4(q+1)}{6}\leq\delta\leq\frac{5(q+1)}{6}-1$,

$T_4(\delta)=\{i=1+6j|q-\delta\leq j\leq q-2\}$ for $\frac{5q+1)}{6}\leq\delta\leq q$,

$T_6(\delta)=\{i=1+6j|0\leq j\leq\delta-2\}$ for $q+1\leq\delta\leq\frac{7(q+1)}{6}-1$.

From Lemma 9, we can derive the following corollary.

Corollary 11 *Let $T_i(\delta)$ for $i=0,2,4,6$ be given as above.*

(1) If $2\leq\delta\leq\frac{4(q+1)}{6}-1$, then $T_0(\delta)_{ss}=T_0(\delta)\bigcap T_0(\delta)^{-q}=\emptyset$.
(2) If $\frac{4(q+1)}{6}\leq\delta\leq\frac{5(q+1)}{6}-1$, then $T_2(\delta)_{ss}=T_2(\delta)\bigcap T_2(\delta)^{-q}=\{2q-3,3q-2\}$.
(3) If $\frac{5q+1)}{6}\leq\delta\leq q$, then $T_4(\delta)_{ss}=T_4(\delta)\bigcap T_4(\delta)^{-q}=\{2q-3,3q-2,q-4,4q-1\}$.

Table 1 Some new EAQMDS codes of length $n = \frac{q+1}{3}(q-1), d \leq \frac{n+2}{2}$

	Paras.	q	d	References
QMDS	$[[n, n+2-2d, d]]_q$		$2 \leq d \leq \frac{2(q+1)}{3} - 1$	[16,17,22]
EAQMDS	$[[n, n+3-2d, d; 1]]_q$		$\frac{2(q+1)}{3} \leq d \leq q$	New
EAQMDS	$[[n, n+5-2d, d; 3]]_q$	Odd	$\frac{2(q+1)}{3} + 2 \leq d \leq \frac{4(q+1)}{3} - 2$	[26]
EAQMDS	$[[n, n+5-2d, d; 3]]_q$	Even	$q+1 \leq d \leq \frac{4(q+1)}{3} - 2$	New

Table 2 Some new EAQMDS codes of length $n = \frac{q+1}{5}(q-1), d \leq \frac{n+2}{2}$

	Paras.	q	d	References
QMDS	$[[n, n+2-2d, d]]_q$		$2 \leq d \leq \frac{3(q+1)}{5} - 1$	[16,17]
EAQMDS	$[[n, n+3-2d, d; 1]]_q$		$\frac{3(q+1)}{5} \leq d \leq \frac{4(q+1)}{5} - 1$	New
EAQMDS	$[[n, n+5-2d, d; 3]]_q$		$\frac{4(q+1)}{5} \leq d \leq q$	New
EAQMDS	$[[n, n+7-2d, d; 5]]_q$	Odd	$\frac{4(q+1)}{5} + 2 \leq d \leq \frac{6(q+1)}{5} - 2$	[26]
EAQMDS	$[[n, n+7-2d, d; 5]]_q$	Odd	$d = \frac{6(q+1)}{5} - 1$	New
EAQMDS	$[[n, n+7-2d, d; 5]]_q$	Even	$q+1 \leq d \leq \frac{6(q+1)}{5} - 1$	New

(4) If $q+1 \leq \delta \leq \frac{8(q+1)}{7} - 1$, *then* $T_6(\delta)_{ss} = \{2q-3, 3q-2, q-4, 4q-1, 6q-5, 5q-6\}$.

In a similar way to the proof of Theorem 4, we shall verify the following theorem by Corollary 3.

Theorem 12 *Suppose that* $n = \frac{q+1}{6}(q-1)$. *Set* $\delta \leq \frac{n+2}{2}$, *then there exist EAQMDS codes with parameters*

$$\begin{cases} [[n, n-2\delta+4, \delta; 2]]_q \text{ if } \frac{4(q+1)}{6} \leq \delta \leq \frac{5(q+1)}{6} - 1; \\ [[n, n-2\delta+6, \delta; 4]]_q \text{ if } \frac{5q+1)}{6} \leq \delta \leq q; \\ [[n, n-2\delta+8, \delta; 6]]_q \text{ if } q+1 \leq \delta \leq \frac{7(q+1)}{6} - 1. \end{cases}$$

In this section, we have constructed two classes of EAQMDS codes from η-constacyclic codes of lengths $\frac{q+1}{4}(q-1)$ and $\frac{q+1}{6}(q-1)$.

For $n = \frac{q+1}{4}(q-1)$ and $\frac{q+1}{6}(q-1)$, it is easy to know that the cyclotomic cosets $C_{\frac{(q-1)i}{2}}$ $(i = 0, 1, 2\ldots)$ modulo n are skew symmetric. From Lemma 2, we shall derive that the maximum designed distance of a Hermitian dual-containing cyclic code of length n is at most $\frac{q-1}{2}$, which is less than that of a Hermitian dual-containing constacyclic code of length n. As thus, applying cyclic codes, the parameters of EAQMDS codes are not so good as that of ones derived from constacyclic codes.

For $n = \frac{q+1}{4}(q-1)$, note that $C_{\frac{(q-1)(1+2i)}{2}}$ $(i = 0, 1, 2\ldots)$ modulo $2n$ are skew symmetric. Similar to cyclic codes, according to Lemma 2, negacyclic codes cannot work well when they are employed to construct EAQMDS codes compared with

Table 3 Some new EAQMDS codes of length $n = \frac{q+1}{7}(q-1), d \leq \frac{n+2}{2}$

	Paras.	q	d	References
QMDS	$[[n, n+2-2d, d]]_q$		$2 \leq \delta \leq \frac{4(q+1)}{7} - 1$	[16,17]
EAQMDS	$[[n, n+3-2d, d; 1]]_q$		$\frac{4(q+1)}{7} \leq d \leq \frac{5(q+1)}{7} - 1$	New
EAQMDS	$[[n, n+5-2d, d; 3]]_q$		$\frac{5(q+1)}{7} \leq d \leq \frac{6(q+1)}{7} - 2$	New
EAQMDS	$[[n, n+7-2d, d; 5]]_q$		$\frac{6(q+1)}{7} \leq d \leq q$	New
EAQMDS	$[[n, n+9-2d, d; 7]]_q$	Odd	$\frac{6(q+1)}{7} + 2 \leq d \leq \frac{8(q+1)}{7} - 2$	[26]
EAQMDS	$[[n, n+9-2d, d; 7]]_q$	Odd	$d = \frac{8(q+1)}{7} - 1$	New
EAQMDS	$[[n, n+9-2d, d; 7]]_q$	Even	$q+1 \leq d \leq \frac{8(q+1)}{7} - 1$	New

Table 4 Some new EAQMDS codes of length $n = \frac{q+1}{4}(q-1), d \leq \frac{n+2}{2}$

	Paras.	q	d	References
QMDS	$[[n, n+2-2d, d]]_q$	Odd	$2 \leq d \leq \frac{3(q+1)}{4} - 1$	[13,16]
EAQMDS	$[[n, n+4-2d, d; 2]]_q$	Odd	$\frac{3(q+1)}{4} \leq d \leq q$	New
EAQMDS	$[[n, n+6-2d, d; 4]]_q$	Odd	$q+1 \leq d \leq \frac{5(q+1)}{4} - 1$	New

Table 5 Some new EAQMDS codes of length $n = \frac{q+1}{6}(q-1), d \leq \frac{n+2}{2}$

	Paras.	q	d	References
QMDS	$[[n, n+2-2d, d]]_q$	Odd	$2 \leq d \leq \frac{4(q+1)}{6} - 1$	[16]
EAQMDS	$[[n, n+4-2d, d; 2]]_q$	Odd	$\frac{4(q+1)}{6} \leq d \leq \frac{5(q+1)}{6} - 1$	New
EAQMDS	$[[n, n+6-2d, d; 4]]_q$	Odd	$\frac{5q+1}{6} \leq d \leq q$	New
EAQMDS	$[[n, n+8-2d, d; 6]]_q$	Odd	$q+1 \leq d \leq \frac{8(q+1)}{7} - 1$	New

Table 6 Code comparisons of length $n = \frac{q+1}{r}(q-1)$ for $r = 3, 5, 7$ and $d \leq \frac{n+2}{2}$

q	d	Our Paras.	Paras. in [26]
Odd	$\frac{(r-1)(q+1)}{r} + 2 \leq d \leq q$	$[[n, n+r-2d, d; r-2]]_q$	$[[n, n+r+2-2d, d; r]]_q$

constacyclic codes. When $n = \frac{q+1}{6}(q-1)$, in a similar way to the above procedures for constacyclic codes, the same conclusions shall be obtained applying negacyclic codes with responding lengths.

Combining the discussions at the end of last section, it is not difficult to find the advantages of constacyclic codes compared with cyclic (negacyclic) codes. More specially, to unify all results of the whole paper, it is very necessary for constacyclic codes to be investigated and employed.

Table 7 Some detailed comparisons for $n = \frac{q+1}{5}(q-1)$ for $q = 19$ Let T be the defining set of underlying constacyclic codes to construct EAQMDS codes

Ours			[26]		
Paras.	$T = \{1+5j\}$	T_{ss}	Paras.	$T = \{1+5j\}$	Rank$(HH^{\dagger})$
$[[72, 51, 12; 1]]_{19}$	$7 \le j \le 17$	1			–
$[[72, 49, 13; 1]]_{19}$	$6 \le j \le 17$	1			–
$[[72, 47, 14; 1]]_{19}$	$5 \le j \le 17$	1			–
$[[72, 45, 15; 1]]_{19}$	$4 \le j \le 17$	1			–
$[[72, 45, 16; 3]]_{19}$	$3 \le j \le 17$	3			–
$[[72, 43, 17; 3]]_{19}$	$2 \le j \le 17$	3			–
$[\mathbf{72}, \mathbf{41}, \mathbf{18}; \mathbf{3}]]_{\mathbf{19}}$	$\mathbf{1 \le j \le 17}$	3	$[[\mathbf{72}, \mathbf{43}, \mathbf{18}; \mathbf{5}]]_{\mathbf{19}}$	$\mathbf{-1 \le j \le 15}$	5
$[[\mathbf{72}, \mathbf{39}, \mathbf{19}; \mathbf{3}]]_{\mathbf{19}}$	$\mathbf{0 \le j \le 17}$	3	$[[\mathbf{72}, \mathbf{41}, \mathbf{19}; \mathbf{5}]]_{\mathbf{19}}$	$\mathbf{-2 \le j \le 15}$	5
$[[72, 39, 20; 5]]_{19}$	$0 \le j \le 18$	5	$[[72, 39, 20; 5]]_{19}$	$-3 \le j \le 15$	5
$[[72, 37, 21; 5]]_{19}$	$0 \le j \le 29$	5	$[[72, 37, 21; 5]]_{19}$	$-3 \le j \le 16$	5
$[[72, 35, 22; 5]]_{19}$	$0 \le j \le 20$	5	$[[72, 35, 22; 5]]_{19}$	$-3 \le j \le 17$	5
$[[\mathbf{72}, \mathbf{33}, \mathbf{23}; \mathbf{5}]]_{\mathbf{19}}$	$\mathbf{0 \le j \le 21}$	5			–

Codes have better performance are given in bold

5 Code comparisons and conclusion

In this paper, we have derived five classes of EAQMDS codes from η-constacyclic MDS codes of lengths $n = \frac{q+1}{r}(q-1)(r = 3, 4, 5, 6, 7)$. For given r and $n = \frac{q+1}{r}(q-1)$, some standard QMDS codes have been obtained in [13,16,17,22]. We constructed many EAQMDS codes of relatively large distances up to $q + \frac{q+1}{r}(q + \frac{q+1}{r} - 1$ for $r = 3$) with a small number of pre-shared entangled states.

For comparison, we first give the following theorem.

Theorem 13 *(Theorem 6 in [26]) Let $t \geq 3$ be an odd integer and let q be an odd prime power with $t|(q+1)$. Then, there exists an EAQMDS code with parameters $[[\frac{q^2-1}{t}, \frac{q^2-1}{t} - 2d + t + 2, d; t]]_q$, where $\frac{(t-1)(q-1)}{t} + 2 \leq d \leq \frac{(t+1)(q-1)}{t} - 2$.*

On the one hand, a lot of EAQMDS codes constructed in this paper are new in the sense that they are not available in the literature. When $r = 3, 5, 7$ and $1 \leq c \leq r-2$, the $[[n, n-2d+c+2, d; c]]_q$ EAQMDS codes are new. when q is a power of 2, the $[[n, n-2d+r+2, d; r]]_q$ are also new. In addition, notice that the EAQMDS codes in [26] have the minimum distance less than $q + \frac{q+1}{r} - 1$. Hence, for a given odd prime power q, if $d = q + \frac{q+1}{r} \leq \frac{n+2}{2}$ and $r = 5, 7$, our EAQMDS codes $[[n, n-2d+r+2, d; r]]_q$ obtained in this paper are also new. For clarity, these new codes are listed in Tables 1, 2 and 3. When $r = 4, 6$, all the EAQMDS codes are new, which are detailedly shown in Tables 4 and 5.

On the other hand, some EAQMDS codes newly obtained in this paper have better performance than ones in the literature. Compared with EAQMDS codes derived from λ-constacyclic in [26], we employed underlying η-constacyclic codes with *different defining sets* (see the proof of Theorem 13). As thus, some relatively good EAQMDS

Table 8 Some new EAQMDS codes and code comparisons

q, r	d	Paras.	Paras. in [26]	References
$q = 7, r = 4$	$2 \leq d \leq 5$	$[[12, 14 - 2d, d]]_7$		[13,16]
	$d = 6, 7$	$[[12, 16 - 2d, d; 2]]_7$		New
$q = 8, r = 3$	$2 \leq d \leq 5$	$[[21, 23 - 2d, 6]]_8$		[16,17,22]
	$d = 6, 7, 8$	$[[21, 24 - 2d, 6; 1]]_8$		New
	$d = 9, 10$	$[[21, 26 - 2d, 6; 3]]_8$		New
$q = 9, r = 5$	$2 \leq d \leq 5$	$[[16, 18 - 2d, d]]_9$		[16,17]
	$d = 6, 7$	$[[16, 19 - 2d, d; 1]]_9$		New
	$d = 8, 9$	$[[16, 21 - 2d, d; 3]]_9$		New
$q = 11, r = 3$	$2 \leq d \leq 7$	$[[40, 42 - 2d, d]]_{11}$		[16,17]
	$d = 8, 9$	$[[40, 43 - 2d, d; 1]]_{11}$		New
	$d = 10, 11$	$[[40, 43 - 2d, d; 1]]_{11}$	$[[40, 45 - 2d, d; 3]]_{11}$	New
$r = 4$	$2 \leq d \leq 8$	$[[30, 32 - 2d, d]]_{11}$		[13,16]
	$d = 9, 10, 11$	$[[30, 34 - 2d, d; 2]]_{11}$		New
	$d = 12, 13, 14$	$[[30, 36 - 2d, d; 4]]_{11}$		New
$r = 6$	$2 \leq d \leq 7$	$[[20, 22 - 2d, d]]_{11}$		[16]
	$d = 8, 9$	$[[20, 24 - 2d, d; 2]]_{11}$		New
	$d = 10, 11$	$[[20, 26 - 2d, d; 4]]_{11}$		New
$q = 13, r = 7$	$2 \leq d \leq 7$	$[[24, 26 - 2d, d]]_{13}$		[16,17]
	$d = 8, 9$	$[[24, 27 - 2d, d; 1]]_{13}$		New
	$d = 10, 11$	$[[24, 29 - 2d, d; 3]]_{13}$		New
	$d = 12, 13$	$[[24, 31 - 2d, d; 5]]_{13}$		New
$q = 17, r = 3$	$2 \leq d \leq 11$	$[[96, 98 - 2d, d]]_{17}$		[16,17]
	$12 \leq d \leq 13$	$[[96, 99 - 2d, d; 1]]_{17}$		New
	$14 \leq d \leq 17$	$[[96, 99 - 2d, d; 1]]_{17}$	$[[96, 101 - 2d, d; 3]]_{17}$	New
$r = 6$	$2 \leq d \leq 11$	$[[54, 56 - 2d, d]]_{17}$		[16]
	$d = 12, 13, 14$	$[[54, 58 - 2d, d; 2]]_{17}$		New
	$d = 15, 16, 17$	$[[54, 60 - 2d, d; 4]]_{17}$		New
	$d = 18, 19, 20$	$[[54, 62 - 2d, d; 6]]_{17}$		New
$q = 19, r = 4$	$2 \leq d \leq 14$	$[[90, 92 - 2d, d]]_{19}$		[13,16]
	$15 \leq d \leq 19$	$[[90, 94 - 2d, d; 2]]_{19}$		New
	$20 \leq d \leq 24$	$[[90, 96 - 2d, d; 4]]_{19}$		New
$r = 5$	$2 \leq d \leq 11$	$[[72, 74 - 2d, d]]_{19}$		[16,17]
	$12 \leq d \leq 15$	$[[72, 75 - 2d, d; 1]]_{19}$		New
	$16 \leq d \leq 17$	$[[72, 77 - 2d, d; 3]]_{19}$		New
	$18 \leq d \leq 19$	$[[72, 77 - 2d, d; 3]]_{19}$	$[[72, 79 - 2d, d; 5]]_{19}$	New
	$20 \leq d \leq 22$	$[[72, 79 - 2d, d; 5]]_{19}$		[26]
	$d = 23$	$[[72, 79 - 2d, d; 5]]_{19}$		New

codes can be obtained. For $\frac{(r-1)(q+1)}{r}+2 \leq d \leq q$ and $c=r-2$, our $[[n, n-2d+c+2, d; c]]_q$ EAQMDS codes consume less entanglement states than the $[[n, n-2d+r+2, d; r]]_q$ codes constructed in [26], yet have the same net rate and error-correcting ability. We displayed these comparisons in Table 6. As an example for $n=\frac{q+1}{5}(q-1)$ and $q=19$, we presented the detailed comparisons with [26] in Table 7.

For clarity, for $q=7, 8, 9, 11, 13, 17, 19$, Table 8 further shows a series of new EAQMDS codes constructed in this paper and provides some code comparisons in detail. In the future work, we look forward to getting more EAQMDS codes with large minimum distance from pseudo-cyclic codes, quasi-cyclic codes, generalized Reed–Solomon codes and so on.

Acknowledgements We are sincerely indebted to two anonymous reviewers for their meticulous comments and suggestions, which much improved the presentation and quality of this paper.

References

1. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction and orthogonal geometry. Phys. Rev. Lett. **78**, 405–408 (1997)
2. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over GF(4). IEEE. Trans. Inf. Theory **44**, 1369 (1998)
3. Gottesman, D.: Stabilizer codes and quantum error correction. Ph.D. Thesis, California Institute of Technology (1997)
4. Gottesman, D.: Fault-tolerant quantum computation with higher-dimensional systems. Phys. Rev. A **57**(1), 127–137 (1998)
5. Bowen, G.: Entanglement required in achieving entanglement-assisted channel capacities. Phys. Rev. A **66**, 052313 (2002)
6. Brun, T., Devetak, I., Hsieh, M.-H.: Correcting quantum errors with entanglement. Science **52**, 436–439 (2006)
7. Grassl, M.: Entanglement-assisted quantum communication beating the quantum Singleton bound. Talk at AQIS, Taiwan (2016)
8. 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)
9. Krishna, A., Sarwate, D.V.: Pseudo-cyclic maximum-distance separable codes. IEEE Trans. Inf. Theory **36**, 880–884 (1990)
10. Jin, L., Ling, S., Luo, J., Xing, C.: Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes. IEEE Trans. Inf. Theory **56**(9), 4735–4740 (2010)
11. La Guardia, G.G.: New quantum MDS codes. IEEE Trans. Inf. Theory **57**(8), 5551–5554 (2011)
12. Kai, X., Zhu, S.: New quantum MDS codes from negacyclic codes. IEEE Trans. Inf. Theory **59**(2), 1193–1197 (2013)
13. Zhang, G., Chen, B.: New quantum MDS codes. Int. J. Quantum Inf. **12**(4), 5551–5554 (2014)
14. Kai, X., Zhu, S., Li, P.: Constacyclic codes and some new quantum MDS codes. IEEE Trans. Inf. Theory **60**(4), 2080–2086 (2014)
15. Jin, L., Xing, C.: A construction of new quantum MDS codes. IEEE Trans. Inf. Theory **60**(5), 2921–2925 (2014)
16. Wang, L., Zhu, S.: New quantum MDS codes derived from constacyclic codes. Quantum Inf. Process. **14**(3), 881–889 (2015)
17. Chen, B., Ling, S., Zhang, G.: Application of constacyclic codes to quantum MDS codes. IEEE Trans. Inform. Theory **61**, 1474–1484 (2015)
18. He, X., Xu, L., Chen, H.: New q-ary quantum MDS codes with distance bigger than $\frac{q}{2}$. Quantum Inf. Process **15**, 2745–2758 (2016)
19. Zhang, T., Ge, G.: Quantum MDS codes with large minimun distance. Des. Codes Cryptogr. **83**(3), 503–517 (2016)

20. Shi, X., Yue, Q., Zhu, X.: Construction of some new quantum MDS codes. Finite Fields Appl. **46**, 347–362 (2017)
21. Jin, L., Kan, H., Wen, J.: Quantum MDS codes with relatively large minimum distance from Hermitian self-orthogonal codes. Des. Codes Cryptogr. **84**(3), 463–471 (2017)
22. Qian, J., Zhang, L.: Improved constructions for quantum maximum distance separable codes. Quantum Inf. Process. **16**(1), 20 (2017). https://doi.org/10.1007/s11128-016-1490-x
23. Lai, C., Brun, T.A.: Entanglement increases the error-correcting ability of quantum error-correcting codes. Phys. Rev. A **88**, 012320 (2013). See also arXiv:1008.2598v1
24. Lai, C., Brun, T. A., Wilde, M. M.: Dualities and identities for entanglement-assisted quantum codes. (2011). See also arXiv:1010.5506v2
25. Li, R., Guo, L., Xu, Z.: Entanglement-assisted quantum codes achieving the quantum Singleton bound but violating the quantum Hamming bound. Quantum Inf. Comput. **14**, 1107–1116 (2014)
26. 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)
27. Chen, J., Huang, Y., Feng, C., Chen, R.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. Quantum Inf. Process. **16**, 303 (2017). https://doi.org/10.1007/s11128-017-1750-4
28. Guenda, K., Jitman, S., Gulliver, T.A.: Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr. (2017). https://doi.org/10.1007/s10623-017-0330-z
29. Li, R., Xu, G., Lv, L.: Decomposition of defining set of BCH codes and its applications. J. Air Force Eng. Univ. (Nat. Sci.Ed.) **14**(2), 87 (2013). (In Chinese)
30. Macwilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, Amsterdam (1977)
31. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
32. Lidar, A., Brun, T.A.: Quantum Error Correction. Cambridge University Press, Cambridge (2013)
33. 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**(1), 87 (2011). (In Chinese)
34. Sloane, N.J.A., Thompson, J.G.: Cyclic self-dual codes. IEEE Trans. Inf. Theory **29**, 364–366 (1983)
35. Li, R., Zuo, F., Liu, Y., Xu, Z.: Hermitian dual-containing BCH codes and construction of new quantum codes. Quantum Inf. Comput. **12**, 0021–0035 (2013)
36. Aydin, N., Siap, I., Ray-Chaudhuriand, D.K.: The strucure of 1-generator quasi-twisted codes and new linear codes. Des. Codes Cryptogr. **24**, 313–326 (2001)
37. Wilde, M.M., Brun, T.A.: Optimal entanglement formulas for entanglement-assisted quantum coding. Phys. Rev. A. **77**, 064302 (2008)
38. Guo, L., Li, R.: Linear Plotkin bound for entanglement-assisted quantum codes. Phys. Rev. A **87**, 032309 (2013)
39. Lü, L., Li, R.: Entanglement-assisted quantum codes constructed from primitive quaternary BCH codes. Int. J. Quantum Inf. **12**, 1450015 (2014)