RESEARCH



New Entanglement-Assisted Quantum Constacyclic Codes

Yajing Zhou¹ · Xiaoshan Kai¹

Received: 15 June 2023 / Accepted: 1 September 2023 / Published online: 18 September 2023 © The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract

The entanglement-assisted quantum error-correcting (EAQEC) codes have the potential to greatly generalize and enhance the performance of existing quantum error-correcting codes. In this paper, we investigate EAQEC codes of length $\frac{q^2-1}{r}$, where *r* is a positive divisor of q + 1. Most of these codes are new, and some of them have better performance than ones obtained in the literature. The resulting EAQEC codes are maximum-distance-separable (MDS) if the minimum distance $d \le \frac{n+2}{2}$.

Keywords Entanglement-assisted quantum codes · Constacyclic codes · Defining sets

1 Introduction

Quantum codes are used in quantum computation and quantum communication to lessen decoherence. It is well known that the standard quantum codes can be constructed from classical linear codes that must meet specific dual-containing condition [3]. The dual-containing condition limits that many linear codes with good performance can not produce quantum codes.

In 2002, Bowen [1] found that pre-shared entangle states between the sender and the receiver can increase both quantum and classical capacity for communication. In 2006, Brun et al. [2] showed that non-dual-containing quaternary linear codes can be applied to construct entanglement-assisted quantum error-correcting (EAQEC) codes. Later, a general coding scheme for creating binary EAQEC codes was developed, and many specific construction methods were put forward [11, 12, 18, 35]. In [9], the authors generalized these methods to an arbitrary finite field. Afterwards, many classes of non-binary EAQEC codes have been derived from classical linear codes such as constacyclic codes, linear complementary dual (LCD) codes, generalized Reed-Solomom (GRS) codes, extended GRS codes and Goppa codes (see [6, 7, 13, 14, 22, 23, 28, 31, 33]).

⊠ Xiaoshan Kai kxs6@sina.com

Yajing Zhou yjzhou0105@163.com

¹ School of Mathematics, Hefei University of Technology, Hefei 230601, Anhui, China

EA-quantum Singleton bound of EAQEC codes was proposed by Brun et al. in [2]. In 2016, Grassl [10] gave some examples of EAQEC codes and showed that the bound was not incomplete. In fact, this bound holds if $d \le \frac{n+2}{2}$ [17]. Now, we present the bound as follows.

Theorem 1 [2, 10, 18] (*EA-quantum Singleton bound*) For any $[[n, k, d; c]]_q$ EAQEC code, if $d \le \frac{n+2}{2}$, then $n + c - k \ge 2(d-1)$, where $0 \le c \le n-1$.

An EAQEC code with $d \leq \frac{n+2}{2}$ achieves the EA-quantum Singleton bound, then it is called an entanglement-assisted quantum maximum distance separable (EAQMDS) code.

Constacyclic codes including cyclic codes and negacyclic codes have been applied extensively to construct EAQEC codes because they have good algebraic structure. In 2011, Li et al. [20, 21] proposed the decomposition of defining sets of cyclic codes and they obtained EAQMDS codes with large minimum distance. In [5, 24], the authors expanded the concept to general constacyclic codes, and many families of EAQMDS codes of length n dividing $q^2 + 1$ or $q^2 - 1$ were constructed. Lu et al. [27] constructed EAQMDS codes from constacyclic codes with special lengths by consuming one or four entanglement bits. Liu et al. [24] used constacyclic codes to get EAQMDS codes of length $\frac{q+1}{r}(q-1)$, where $3 \le r \le 7$. In 2019, Qian et al. [29] derived a family of EAQEC codes with flexible parameters from cyclic codes. In the same year, Sari et al. [30] applied constacyclic codes of length $\frac{q^2-1}{4}$ to construct EAQMDS codes. In 2020, Wang et al. [32] obtained a series of EAQEC codes of length $\frac{q-1}{a}(q+1)$ from cyclic and negacyclic codes, and they turned out that the number of required entanglement bits can take almost all possible values. In 2022, Lu et al. [25, 26] constructed EAQMDS codes from cyclic codes with flexible parameters and large minimum distance.

In this work, we pay attention to EAQEC codes of length $n = \frac{q^2-1}{r}$, where *r* is a positive divisor of q + 1. Most of these codes are new, and some of them have better performance than ones obtained in the literature [8, 24, 25, 27, 30]. The EAQEC codes in this paper are MDS if the minimum distance $d \le \frac{n+2}{2}$. The paper is organized as follows. Some related basic knowledge and theorems are listed in Section 2. In Section 3, by characterizing the q^2 -cyclotomic cosets modulo *rn*, some EAQEC codes with large minimum distance are provided. In Section 4, two classes of EAQMDS codes consuming one or two pairs of maximally entangled states with larger minimum distance are obtained. Section 5 compares EAQEC codes in this paper with the known ones.

2 Preliminaries

Let *q* be a prime power. Let \mathbb{F}_{q^2} denote the finite field with q^2 elements, and $\mathbb{F}_{q^2}^*$ denote the multiplicative group consisted of the nonzero elements of \mathbb{F}_{q^2} . For each $\alpha \in \mathbb{F}_{q^2}^*$, the conjugate of α is defined by $\bar{\alpha} = \alpha^q$. Given two vectors $\mathbf{x} = (x_1, x_2, \dots, x_n), \mathbf{y} = (y_1, y_2, \dots, y_n) \in \mathbb{F}_{q^2}^n$, their Hermitian inner product is defined by

$$(\mathbf{x}, \mathbf{y})_h = \sum_{i=1}^n \bar{x}_i y_i = \bar{x}_1 y_1 + \bar{x}_2 y_2 + \dots + \bar{x}_n y_n.$$

A linear code C over \mathbb{F}_{q^2} of length *n* is a subspace of $\mathbb{F}_{q^2}^n$. The Hermitian dual code of C is

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

🖄 Springer

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

Assume that gcd(n, q) = 1. Let $\lambda \in \mathbb{F}_{q^2}^*$ have order r, i.e., $ord(\lambda) = r$. For each vector $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_{q^2}^n$, a λ -constacyclic shift f_{λ} is denoted by

$$f_{\lambda}(c_0, c_1, \ldots, c_{n-1}) = (\lambda c_{n-1}, c_0, \ldots, c_{n-2}).$$

A linear code C over \mathbb{F}_{q^2} of length n is a λ -constacyclic code if it is invariant under the λ constacyclic shift f_{λ} on $\mathbb{F}_{q^2}^n$. By identifying a vector $c = (c_0, c_1, \ldots, c_{n-1})$ with a polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$, a λ -constacyclic code C over \mathbb{F}_{q^2} of length n is an ideal in $\frac{\mathbb{F}_{q^2}[x]}{\langle x^n - \lambda \rangle}$. Note that $\frac{\mathbb{F}_{q^2}[x]}{\langle x^n - \lambda \rangle}$ is a principal ideal ring. So, there is a monic divisor g(x) of $x^n - \lambda$ in $\mathbb{F}_{q^2}[x]$ such that $C = \langle g(x) \rangle$. The polynomial g(x) is called the generator polynomial and the dimension of C is $n - \deg(g(x))$.

Let *m* be the multiplicative order of q^2 modulo *rn*. Then $rn \mid (q^{2m} - 1)$, and so $n \mid (q^{2m} - 1)$. Let β be a primitive *rn*-th root of unity in $\mathbb{F}_{q^{2m}}$ and $\xi = \beta^r \in \mathbb{F}_{q^{2m}}$. Then ξ is a primitive *n*-th root of unity. Thus, $\beta\xi^i = \beta^{1+ri}$, $0 \le i \le n-1$, are the roots of $x^n - \lambda$. Denote $\Gamma_{rn} = \{1 + ri \mid 0 \le i \le n-1\}$. The set

$$T = \{i \in \Gamma_{rn} \mid g(\beta^i) = 0\}$$

is called the defining set of C. The q^2 -cyclotomic coset of i modulo rn is given by

$$C_i = \{iq^{2j} \pmod{rn} \mid j = 0, 1, \dots, m_i - 1\},\$$

where m_i is the smallest positive integer l such that $iq^{2l} \equiv i \pmod{rn}$. Then, $M_s(x) = \prod_{j \in C_s} (x - \beta^j)$ must be in $\mathbb{F}_{q^2}[x]$ and is called the minimal polynomial of β^s over \mathbb{F}_{q^2} . If $rn - qi \in C_i$, then C_i is skew symmetric, otherwise skew asymmetric. The skew asymmetric cosets C_i and $C_{-qi} = C_{rn-qi}$ come in pair, and we denote such skew asymmetric pair as (C_i, C_{-qi}) .

Assume that $r \mid (q + 1)$. Then the Hermitian dual codes of λ -constacyclic codes over \mathbb{F}_{q^2} are still λ -constacyclic. A λ -constacyclic code C of length n over \mathbb{F}_{q^2} is a constacyclic BCH code with designed distance δ ($\delta \geq 2$) if, for some b = 1 + ri, its generator polynomial is

$$g(x) = \operatorname{lcm} \left\{ M_b(x), M_{b+r}(x), \dots, M_{b+r(\delta-2)}(x) \right\}.$$

For a constacyclic code, the minimum distance has the following bound.

Lemma 1 (*BCH* bound for constacyclic codes) [36] Let *C* be a λ -constacyclic code over \mathbb{F}_{q^2} of length *n*. Let $ord(\lambda) = r$ and β be a primitive *rn*-th root of unity. If the generator polynomial g(x) of *C* has the elements { $\beta^{1+ri} \mid 0 \leq i \leq \delta-2$ } as the roots, then the minimum distance of *C* is not less than δ .

Definition 1 [19] Let $\lambda \in \mathbb{F}_{q^2}$ be a primitive *r*-th root of unity and $r \mid (q+1)$. Let \mathcal{C} be a λ -constacyclic code over \mathbb{F}_{q^2} of length *n* with defining set T. Denote $T_{ss} = -qT \cap T$ and $T_{sas} = T \setminus T_{ss}$, where $-qT = \{rn - qi \mid i \in T\}$. We call $T = T_{ss} \cup T_{sas}$ is a decomposition of the defining set of \mathcal{C} .

According to Definition 1, Liu et al. [24] gave the following lemma to calculate the number of needed ebits.

Lemma 2 [24] Let C be a λ -constacyclic code over \mathbb{F}_{q^2} of length n with defining set T. Suppose that $T = T_{ss} \cup T_{sas}$ is the decomposition of T. If C has parameters [n, n - |T|, d], then there is an $[[n, n - 2|T| + |T_{ss}|, d; |T_{ss}|]]_q$ EAQEC code.

Throughout this paper, denote by [u, v] a positive integers set, whose elements are not less than u and not bigger than v. Assume that $u \equiv 1 \pmod{r}$. Denote $[u, v]_r \subseteq [u, v]$ and $s \equiv 1 \pmod{r}$ with $s \in [u, v]_r$. The following lemma is useful in the sequel.

Lemma 3 [24] Let r be a positive divisor of q + 1 and $n = \frac{q^2 - 1}{r}$. For a given integer $i_2 \in \Gamma_{rn}$, i_2 can be denoted by $i_2 = \alpha q - \beta$ for two proper integers $1 \le \alpha, \beta \le q$. Then, there is an integer $i_1 \in \Gamma_{rn}$ such that (C_{i_1}, C_{i_2}) is a skew asymmetric pair if and only if $i_1 = \beta q - \alpha$.

3 EAQEC Codes with Large Minimum Distance

Let q be a prime power, and r be a positive divisor of q + 1. We take $n = \frac{q^2-1}{r}$ and $a = \frac{q+1}{r}$. In this section, we will construct new $[[n, n - 2d + c + 2, d; c]]_q$ EAQEC codes with $1 \le c \le 6r - 4$ and $\frac{q+3-a}{2} \le d \le \frac{5q-3}{2}$.

Lemma 4 Let r be an odd integer with $r \mid (q + 1)$, and let $s_1 \ge s_2 > 0$ be integers with $s_1, s_2 \in \Gamma_{rn}$. Then $C_{s_1} = -qC_{s_2}$ if and only if s_1 and s_2 satisfy one of the following forms: when l is odd,

$$\begin{cases} s_1 = (\frac{rl-1}{2} + t)q - (\frac{rl-1}{2} - t), \\ s_2 = (\frac{rl-1}{2} - t)q - (\frac{rl-1}{2} + t), \end{cases}$$
(1)

and when l is even,

$$\begin{cases} s_1 = (\frac{rl}{2} + t)q - (\frac{rl}{2} - t - 1), \\ s_2 = (\frac{rl}{2} - t - 1)q - (\frac{rl}{2} + t), \end{cases}$$
(2)

where $0 \le t \le \lfloor \frac{rl-1}{2} \rfloor - 1$ and $1 \le l \le 2a - 1$.

Proof If $C_{s_1} = -qC_{s_2}$, then $s_1 + qs_2 \equiv 0 \pmod{rn}$. Thus, $s_1 + s_2 \equiv 0 \pmod{q-1}$ and $s_1 - s_2 \equiv 0 \pmod{q+1}$. Then there are integers l_1, l_2 such that

$$s_1 + s_2 = l_1(q-1) \text{ and } s_1 - s_2 = l_2(q+1).$$
 (3)

Since $s_1 \equiv s_2 \equiv 1 \pmod{r}$ and $q \equiv -1 \pmod{r}$, then $-2l_1 \equiv l_1(q-1) = s_1 + s_2 \equiv 2 \pmod{r}$. Then $l_1 \equiv -1 \pmod{r}$ since *r* is odd. Thus there is an integer *l* such that $l_1 = rl - 1$. By (3), we get

$$\begin{cases} s_1 = \frac{rl - 1 + l_2}{2}q - \frac{rl - 1 - l_2}{2}, \\ s_2 = \frac{rl - 1 - l_2}{2}q - \frac{rl - 1 + l_2}{2}. \end{cases}$$

Since s_1 , s_2 are positive integers and r is odd, then l, l_2 have different parities. Let $t = \lfloor \frac{l_2}{2} \rfloor$. Based on the parity of l, we can get (1) and (2). From $s_1 \ge s_2 \ge 1$ and $1 < s_1 < q^2 - 1$, we have $0 \le t \le \lfloor \frac{rl-1}{2} \rfloor - 1$ and $1 \le l \le 2a - 1$.

If s_1, s_2 satisfy (1) and (2), then one can get $C_{s_1} = -qC_{s_2}$ easily. This completes the proof.

Lemma 4 shows when r is odd, C_s is skew symmetric if and only if t = 0 and l is odd; if and only if (q - 1) | s. By Lemmas 3 and 4, if $s_1 > s_2$ and (C_{s_1}, C_{s_2}) is a skew asymmetric pair, s_2 can be determined by s_1 immediately. To be specific, set $i_1 = \frac{rl-1+l_2}{2}$ and $i_2 = \frac{rl-1-l_2}{2}$. If $s_1 = i_1q - i_2$, then $s_2 = i_2q - i_1$. Thus, we only give the value of s_1 in the following discussions.

Lemma 5 Let $r \ge 5$ be an odd divisor of q + 1 and $a = \frac{q+1}{r} \ge 2$. Let C be a λ -constacyclic code over \mathbb{F}_{q^2} of length n with defining set $T = \bigcup_{i=0}^{d-2} C_{1+ri}$, where $2 \le d \le \frac{5q-3-a}{2}$. Let $T = Tss \cup Tsas$. For a fixed integer t with $0 \le t \le \frac{r-5}{2}$,

$$|T_{ss}| = \begin{cases} 1+2t, & \frac{q+3-a}{2}+at \le d \le \frac{q+1+a}{2}+at, \\ r-2, & q+2-2a \le d \le q, \\ r+2t, & q+1+at \le d \le q+a(t+1), \\ 2r-3, & \frac{3}{2}(q+1-a) \le d \le \frac{3q-1-a}{2}, \\ 2r+4t, & \frac{3q+3-a}{2}+at \le d \le \frac{3q-1+a}{2}+at \text{ and } 0 \le t \le \frac{r-3}{2}, \\ 4r-4, & 2q+1-a \le d \le 2q-1, \\ 4r+4t, & 2q+1+at \le d \le 2q-1+a(t+1), \\ 6r-6, & \frac{5q+3-3a}{2} \le d \le \frac{5q-3-a}{2}, a \ge 3. \end{cases}$$
(4)

Proof If $0 \le i \le \frac{5q-3-a}{2} - 2$, then $1 \le 1 + ri \le \frac{5r-1}{2}q - \frac{7r-1}{2}$. Denote the set $L = [1, \frac{5r-1}{2}q - \frac{7r-1}{2}]_r$. By Lemma 4, we can get the skew symmetric cyclotomic cosets C_s and skew asymmetric pairs (C_{s_1}, C_{s_2}) satisfying $s_1 > s_2$ in L are contained in the following set

$$\Omega = \left\{ s_1, s_2 : s_1, s_2 \text{ satisfy (1) or (2), for } 1 \le l \le 4 \text{ and } 0 \le t \le \left\lfloor \frac{rl-1}{2} \right\rfloor - 1 \right\}.$$

Denote the set Ω by S_l when $1 \le l \le 4$. Then

$$S_1 = \left\{ s_1 = \left(\frac{r-1}{2} + t\right)q - \left(\frac{r-1}{2} - t\right) : 0 \le t \le \frac{r-3}{2} \right\} \cup \left\{ s_2 : 0 \le t \le \frac{r-3}{2} \right\}.$$

Assume that

$$S_{21} = \left\{ s_1 = (r+t)q - (r-t-1) : 0 \le t \le \frac{r-3}{2} \right\} \cup \left\{ s_2 : 0 \le t \le \frac{r-3}{2} \right\}$$

and

$$S_{22} = \left\{ s_1 = \left(\frac{3r-1}{2} + t\right)q - \left(\frac{r-1}{2} + t\right) : 0 \le t \le \frac{r-3}{2} \right\} \cup \left\{ s_2 : 0 \le t \le \frac{r-3}{2} \right\}.$$

Then

$$S_2 = \{s_1 = (r+t)q - (r-t-1) : 0 \le t \le r-2\} \cup \{s_2 : 0 \le t \le r-2\} = S_{21} \cup S_{22}.$$

Assume that

$$S_{31} = \left\{ s_1 = \left(\frac{3r-1}{2} + t\right)q - \left(\frac{3r-1}{2} - t\right) : 0 \le t \le \frac{r-3}{2} \right\} \cup \left\{ s_2 : 0 \le t \le \frac{r-3}{2} \right\},$$
$$S_{32} = \{(2r-1)q - r, rq - (2r-1)\},$$
$$S_{33} = \left\{ s_1 = (2r+t)q - (r-t-1) : 0 \le t \le \frac{r-3}{2} \right\} \cup \left\{ s_2 : 0 \le t \le \frac{r-3}{2} \right\},$$

and

$$S_{34} = \left\{ s_1 = \left(\frac{5r-1}{2} + t\right)q - \left(\frac{r-1}{2} - t\right) : 0 \le t \le \frac{r-3}{2} \right\} \cup \left\{ s_2 : 0 \le t \le \frac{r-3}{2} \right\}.$$

Springer

Then

$$S_{3} = \left\{ s_{1} = \left(\frac{3r-1}{2} + t\right) q - \left(\frac{3r-1}{2} - t\right) : 0 \le t \le \frac{3r-3}{2} \right\} \cup \left\{ s_{2} : 0 \le t \le \frac{3r-3}{2} \right\}$$
$$= \bigcup_{i=1}^{4} S_{3i}.$$

Assume that

$$S_{41} = \left\{ s_1 = (2r+t)q - (2r-t-1) : 0 \le t \le \frac{r-3}{2} \right\} \cup \left\{ s_2 : 0 \le t \le \frac{r-3}{2} \right\},$$

then

$$S_4 = S_{41} \cup \left\{ s_1 = (2r+t)q - (2r-t-1) : \frac{r-1}{2} \le t \le 2r-2 \right\} \cup \left\{ s_2 : \frac{r-1}{2} \le t \le 2r-2 \right\}.$$

In fact, we can get that the skew symmetric cyclotomic cosets C_s and skew asymmetric pairs (C_{s_1}, C_{s_2}) satisfying $s_1 > s_2$ in L form the set $S = S_1 \cup S_2 \cup S_{31} \cup S_{32} \cup S_{33} \cup S_{41}$.

For the sake of expressing clearly, let T_i and T_{ssi} substitute for the defining set T of C and T_{ss} in the (*i*)-th case respectively, where $1 \le i \le 8$. Thus, in order to determine T_{ssi} , we need to discuss $T_i \cap S$.

(1) For a fixed integer t with $0 \le t \le \frac{r-5}{2}$, assume that

$$T_{10} = \left[1, 1 + r\left(\frac{q-1-a}{2} + at\right)\right]_r = \left[1, \left(\frac{r-1}{2} + t\right)q - \left(\frac{r-1}{2} - t\right)\right]_r,$$

and

$$T_{11} = \left[1, 1 + r\left(\frac{q-3+a}{2} + at\right)\right]_r = \left[1, \left(\frac{r+1}{2} + t\right)q - \left(\frac{3r-1}{2} - t - 1\right)\right]_r.$$

If C is a λ -constacyclic code with defining set $T_1 = \bigcup_{i=0}^{d-2} C_{1+ri}$, where $\frac{q+3-a}{2} + at \le d \le \frac{q+1+a}{2} + at$, then $T_{10} \subseteq T_1 \subseteq T_{11}$ and $(T_{11} \setminus T_{10}) \cap S = \emptyset$. Thus,

$$T_{ss1} = -qT_1 \cap T_1 = -qT_{10} \cap T_{10}$$

= $\left\{ s_1 = \left(\frac{r-1}{2} + t' \right) q - \left(\frac{r-1}{2} - t' \right) : 0 \le t' \le t \right\} \cup \left\{ s_2 : 0 \le t' \le t \right\}.$

Thus, $|T_{ss1}| = 1 + 2t$.

(2) Assume that

$$T_{20} = [1, 1 + r(q - 2a)]_r = [1, (r - 2)q - 1]_r,$$

and

$$T_{21} = [1, 1 + r(q - 2)]_r = [1, rq - 2r + 1]_r$$

If C is a λ -constacyclic code with defining set $T_2 = \bigcup_{i=0}^{d-2} C_{1+ri}$, where $q+2-2a \le d \le q$, then $T_{20} \subseteq T_2 \subseteq T_{21}$ and $(T_{21} \setminus T_{20}) \cap S = \emptyset$. Thus, we can get $T_{ss2} = -qT_2 \cap T_2 = -qT_{20} \cap T_{20} = S_1$. Thus, $|T_{ss2}| = r-2$.

(3) For a fixed integer t with $0 \le t \le \frac{r-5}{2}$, assume that

$$T_{30} = [1, 1 + r(q - 1 + at)]_r = [1, (r + t)q - r + t + 1]_r,$$

and

$$T_{31} = [1, 1 + r(q + a(t+1) - 2)]_r = [1, (r+t+1)q - 2r + t + 2]_r.$$

D Springer

If C is a λ -constacyclic code with defining set $T_3 = \bigcup_{i=0}^{d-2} C_{1+ri}$, where $q + 1 + at \le d \le q + a(t+1)$, then $T_{30} \subseteq T_3 \subseteq T_{31}$. Notice that $(T_{31} \setminus T_{30}) \cap S = \emptyset$. Thus, we have

$$T_{ss3} = -qT_3 \cap T_3 = -qT_{30} \cap T_{30}$$

= $T_{ss2} \cup \{s_1 = (r+t')q - (r-t'-1) : 0 \le t' \le t\} \cup \{s_2 : 0 \le t' \le t\}.$

Thus, $|T_{ss3}| = r - 2 + 2(1 + t) = r + 2t$.

(4) Assume that

$$T_{40} = \left[1, 1 + r\left(\frac{3}{2}(q+1-a) - 2\right)\right]_r = \left[1, \frac{3(r-1)}{2}q - \frac{r+1}{2}\right]_r$$

and

$$T_{41} = \left[1, 1 + r\left(\frac{3q - 1 - a}{2} - 2\right)\right]_r = \left[1, \frac{3r - 1}{2}q - \frac{5r - 1}{2}\right]_r$$

If C is a λ -constacyclic code with defining set $T_4 = \bigcup_{i=0}^{d-2} C_{1+ri}$, where $\frac{3}{2}(q+1-a) \le d \le \frac{3q-1-a}{2}$, then $T_{40} \subseteq T_4 \subseteq T_{41}$ and $(T_{41} \setminus T_{40}) \cap S = \emptyset$. Thus,

$$T_{ss4} = -q T_4 \cap T_4 = -q T_{40} \cap T_{40} = T_{ss2} \cup S_{21}$$

Thus, $|T_{ss4}| = r - 2 + 2 \cdot \frac{r-1}{2} = 2r - 3$.

(5) For a fixed integer t with $0 \le t \le \frac{r-3}{2}$, assume that

$$T_{50} = \left[1, 1 + r\left(\frac{3q+3-a}{2} + at - 2\right)\right]_r = \left[1, \left(\frac{3r-1}{2} + t\right)q - \left(\frac{r-1}{2} - t\right)\right]_r,$$

and

$$T_{51} = \left[1, 1+r\left(\frac{3q-1+a}{2}+at-2\right)\right]_r = \left[1, \left(\frac{3r+1}{2}+t\right)q - \left(\frac{5r-3}{2}-t\right)\right]_r.$$

If C is a λ -constacyclic code with defining set $T_5 = \bigcup_{i=0}^{d-2} C_{1+ri}$, where $\frac{3q+3-a}{2} + at \le d \le \frac{3q-1+a}{2} + at$, then $T_{50} \subseteq T_5 \subseteq T_{51}$ and $(T_{51} \setminus T_{50}) \cap S = \emptyset$. Let $S'_{22} = \{s_1 = (\frac{3r-1}{2} + t')q - (\frac{r-1}{2} - t') : 0 \le t' \le t\} \cup \{s_2 : 0 \le t' \le t\}$ and $S'_{31} = \{s_1 = (\frac{3r-1}{2} + t')q - (\frac{3r-1}{2} - t') : 0 \le t' \le t\} \cup \{s_2 : 0 \le t' \le t\}$. Then $S'_{22} \subseteq S_{22}$ and $S'_{31} \subseteq S_{31}$. Hence,

$$T_{ss5} = -qT_5 \cap T_5 = T_{ss2} \cup S'_{22} \cup S'_{31}.$$

Thus, $|T_{ss5}| = 2r - 3 + 2(t + 1) + 1 + 2t = 2r + 4t$.

(6) Assume that

$$T_{60} = [1, 1 + r(2q - 1 - a)]_r = [1, (2r - 1)q - r]_r,$$

and

$$T_{61} = [1, 1 + r(2q - 3)]_r = [1, (2r - 1)q - r]_r$$

If C is a λ -constacyclic code with defining set $T_6 = \bigcup_{i=0}^{d-2} C_{1+ri}$, where $2q + 1 - a \le d \le 2q - 1$, then $T_{60} \subseteq T_6 \subseteq T_{61}$ and $(T_{61} \setminus T_{60}) \cap S = \emptyset$. This gives that

$$T_{ss6} = -q T_6 \cap T_6 = T_{ss4} \cup S_{22} \cup S_{31} \cup S_{32}.$$

Thus, $|T_{ss6}| = 2r - 3 + 2\frac{r-1}{2} + 1 + 2\frac{r-3}{2} + 2 = 4r - 4.$

D Springer

(7) For a fixed integer t with $0 \le t \le \frac{r-5}{2}$, assume that

$$T_{70} = [1, 1 + r(2q - 1 + at)]_r = [1, (2r + t)q - r + t + 1]_r$$

and

$$T_{71} = [1, 1 + r(2q - 3 + a(t+1))]_r = [1, (2r + t + 1)q - 3r + t + 2]_r.$$

If C is a λ -constacyclic code with defining set $T_7 = \bigcup_{i=0}^{d-2} C_{1+ri}$, where 2q + 1 + 1 $\begin{array}{l} at \leq d \leq 2q - 1 + a(t+1), \text{ then } T_{70} \subseteq T_7 \subseteq T_{71} \text{ and } (T_{71} \setminus T_{70}) \cap S = \emptyset. \\ \text{Let } S'_{32} = \left\{ s_1 = (2r+t')q - (r-t'-1): 0 \leq t' \leq t \right\} \cup \left\{ s_2: 0 \leq t' \leq t \right\} \text{ and } S'_{41} = \left\{ s_1 = (2r+t')q - (2r-t'-1): 0 \leq t' \leq t \right\} \cup \left\{ s_2: 0 \leq t' \leq t \right\}, \text{ then } S'_{32} \subseteq S_{32} \text{ and} \end{array}$ $S'_{41} \subseteq S_{41}$. By Lemma 4, we know

$$T_{ss7} = -q T_7 \cap T_7 = T_{ss3} \cup S'_{32} \cup S'_{41}$$

Thus, $|T_{ss7}| = 4r - 4 + 4(t+1) = 4r + 4t$. (8) Assume that $T_{80} = \left[1, 1 + r\frac{5q - 1 - 3a}{2}\right]_r = \left[1, \frac{5r - 3}{2}q - \frac{r+1}{2}\right]_r$. If C is a λ -constacyclic code with defining set $T_8 = \bigcup_{i=0}^{d-2} C_{1+ri}$, where $\frac{5q+3-3a}{2} \le d \le \frac{5q-3-a}{2}$ and $a \ge 3$, then $T_{80} \subseteq T_8 \subseteq L$ and $T_{ss8} = -qT_8 \cap T_8 = T_{ss6} \cup S_{33} \cup \tilde{S}_{41}$. Thus, $|T_{ss8}| = 4r - 4 + 4 \cdot \frac{r-1}{2} = 4r - 4 + 4 \cdot \frac{r-1}{2}$ 6r - 6. This completes the proof.

By Lemmas 2 and 5, new EAQEC codes of length n with flexible parameters can be constructed from λ -constacyclic codes over \mathbb{F}_{q^2} of length *n*, as below.

Theorem 2 Let $r \ge 5$ be an odd divisor of q + 1 and $a = \frac{q+1}{r} \ge 2$. Then for a fixed integer t with $0 \le t \le \frac{r-5}{2}$, there are EAQEC codes with the following parameters

(1) $[[n, n-2d+2t+3, d; 1+2t]]_q$, where $\frac{q+3-a}{2} + at \le d \le \frac{q+1+a}{2} + at$; (2) $[[n, n-2d+r, d; r-2]]_q$, where $q + 2 - 2a \le d \le q$; (3) $[[n, n-2d+r+2+2t, d; r+2t]]_q$, where $q + 1 + at \le d \le q + a(t+1)$; (4) $[[n, n-2d+2r-1, d; 2r-3]]_q$, where $\frac{3}{2}(q+1-a) \le d \le \frac{3q-1-a}{2}$; (5) $[[n, n-2d+2r+2+4t, d; 2r+4t]]_q$, where $\frac{3q+3-a}{2} + at \le d \le \frac{3q-1+a}{2} + at$ and $0 \le t \le \frac{r-3}{2};$ (6) $[[n, n-2d+4r-2, d; 4r-4]]_q$, where $2q+1-a \le d \le 2q-1$; (7) $[[n, n-2d+4r+2+4t, d; 4r+4t]]_q$, where $2q+1+at \le d \le 2q-1+a(t+1);$ (8) $[[n, n-2d+6r-4, d; 6r-6]]_q$, where $\frac{5q+3-3a}{2} \le d \le \frac{5q-3-a}{2}$, $a \ge 3$.

Remark 1 In fact, for r = 3, Lemma 5 and Theorem 2 hold true if the cases (2), (4), (6) and (8) are only considered.

Lemma 6 Let r be an even divisor of q + 1. Let $s_1 \ge s_2 > 0$ be integers with $s_1, s_2 \in \Gamma_{rn}$. Then $C_{s_1} = -qC_{s_2}$ if and only if

$$\begin{cases} s_1 = (\frac{rl}{2} + t)q - (\frac{rl}{2} - t - 1), \\ s_2 = (\frac{rl}{2} - t - 1)q - (\frac{rl}{2} + t), \end{cases}$$
(5)

where l, t are integers with $0 \le t \le \frac{rl}{2} - 2$ and $1 \le l \le 2a - 1$.

Proof Similar to Lemma 4, we can get $-2l_1 \equiv l_1(q-1) = s_1 + s_2 \equiv 2 \pmod{r}$. Then $l_1 \equiv -1 \pmod{\frac{r}{2}}$. So there is an integer l' such that $l_1 = \frac{r}{2}l' - 1$. Then we can get

$$\begin{cases} s_1 = (\frac{\frac{r}{2}l' - 1 + l_2}{2})q - (\frac{\frac{r}{2}l' - 1 - l_2}{2}), \\ s_2 = (\frac{\frac{r}{2}l' - 1 - l_2}{2})q - (\frac{\frac{r}{2}l' - 1 + l_2}{2}). \end{cases}$$

Since $q \equiv -1 \pmod{r}$, then $s_1 \equiv -\frac{r}{2}l' + 1 \pmod{r}$ and $s_2 \equiv -\frac{r}{2}l' + 1 \pmod{r}$. It follows that l' is even due to $s_1 \equiv s_2 \equiv 1 \pmod{r}$. Assume that l' = 2l and $t = \frac{l_2-1}{2}$, then the system (5) can be derived. Similar to Lemma 4 the ranges of t and l can be obtained. And the sufficiency can be verified easily. This completes the proof.

In fact, Lemma 6 gives a necessary and sufficient condition of two q^2 -cyclotomic cosets modulo rn to be a skew asymmetric pair when r is even. And Lemma 6 shows when r is even, it is impossible that C_s is skew symmetric. If $s_1 > s_2$ and (C_{s_1}, C_{s_2}) is a skew asymmetric pair, by Lemmas 3 and 6, s_2 can be determined by s_1 immediately. To be specific, set $i_1 = \frac{rl}{2} + t$ and $i_2 = \frac{rl}{2} - t - 1$. If $s_1 = i_1q - i_2$, then $s_2 = i_2q - i_1$. Thus, we only give the value of s_1 in the following discussions.

Lemma 7 Let $r \ge 6$ be an even divisor of q + 1 and $a = \frac{q+1}{r} > 2$. Let C be a λ -constacyclic code over \mathbb{F}_{q^2} of length $n = \frac{q^2-1}{r}$ with defining set $T = \bigcup_{i=0}^{d-2} C_{1+ri}$, where $2 \le d \le \frac{5q-3}{2}$. Let $T = T_{ss} \cup T_{sas}$. For a fixed integer t with $0 \le t \le \frac{r}{2} - 2$,

$$|T_{ss}| = \begin{cases} 2(t+1), & \frac{q+3}{2} + at \le d \le \frac{q+1}{2} + a(t+1) \text{ and } t \le \frac{r}{2} - 3, \\ r-2, & q+2-2a \le d \le q, \\ r+2t, & q+1+at \le d \le q+a(t+1), \\ 2r-2, & \frac{3}{2}(q+1) - a \le d \le \frac{3q-1}{2}, \\ 2r+4t+2, & \frac{3q+3}{2} + at \le d \le \frac{3q-1}{2} + a(t+1), \\ 4r-4, & 2q+1-a \le d \le 2q-1, \\ 4r+4t, & 2q+1+at \le d \le 2q-1+a(t+1), \\ 6r-4, & \frac{5q+3}{2} - a \le d \le \frac{5q-3}{2}, a \ge 3. \end{cases}$$
(6)

Proof If $0 \le i \le \frac{5q-3}{2} - 2$, then $1 \le 1 + ri \le \frac{5r}{2}q - \frac{7r}{2} + 1$. Denote the set $M = [1, \frac{5r}{2}q - \frac{7r}{2} + 1]_r$. By Lemma 6, we know there do not exist skew symmetric cyclotomic cosets in M and we can get the skew asymmetric pairs (C_{s_1}, C_{s_2}) satisfying $s_1 > s_2$ in M are contained in the following set

$$\Lambda = \left\{ s_1, s_2 : s_1, s_2 \text{ satisfy the system (5) with } 1 \le l \le 4 \text{ and } 0 \le t \le \frac{rl}{2} - 2 \right\}.$$

Denote the set Λ by S_l when $1 \le l \le 4$. Then

$$S_1 = \left\{ s_1 = \left(\frac{r}{2} + t\right) q - \left(\frac{r}{2} - t - 1\right) : 0 \le t \le \frac{r}{2} - 2 \right\} \cup \left\{ s_2 : 0 \le t \le \frac{r}{2} - 2 \right\}.$$

Assume that

$$S_{21} = \left\{ s_1 = (r+t)q - (r-t-1) : 0 \le t \le \frac{r}{2} - 2 \right\} \cup \left\{ s_2 : 0 \le t \le \frac{r}{2} - 2 \right\},$$

and

$$S_{22} = \left\{ s_1 = \left(\frac{3r}{2} + t\right)q - \left(\frac{r}{2} + t - 1\right) : 0 \le t \le \frac{r}{2} - 2 \right\} \cup \left\{ s_2 : 0 \le t \le \frac{r}{2} - 2 \right\}.$$

Deringer

Then

$$S_2 = \{s_1 = (r+t)q - (r-t-1) : 0 \le t \le r-2\} \cup \{s_2 : 0 \le t \le r-2\}$$

= $S_{21} \cup S_{22}$.

Assume that

$$S_{31} = \left\{ s_1 = \left(\frac{3r}{2} + t\right) q - \left(\frac{3r}{2} - t - 1\right) : 0 \le t \le \frac{r}{2} - 2 \right\} \cup \left\{ s_2 : 0 \le t \le \frac{r}{2} - 2 \right\},$$

$$S_{32} = \left\{ (2r - 1)q - r, rq - (2r - 1) \right\},$$

$$S_{33} = \left\{ s_1 = (2r + t)q - (r - t - 1) : 0 \le t \le \frac{r}{2} - 2 \right\} \cup \left\{ s_2 : 0 \le t \le \frac{r}{2} - 2 \right\}$$

$$S_{34} = \left\{ s_1 = \left(\frac{5r}{2} + t\right)q - \left(\frac{r}{2} - t - 1\right) : 0 \le t \le \frac{r}{2} - 2 \right\} \cup \left\{ s_2 : 0 \le t \le \frac{r}{2} - 2 \right\}.$$

Then

$$S_{3} = \left\{ s_{1} = \left(\frac{3r}{2} + t\right)q - \left(\frac{3r}{2} - t - 1\right) : 0 \le t \le \frac{3r}{2} - 2 \right\} \cup \left\{ s_{2} : 0 \le t \le \frac{3r}{2} - 2 \right\}$$
$$= \bigcup_{i=1}^{4} S_{3i}.$$

Assume that

$$S_{41} = \left\{ s_1 = (2r+t)q - (2r-t-1) : 0 \le t \le \frac{r}{2} - 2 \right\} \cup \left\{ s_2 : 0 \le t \le \frac{r}{2} - 2 \right\},$$

then

$$S_4 = S_{41} \cup \left\{ s_1 = (2r+t)q - (2r-t-1) : \frac{r}{2} - 1 \le t \le 2r - 2 \right\} \cup \left\{ s_2 : \frac{r}{2} - 1 \le t \le 2r - 2 \right\}.$$

In fact, we can get the skew asymmetric pairs (C_{s_1}, C_{s_2}) satisfying $s_1 > s_2$ in Λ form the set $S = S_1 \cup S_2 \cup S_{31} \cup S_{32} \cup S_{33} \cup S_{41}$.

Using a similar method to the proof of Lemma 5, one can derive the value of $|T_{ss}|$ in different cases.

By Lemmas 2 and 7, new EAQEC codes of length $n = \frac{q^2 - 1}{r}$, where *r* is an even divisor of q + 1, can be constructed from λ -constacyclic codes over \mathbb{F}_{q^2} of length *n* as follows.

Theorem 3 Let $r \ge 6$ be an even divisor of q + 1 and $a = \frac{q+1}{r} > 2$. Then for a fixed integer t with $0 \le t \le \frac{r}{2} - 2$, there are EAQEC codes with the following parameters

$$\begin{array}{l} (1) \ [[n,n-2d+2t+4,d;2(t+1)]]_q, \ where \ \frac{q+3}{2}+at \leq d \leq \frac{q+1}{2}+a(t+1) \ and \ t \leq \frac{r}{2}-3; \\ (2) \ [[n,n-2d+r,d;r-2]]_q, \ where \ q+2-2a \leq d \leq q; \\ (3) \ [[n,n-2d+r+2+2t,d;r+2t]]_q, \ where \ q+1+at \leq d \leq q+a(t+1); \\ (4) \ [[n,n-2d+2r,d;2r-2]]_q, \ where \ \frac{3}{2}(q+1)-a \leq d \leq \frac{3q-1}{2}; \\ (5) \ [[n,n-2d+2r+4+4t,d;2r+4t+2]]_q, \ where \ \frac{3q+3}{2}+at \leq d \leq \frac{3q-1}{2}+a(t+1); \end{array}$$

🖄 Springer

(6) $[[n, n-2d+4r-2, d; 4r-4]]_q$, where $2q + 1 - a \le d \le 2q - 1$; (7) $[[n, n-2d+4r+2+4t, d; 4r+4t]]_q$, where $2q + 1 + at \le d \le 2q - 1 + a(t+1)$; (8) $[[n, n-2d+6r-2, d; 6r-4]]_q$, where $\frac{5q+3}{2} - a \le d \le \frac{5q-3}{2}$, $a \ge 3$.

Remark 2 In fact, for r = 4, Lemma 7 and Theorem 3 are ture in the cases (2),(4),(6) and (8).

4 EAQMDS Codes with c = 1 or 2

An $[[n, k, d; c]]_q$ EAQMDS code can encode k logical qudits into n physical qudits by using c pairs of maximally entangled states, and can correct up to $\lfloor \frac{d-1}{2} \rfloor$ quantum errors. Thus, for fixed n and k, we wish that c would be smaller and d would be larger, in order to reduce the overhead in practice. In this section, two classes of EAQMDS codes consuming one or two pairs of maximally entangled states are obtained, whose minimum distances are larger than those in Theorems 2 and 3.

Lemma 8 Let r be an even divisor of q + 1 and $a = \frac{q+1}{r} > 2$. Let C be a λ -constacyclic code of length $n = \frac{q^2-1}{r}$ with defining set

$$T = \bigcup_{i=\frac{q+1}{2}-2a}^{k} C_{1+ri}, \text{ where } \frac{q+1}{2} - 2a \le k \le q-2$$

Assume that $T = T_{ss} \cup T_{sas}$, then (1) $(C_{1+r\frac{q-1}{2}}, C_{1+r(\frac{q-1}{2} - \frac{q+1}{r})})$ is a skew asymmetric pair; (2) $|T_{ss}| = 2$ if $\frac{q-1}{2} \le k \le q-2$.

Proof Since $-q(1 + r\frac{q-1}{2}) = -q(\frac{r}{2}q - (\frac{r}{2} - 1)) \equiv -\frac{r}{2} + (\frac{r}{2} - 1)q = 1 + r(\frac{q-1}{2} - \frac{q+1}{2}) \pmod{rn}$, then $(C_{1+r\frac{q-1}{2}}, C_{1+r(\frac{q-1}{2} - \frac{q+1}{2})})$ is a skew asymmetric pair.

If $\frac{q+1}{2} - 2a \le i \le q - 2$, then $(\frac{r}{2} - 2)q + \frac{r}{2} - 1 \le 1 + ri \le rq - 2r + 1$. Denote the set $\Lambda = \left[(\frac{r}{2} - 2)q + \frac{r}{2} - 1, rq - 2r + 1\right]_r$, then $T \le \Lambda$. Assume that

$$S = \left\{ s_1 : s_1 = \left(\frac{r}{2} + t\right) q - \left(\frac{r}{2} - t - 1\right), \ 0 \le t \le \frac{r}{2} - 2 \right\},\$$

obviously, $S \subseteq \Lambda$. By Lemma 6, we know

$$-qS = \left\{ s_2 : s_2 = \left(\frac{r}{2} - t - 1\right)q - \left(\frac{r}{2} + t\right), \ 0 \le t \le \frac{r}{2} - 2 \right\},\$$

and for fixed q and t, $s_1 > s_2$. If t = 0, then $s_1 = 1 + r\frac{q-1}{2}$ and $s_2 = 1 + r(\frac{q-1}{2} - \frac{q+1}{r}) \in \Lambda$, and (C_{s_1}, C_{s_2}) forms a skew asymmetric pair in Λ . Now we consider the case $1 \le t \le \frac{r}{2} - 2$. When t = 1, s_2 is the maximum one in -qS. And the value is $(\frac{r}{2} - 2)q - (\frac{r}{2} + 1)$, which is smaller than the smallest value $(\frac{r}{2} - 2)q + \frac{r}{2} - 1$ in Λ . Hence, $-qS \cap T = \{1 + r(\frac{q-1}{2} - \frac{q+1}{r})\}$ if $\frac{q-1}{2} \le k \le q - 2$.

Let

$$M = \left[\left(\frac{r}{2} - 1\right)q - \left(q - \frac{r}{2} + 1\right), \left(\frac{r}{2} - 1\right)q - \frac{3r}{2} \right]_{r},$$
$$L_{t} = \left[\left(\frac{r}{2} + t\right)q - \left(q - \frac{r}{2} - t\right), \left(\frac{r}{2} + t\right)q - \left(\frac{3r}{2} - t - 1\right) \right]_{r},$$

Deringer

 $N_1 = [(r-2)q - 1 + r, (r-1)q - r]_r$ and $N_2 = [rq - q, rq - (r-1) - r]_r$,

where $0 \le t \le \frac{r}{2} - 2$. Assume that $s_{(2,0)} = 1 + r(\frac{q-1}{2} - \frac{q+1}{r})$, then

$$\Lambda \setminus (S \cup \{s_{(2,0)}\}) = \bigcup_{t=0}^{\frac{r}{2}-2} L_t \bigcup_{i=1}^{2} N_i \cup M$$

and the intersections of M, L_t , and N_i are empty. Next, we claim that $-q(\Lambda \setminus (S \cup \{s_{(2,0)}\})) \cap T = \emptyset$. By Lemma 3, we can get

$$-qL_t = \left[\left(\frac{3r}{2}-t-1\right)q - \left(\frac{r}{2}+t\right), \left(q-\frac{r}{2}-t\right)q - \left(\frac{r}{2}+t\right)\right]_r,$$

where $0 \le t \le \frac{r-4}{2}$. When $t = \frac{r-4}{2}$, the value of $(\frac{3r-1}{2} - t)q - (\frac{r-1}{2} + t)$ is the minimum, and it is equal to (r + 1)q - (r - 2), which is bigger than the largest value rq - 2r + 1 in Λ . Thus $-qL_t \cap T = \emptyset$. Again by Lemma 3, we have

$$-qM = \left[\frac{3r}{2}q - \left(\frac{r}{2} - 1\right), \left(q - \frac{r}{2} + 1\right)q - \left(\frac{r}{2} - 1\right)\right]_{r},$$

$$-qN_{1} = [rq - (r-1), q - (r-2)]_{r} \text{ and } -qN_{2} = \left[(2r-1)q - r, q^{2} - r\right]_{r}.$$

And $\frac{3r}{2}q - (\frac{r}{2} - 1), rq - (r - 1)$ and (2r - 1)q - r are bigger than the largest value rq - 2r + 1in Λ . Hence, $-qM \cap T = \emptyset$ and $-qN_i \cap T = \emptyset$, i = 1, 2. Thus, $-q(\Lambda \setminus (S \cup \{s_{(2,0)}\})) \cap T = \emptyset$, and $T_{ss} = -qT \cap T = \left\{1 + r\frac{q-1}{2}, 1 + r(\frac{q-1}{2} - \frac{q+1}{r})\right\}$ if $\frac{q-1}{2} \le k \le q - 2$. The desired result follows.

Theorem 4 Let r be an even divisor of q + 1, $a = \frac{q+1}{r} > 2$. Then there exists a q-ary $[[n, n - 2d + 4, d; 2]]_q$ EAQMDS code, where $2a + 1 \le d \le 2a + \frac{q-1}{2}$.

Lemma 9 Let r be an odd positive divisor of q + 1, and $a = \frac{q+1}{r} > 1$. Let C be a λ -constacyclic code of length $n = \frac{q^2-1}{r}$ with defining set

$$T = \bigcup_{i=\frac{r-3}{2}a}^{k} C_{1+ri}, \text{ where } \frac{r-3}{2}a \le k \le q-2.$$

Assume that $T = T_{ss} \cup T_{sas}$, then (1) $C_{1+r\frac{q-1-a}{2}}$ is skew symmetric, (2) $|T_{ss}| = 1$ if $\frac{q-1-a}{2} \le k \le q-2$.

Deringer

Proof Notice that $-q(1+r\frac{q-1-a}{2}) = -q(\frac{r-1}{2}(q-1)) \equiv -\frac{r-1}{2} + \frac{r-1}{2}q = 1 + r\frac{q-1-a}{2} \pmod{rn}$, thus $C_{1+r\frac{q-1-a}{2}}$ is skew symmetric.

If $\frac{r-3}{2}a \le i \le q-2$, then $\frac{r-3}{2}q + \frac{r-1}{2} \le 1 + ri \le rq - 2r + 1$. Assume that $\Omega = \left[\frac{r-3}{2}q + \frac{r-1}{2}, rq - 2r + 1\right]_r$, then $T \subseteq \Omega$. Let

$$S = \left\{ s_1 : s_1 = \left(\frac{r-1}{2} + t \right) q - \left(\frac{r-1}{2} - t \right), 0 \le t \le \frac{r-3}{2} \right\},\$$

It can be checked easily that $S \subseteq \Omega$. By Lemma 4, we know

$$-qS = \left\{ s_2 : s_2 = \left(\frac{r-1}{2} - t\right)q - \left(\frac{r-1}{2} + t\right), 0 \le t \le \frac{r-3}{2} \right\}$$

For a fixed q, if t = 0, then $s_1 = s_2 = 1 + r\frac{q-1-a}{2} \in \Omega$. Now we consider the case $1 \le t \le \frac{r-3}{2}$. If t = 1, s_2 is the maximum in -qS and the value is $\frac{r-3}{2}q - \frac{r+1}{2}$ which is smaller than the smallest value $\frac{r-3}{2}q + \frac{r-1}{2}$ in Ω . Hence, $-qS \cap T = \left\{1 + r\frac{q-1-a}{2}\right\}$ if $\frac{q-1-a}{2} \le k \le q-2$. Let the sets

$$L_t = \left[\left(\frac{r-1}{2} + t\right) q - \left(q - \frac{r-1}{2} - t\right), \left(\frac{r-1}{2} + t\right) q - \left(\frac{3r-1}{2} - t\right) \right]_r$$
$$N_1 = \left[(r-2)q - 1 + r, (r-1)q - r \right]_r \text{ and } N_2 = [rq - q, rq - (2r-1)]_r,$$

where $0 \le t \le \frac{r-3}{2}$. Then $\Omega \setminus S = \bigcup_{t=0}^{\frac{r-3}{2}} L_t \bigcup_{i=1}^2 N_i$ and $L_t \cap N_i = \emptyset$. Next, we claim that $-q(\Omega \setminus S) \cap T = \emptyset$. By Lemma 3, we can get

$$-qL_{t} = \left[\left(\frac{3r-1}{2} - t \right) q - \left(\frac{r-1}{2} + t \right), \left(q - \frac{r-1}{2} - t \right) q - \left(\frac{r-1}{2} + t \right) \right]_{r},$$

where $0 \le t \le \frac{r-3}{2}$. When $t = \frac{r-3}{2}$, the value of $(\frac{3r-1}{2} - t)q - (\frac{r-1}{2} + t)$ is the minimum in the set $-qL_t$, and is equal to (r+1)q - (r-2), which is bigger than the largest value rq - 2r + 1 in Ω . Thus, $-qL_t \cap T = \emptyset$. Again by Lemma 3, we have

$$-qN_1 = [rq - (r-1), q - (r-2)]_r$$
 and $-qN_2 = [(2r-1)q - r, q^2 - r]_r$.

Notice that rq - (r - 1) and (2r - 1)q - r are bigger than the largest value of Ω . Thus, $-qN_i \cap T = \emptyset$, i = 1, 2 and $-q(\Omega \setminus S) \cap T = \emptyset$. Hence, $|T_{ss}| = 1$ if $\frac{q-1-a}{2} \le k \le q-2$.

Theorem 5 Let r be an odd divisor of q + 1, $a = \frac{q+1}{r} > 1$. Then there exists a q-ary $[[n, n-2d+3, d; 1]]_q$ EAQMDS code, where $a + 1 \le d \le \frac{q-1+3a}{2}$.

Proof Let $\lambda \in \mathbb{F}_{q^2}^*$ and $\operatorname{ord}(\lambda) = r$. Let C be a λ -constacyclic code of length $n = \frac{q^2 - 1}{r}$ with defining set $T = \bigcup_{i=\frac{r-3}{2}a}^k C_{1+ri}$, where $\frac{r-3}{2}a \le k \le q-2$. Then there are $k - \frac{r-3}{2}a + 1$ consecutive integers in T and $|T| = k - \frac{r-3}{2}a + 1$ since $|C_{1+ri}| = 1$. By Lemma 1, the minimum distance of C is not less than $k - \frac{r-3}{2}a + 2$. Then C is an MDS code. Applying Lemmas 2 and 9, the desired results follow.

	5	
$\overline{[[n,k,d;c]]_q}$	d in Thm 2	d in Refs.
$[[n, n - 2d + 7, d; 5]]_q, q > 13$	$q+1 \le d \le \frac{6q+1}{5}$	$q+1 \le d \le \frac{6q+1}{5}$ [24]
$[[n, n - 2d + 9, d; 7]]_q, q > 15$	$\frac{6(q+1)}{5} \le d \le \frac{7q-3}{5}$	$\frac{6(q+1)}{5} - 1 \le d \le \frac{7q-3}{5} \ [25]$
$[[n, n - 2d + 12, d; 10]]_q, q > 17$	$\frac{7(q+1)}{5} \le d \le \frac{8q-2}{5}$	New
$[[n, n - 2d + 16, d; 14]]_q, q \ge 19$	$\frac{8(q+1)}{5} \le d \le \frac{9q-1}{5}$	New
$[[n, n - 2d + 18, d; 16]]_q, q > 21$	$\frac{9q+4}{5} \le d \le 2q-1$	New
$[[n, n - 2d + 22, d; 20]]_q, q > 23$	$2q+1 \le d \le \frac{11q-4}{5}$	New
$[[n, n - 2d + 26, d; 24]]_q, q > 25$	$\frac{11q+6}{5} \le d \le \frac{12q-8}{5}$	New

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

Table 2 EAQMDS codes of length $n = \frac{q^2 - 1}{6}$ with $6 \mid (q + 1)$

$[[n, k, d; c]]_q$	d in Thm 3	d in Refs.
$[[n, n - 2d + 8, d; 6]]_q, q > 15$	$q+1 \le d \le \frac{7q+1}{6}$	$q+1 \le d \le \frac{7q+1}{6}$ [24]
$[[n, n - 2d + 10, d; 8]]_q, q > 17$	$\frac{7(q+1)}{6} \le d \le \frac{4q+1}{3}$	New
$[[n, n-2d+12, d; 10]]_q, q > 19$	$\frac{4(q+1)}{3} \le d \le \frac{3q-1}{2}$	New
$[[n, n - 2d + 16, d; 14]]_q, q > 21$	$\frac{3(q+1)}{2} \le d \le \frac{5q-1}{3}$	New
$[[n, n-2d+20, d; 18]]_q, , q \ge 23$	$\frac{5(q+1)}{3} \le d \le \frac{11q-1}{6}$	New
$[[n, n-2d+22, d; 20]]_q, q > 25$	$\frac{11q+5}{3} \le d \le 2q-1$	New
$[[n, n-2d+26, d; 24]]_q, q > 27$	$2q+1 \le d \le \frac{13q-5}{6}$	New
$[[n, n - 2d + 30, d; 28]]_q, q \ge 29$	$\frac{13q+7}{6} \le d \le \frac{7q-2}{3}$	New
$[[n, n - 2d + 34, d; 32]]_q, q > 31$	$\frac{7q+4}{3} \le d \le \frac{5q-3}{2}$	New

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

$\overline{[[n,k,d;c]]_q}$	<i>d</i> in Thm 2	d in Refs.
$[[n, n-2d+9, d; 7]]_q, q > 17$	$q+1 \le d \le \frac{8q+1}{7}$	$q+1 \le d \le \frac{8q+1}{7}$ [24]
$[[n, n - 2d + 11, d; 9]]_q, q > 19$	$\frac{8(q+1)}{7} \le d \le \frac{9q+2}{7}$	$\frac{8q+1}{7} \le d \le \frac{9q-5}{7}$ [25]
$[[n, n - 2d + 13, d; 11]]_q, q > 21$	$\frac{9(q+1)}{7} \le d \le \frac{10q-4}{7}$	$\frac{9q+2}{7} \le d \le \frac{10q-4}{7}$ [25]
$[[n, n - 2d + 16, d; 14]]_q, q > 23$	$\frac{10(q+1)}{7} \le d \le \frac{11q-3}{7}$	New
$[[n, n - 2d + 20, d; 18]]_q, q > 25$	$\frac{11(q+1)}{7} \le d \le \frac{12q-2}{7}$	New
$[[n, n - 2d + 24, d; 22]]_q, q \ge 27$	$\frac{12(q+1)}{7} \le d \le \frac{13q-1}{7}$	New
$[[n, n - 2d + 26, d; 24]]_q, q > 29$	$\frac{13q+6}{7} \le d \le 2q-1$	New
$[[n, n - 2d + 30, d; 28]]_q, q > 31$	$2q+1 \le d \le \frac{15q-6}{7}$	New
$[[n, n-2d+34, d; 32]]_q, q > 33$	$\frac{15q+8}{7} \le d \le \frac{16q-5}{7}$	New
$[[n, n - 2d + 38, d; 36]]_q, q > 35$	$\frac{16q+9}{7} \le d \le \frac{17q-11}{7}$	New

5 Code Comparisons

In this paper, we have derived a family of EAQEC codes from constacyclic codes over \mathbb{F}_{q^2} of length $n = \frac{q^2-1}{r}$, where *r* is a positive divisor of q + 1. Some standard quantum MDS codes with the same length have been obtained in [4, 15, 34], and their minimum distances are not greater than q + 1. The minimum distance of EAQEC codes in this paper is near by $\frac{5q-3}{2}$. If $d \leq \frac{n+2}{2}$, our EAQEC codes are MDS. There are many results [8, 24, 25, 27, 30] about the EAQMDS codes of length $\frac{q+1}{r}(q-1)$ for a certain *r*, our construction generalized almost known results with the same length. And our construction can produce many new EAQMDS codes with large minimum distance which are not covered in the literature.

Liu et al. [24] constructed EAQMDS codes of length $\frac{q^2-1}{r}$ from λ -constacyclic codes, where $3 \le r \le 7$. For other positive divisors of q + 1, the EAQMDS codes in this paper are new. In addition, the minimum distances in their construction are not more than $\frac{(r+1)(q+1)}{r} - 1$. Thus, if $\frac{(r+1)(q+1)}{r} \le d \le \min\left\{\frac{5q-3-a}{2}, \frac{n+2}{2}\right\}$ the EAQMDS codes in Theorems 2 and 3 are new.

Let q be an odd prime power. Recently, Lu et al. [25] constructed EAQMDS codes from cyclic codes of length $\frac{q^2-1}{r}$, where r = 3, 5, 7. The upper limit of minimum distance is $\frac{9q-6}{5}$ if r = 5, and $\frac{11q-10}{7}$ if r = 7, which are all less than $\frac{5q-3}{2}$. In Tables 1, 2 and 3, we compare some EAQMDS codes in this paper with these in [24, 25] when r = 5, 6 and 7, respectively. It can be seen that our construction in Theorems 2 and 3 can produce more codes processing bigger minimum distance.

If q is an odd prime power and r is odd, Fan et al. [8] derived EAQMDS codes with parameters $\left[\left[\frac{q^2-1}{r}, \frac{q^2-1}{r} - 2d + r + 2, d; r\right]\right]_q$, where $\frac{(r-1)(q+1)}{r} + 2 \le d \le \frac{(r+1)(q+1)}{r} - 2$. If r is even, the EAQMDS code in this paper are new. Obviously, $\frac{5q-3}{2} > \frac{(r+1)(q+1)}{r} - 2$. Thus, if $d \le \frac{n+2}{2}$ our construction can produce much more EAQMDS codes with large minimum distance. In Table 5, we compare some EAQMDS codes from our construction with the known ones in [8, 24, 25].

In Theorems 4 and 5, we improved the minimum distance of EAQMDS codes with c = 1 or 2 in Theorems 2 and 3. In Table 4, we compare some EAQMDS codes which consume one or two pairs of maximally entangled states in Theorems 4 and 5 with these in Theorems 2 and 3. The minimum distance of EAQMDS codes in Theorems 4 and 5 is larger $\frac{q+1}{r}$ than minimum

\overline{q}	r	Our parameters	d in Thms 4 or 5	d in Thms 2 or 3
17	6	$[[48, 52 - 2d, d; 2]]_{17}$	$7 \le d \le 14$	$10 \le d \le 12$
17	9	$[[32, 35 - 2d, d; 1]]_{17}$	$3 \le d \le 11$	$9 \le d \le 10$
23	6	$[[88, 92 - 2d, d; 2]]_{23}$	$9 \le d \le 19$	$13 \le d \le 16$
23	8	$[[66, 70 - 2d, d; 2]]_{23}$	$7 \le d \le 17$	$13 \le d \le 15$
29	6	$[[140, 144 - 2d, d; 2]]_{29}$	$11 \le d \le 24$	$16 \le d \le 20$
29	15	$[[56, 59 - 2d, d; 1]]_{29}$	$3 \le d \le 17$	$15 \le d \le 16$
31	8	$[[120, 124 - 2d, d; 2]]_{31}$	$9 \le d \le 23$	$17 \le d \le 20$
32	11	$[[93, 96 - 2d, d; 1]]_{32}$	$4 \le d \le 20$	$16 \le d \le 18$

Table 4 Some new EAQMDS codes with a few entanglement bits

\overline{q}	r	Our parameters	d in Thms 2 or 3	d in Refs.
17	6	$[[48, 56 - 2d, d; 6]]_{17}$	$18 \le d \le 20$	$18 \le d \le 20$ [24]
17	6	$[[48, 58 - 2d, d; 8]]_{17}$	$21 \le d \le 23$	New
17	6	$[[48, 60 - 2d, d; 10]]_{17}$	$24 \le d \le 25$	New
19	5	$[[72, 79 - 2d, d; 5]]_{19}$	$20 \le d \le 23$	$20 \le d \le 23$ [24]
19	5	$[[72, 81 - 2d, d; 7]]_{19}$	$24 \le d \le 26$	$23 \le d \le 26$ [25]
19	5	$[[72, 84 - 2d, d; 10]]_{19}$	$28 \le d \le 30$	New
19	5	$[[72, 88 - 2d, d; 14]]_{19}$	$32 \le d \le 34$	New
19	5	$[[72, 90 - 2d, d; 16]]_{19}$	$35 \le d \le 37$	New
23	8	$[[66, 72 - 2d, d; 4]]_{23}$	$16 \le d \le 18$	New
23	8	$[[66, 74 - 2d, d; 6]]_{23}$	$19 \le d \le 23$	New
23	8	$[[66, 76 - 2d, d; 8]]_{23}$	$24 \le d \le 26$	New
23	8	$[[66, 78 - 2d, d; 10]]_{23}$	$27 \le d \le 29$	New
23	8	$[[66, 80 - 2d, d; 12]]_{23}$	$30 \le d \le 32$	New
23	8	$[[66, 82 - 2d, d; 14]]_{23}$	$33 \le d \le 34$	New
53	9	$[[312, 317 - 2d, d; 3]]_{53}$	$31 \le d \le 36$	New
53	9	$[[312, 319 - 2d, d; 5]]_{53}$	$37 \le d \le 42$	New
53	9	$[[312, 321 - 2d, d; 7]]_{53}$	$43 \le d \le 53$	New
53	9	$[[312, 323 - 2d, d; 9]]_{53}$	$54 \le d \le 59$	$50 \le d \le 58$ [8]
53	9	$[[312, 325 - 2d, d; 11]]_{53}$	$60 \le d \le 65$	New
53	9	$[[312, 327 - 2d, d; 13]]_{53}$	$66 \le d \le 71$	New
53	9	$[[312, 329 - 2d, d; 15]]_{53}$	$72 \le d \le 76$	New
53	9	$[[312, 332 - 2d, d; 18]]_{53}$	$78 \le d \le 82$	New
53	9	$[[312, 336 - 2d, d; 22]]_{53}$	$84 \le d \le 88$	New
53	9	$[[312, 340 - 2d, d; 26]]_{53}$	$90 \le d \le 94$	New
53	9	$[[312, 344 - 2d, d; 30]]_{53}$	$96 \le d \le 100$	New
53	9	$[[312, 346 - 2d, d; 32]]_{53}$	$101 \le d \le 105$	New
53	9	$[[312, 350 - 2d, d; 36]]_{53}$	$107 \le d \le 111$	New
53	9	$[[312, 354 - 2d, d; 40]]_{53}$	$113 \le d \le 117$	New
53	9	$[[312, 358 - 2d, d; 44]]_{53}$	$119 \le d \le 123$	New
53	9	$[[312, 362 - 2d, d; 48]]_{53}$	$125 \le d \le 128$	New

Table 5 Some new EAQMDS codes and comparisons

distance of the standard quantum MDS codes in [34]. Let *q* be an odd prime power. In [27], the authors obtained EAQMDS codes with parameters $\left[\left[\frac{q^2-1}{r}, \frac{q^2-1}{r} - 2d + r + 2, d; 1\right]\right]_q$, where r = 3, 5, 7 and $\frac{q+1}{r} + 1 \le d \le \frac{(r+3)(q+1)}{2r} - 1$. Our construction in Theorems 4 and 5 generalized this result. Many new EAQMDS codes could be derived from Theorem 4 if *r* is even, and Theorem 5 if *q* is even, or *r* is another odd divisor of q + 1.

Acknowledgements This study is supported by the National Natural Science Foundation of China (No.61972126, No.62002093, No.U21A20428, No.12171134)

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

Declarations

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

References

- 1. Bowen, G.: Entanglement required in achieving entanglement-assisted channel capacities. Phys. Rev. A **66**, 052313 (2002)
- Brun, T., Devetak, I., Hsieh, M.H.: Correcting quantum errors with entanglement. Science 52, 436–439 (2006)
- Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over GF(4). IEEE. Trans. Inf. Theory 44, 1369–1387 (1998)
- Chen, B., Ling, S., Zhang, G.: Applications of constacyclic codes of quantum MDS codes. IEEE Trans. Inf. Theory 61, 1474–1484 (2015)
- Chen, J., Huang, Y., Feng, C., Chen, R.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. Quantum Inf. Process. 16, 303 (2017)
- Chen, X., Zhu, S., Jiang, W.: Cyclic codes and some new entanglement-assisted quantum MDS codes. Des. Codes Cryptogr. 89, 2533–2551 (2021)
- Chen, X., Zhu, S., Jiang, W., Luo, G.: A new family of EAQMDS codes constructed from constacyclic codes. Des. Codes Cryptogr. 89, 2179–2193 (2021)
- 8. 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)
- 9. Galindo, C., Hernando, F., Matsumoto, R., Ruano, D.: Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. Quantum Inf. Process. 18, 116 (2019)
- 10. Grassl, M.: Entanglement-assisted quantum communication beating the quantum Singleton bound. Talk at AQIS, Taiwan (2016)
- Hsieh, M.H., Brun, T.A., Devetak, I.: Entanglement-assisted quantum quasi-cyclic low-density paritycheck codes. Phys. Rev. A 79, 032340 (2009)
- Hsieh, M.H., Devetak, I., Brun, T.: General entanglement-assisted quantum error-correcting codes. Phys. Rev. A 76, 62313 (2007)
- 13. Hu, P., Liu, X.: EAQEC codes from two distinct constacyclic codes. Quantum Inf. Process. 22, 100 (2023)
- Jiang, W., Zhu, S., Chen, X.: New EAQMDS codes constructed from negacyclic codes. Quantum Inf. Process. 19, 1–19 (2020)
- Kai, X., Zhu, S., Li, P.: Constacyclic codes and some new quantum MDS codes. IEEE Trans. Inf. Theory 60, 2080–2086 (2014)
- Ketkar, A., Klappenecker, A., Kumar, S.: Nonbinary stablizer codes over finite fields. IEEE Trans. Inf. Theory 52, 4892–4914 (2006)
- Lai, C.Y., Ashikhmin, A.: Linear programming bounds for entanglement-assisted quantum error correcting codes by spit weight enumerators. IEEE Trans. Inf. Theory 64, 622–639 (2018)
- Lai, C.Y., Brun, T.A.: Entanglement-assisted quantum error-correcting codes with imperfect ebits. Phys. Rev. A 86, 032319 (2012)
- Li, R., Xu, G., Lv, L.: Decomposition of defining sets of BCH codes and its applications. J. Air Force Eng. Univ. (Natl. Sci. Ed.) 14, 86–89 (2013) (in Chinese)
- Li, R., Zuo, F., Liu, Y.: A study of skew asymmetric q²-cyclotomic coset and its application, J. Air Force Eng. Univ. (Natl. Sci. Ed.) 12, 87–89 (2011) (in Chinese)
- Li, R., Zuo, F., Liu, Y., Xu, Z.: Hermitian dual containing BCH codes and Construction of new quantum codes. Quantum Inf. Comput. 13, 0021 (2013)
- Li, Y., Wan, R., Zhu, S.: MDS codes with Euclidean and Hermitian hulls of flexible dimensions and their applications to EAQECCs. Quantum Inf. Process. 22, 153 (2023)
- Liu, J., Lin, L.: Galois hulls of special Goppa codes and related codes with application to EAQECCs. Finite Fields Appl. 88, 102183 (2023)
- Liu, Y., Li, R., Lv, L., Ma, Y.: Application of constacyclic codes to entanglement-assisted quantum maximum distance separable codes. Quantum Inf. Process. 17, 210 (2018)
- Lu, H., Kai, X., Zhu, S.: Construction of new entanglement-assisted quantum MDS codes via cyclic codes. Quantum Inf. Process. 21, 206 (2022)
- Lu, H., Kai, X., Zhu, S.: Three new classes of entanglement-assisted quantum MDS codes from cyclic codes. Int. J. Theor. Phys. 61, 254 (2022)

- Lu, L., Ma, W., Guo, L.: Two families of entanglement-assisted quantum MDS codes from constacyclic codes. Int. J. Theor. Phys. 59, 1657–1667 (2020)
- Qian, J., Zhang, L.: On MDS linear complementary dual codes and entanglement-assisted quantum codes. Des. Codes Cryptogr. 86, 1565–1572 (2018)
- Qian, J., Zhang, L.: Constructions of new entanglement-assisted quantum MDS codes and almost MDS codes. Quantum Inf. Process. 18, 1–12 (2019)
- Sari, M., Kolotoğlu, E.: An application of constacyclic codes to entanglement-assisted quantum MDS codes. Comput. Appl. Math. 38, 1–13 (2019)
- Wang, G., Tang, C.: Application of GRS codes to some entanglement-assisted quantum MDS codes. Quantum Inf. Process. 21, 98 (2022)
- Wang, J., Li, R., Lv, J., Song, H.: Entanglement-assisted quantum codes from cyclic codes and negacyclic codes. Quantum Inf. Process. 19, 138 (2020)
- Wang, L., Wang, P.: Some new families of entanglement-assisted quantum MDS codes derived from negacyclic codes. Quantum Inf. Process. 21, 318 (2022)
- Wang, L., Zhu, S.: New quantum MDS codes derived from constacyclic codes. Quantum Inf. Process. 14, 881–889 (2015)
- Wilde, M.M., Brun, T.A.: Optimal entanglement formulas for entanglement-assisted quantum coding. Phys. Rev. A 77, 64302 (2008)
- Yang, Y., Cai, W.: On self-dual constacyclic codes over finite fields. Des. Codes Cryptogr. 74, 355–364 (2013)

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

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.