Quantum Information Processing (2020) 19:138
https://doi.org/10.1007/s11128-020-02636-2

Entanglement-assisted quantum codes from cyclic codes and negacyclic codes

Junli Wang[1] · Ruihu Li[1] · Jingjie Lv[1] · Hao Song[1]

Received: 15 July 2019 / Accepted: 5 March 2020 / Published online: 16 March 2020

Abstract

Entanglement-assisted quantum error-correcting (EAQEC) codes could generalize and improve performance of standard quantum error-correcting (QEC) codes to a great extent. In this paper, series of EAQEC codes of length $n = \frac{q-1}{a}(q+1)$ are constructed from cyclic codes and negacyclic codes, where q is a prime power and a is a positive integer such that $a \mid (q-1)$. It turns out that the number of required entanglement bits can take almost all possible values. Consequently, our EAQEC codes have flexible parameters and most of them are new. For given the same length, our construction contain and extend those known consequences in Grassl et al. (Int J Quantum Inf 2(1):55–64, 2004), Jin et al. (IEEE Trans Inf Theory 56:4735–4740, 2010), Kai et al. (IEEE Trans Inf Theory 60:2080–2086, 2014), Jin and Xing (IEEE Trans Inf Theory 60:2921–2925, 2014), Chen et al. (IEEE Trans Inf Theory 61:1474–1484, 2015), Zhang and Ge (IEEE Trans Inf Theory 61:5224–5228, 2015; Des Codes Cryptogr 83(3):503–517, 2016), Shi et al. (Cryptogr Commun 10(6):1165–1182, 2018; Finite Fields Appl 46:347–362, 2017), Fan et al. (Quantum Inf Comput 16:423–434, 2016), Lu et al. (Quantum Inf Process 17(69):1–23, 2018), Li et al. (Int J Quantum Inf 17(1):1950022, 2019), Liu et al. (Quantum Inf Process 17(210):1–19, 2018), Fang et al. (Euclidean and Hermitian Hulls of MDS Codes and Their Applications to EAQECCs. arXiv:https://arxiv.org/abs/1812.09019v3). Above all, all our codes are maximum-distance-separable (MDS) if their minimum distance $d \leq \frac{n+2}{2}$.

Keywords Cyclic code · Negacyclic code · Cyclotomic coset · EAQEC code

This work is supported by National Natural Science Foundation of China under Grant Nos. 11471011, 11801564 and Natural Science Foundation of Shaanxi under Grant No. 2017JQ1032.

✉ Ruihu Li
llzsy2015@163.com

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

1 Introduction

In 1995, Shor [1] presented the first QEC code $[[9, 1, 3]]$ to reduce decoherence in quantum computation. Afterward, binary or nonbinary stabilizer QEC codes were of particular interest and investigated by many researchers, see Refs. [2–10]. Calderbank et al. clarified that binary QEC codes could come from classical codes over $\mathbb{F}_2$ or $\mathbb{F}_4$ in [2]. Later, in [5], Ketkar et al. made it clear that q-ary QEC codes can be constructed from Hermitian self-orthogonal classical codes over $\mathbb{F}_{q^2}$ or from Euclidean self-orthogonal classical codes over $\mathbb{F}_q$. In the past years, constructing QEC codes, denoted as $[[n, k, d]]_q$, with good parameters has become a central topic in coding field. A QEC code is optimal if its parameters satisfy $k = n - 2d + 2$ and called a quantum MDS (QMDS) code. Naturally, many consequences on QMDS codes have been verified in [11–19].

It is well known that the self-orthogonality conditions mentioned above prevent many common classical codes from producing QEC codes. To weaken self-orthogonality condition and simplify the theory of QEC codes, Brun et al. [20] presented entanglement-assisted formalism to obtain entanglement-assisted QEC (EAQEC) codes from any classical linear codes. They showed that EAQEC codes, denoted as $[[n, k, d; c]]_q$, are feasible if pre-shared entanglement bits between the encoder and decoder are available. Clearly, an EAQEC code is a standard QEC code if the number of entanglement bits is $c = 0$. Moreover, EAQEC codes are MDS if they achieve the following EA-Singleton bound. Such codes are called entanglement-assisted QMDS (EAQMDS) codes.

Lemma 1 (EA-Singleton Bound, [20–22]) *For any $[[n, k, d; c]]_q$ EAQEC code, if $d \leq \frac{n+2}{2}$, then it satisfies $2d \leq n - k + c + 2$, where $0 \leq c \leq n - 1$.*

Recently, many EAQMDS codes have been derived from constacyclic codes or generalized Reed-Solomon (GRS) codes, extended GRS codes, see Refs. [23,25–30]. Fan et al. [23] proposed three classes of EAQMDS codes by utilizing only one entanglement bit. In 2018, Lu et al. [25,26] constructed classes of EAQMDS codes with some special lengths by consuming one entanglement bit or four entanglement bits. In [28], Li et al. obtained a family of EAQMDS codes of length $n = \frac{q-1}{2a}(q + 1)$ from negacyclic codes and made a general statement of $c \leq 2a$ instead of some specific values. Liu et al. [29] applied constacyclic codes to EAQMDS codes with length $n = \frac{q+1}{r}(q - 1)$ by determining the value of c from 1 to r, where $3 \leq r \leq 7$. Using more flexible entanglement bits to construct EAQEC codes always means more difficult to verify their parameters. In 2019, Qian et al. [27] derived a family of EAQEC codes with flexible parameters from cyclic codes. Via GRS codes and extended GRS codes, Fang et al. also obtained several families of EAQMDS codes with flexible parameters in [30].

It is fortunate to find that more and more conclusions on EAQEC codes with flexible parameters have been made in recent years although it is hard to determine their required entanglement bits. As shown in the papers mentioned above, the minimum distance of EAQEC codes or EAQMDS codes increased remarkably with the help of pre-shared entanglement bits. However, almost all of them did not use the entanglement resource fully or merely discussed some sparse special lengths under certain conditions. In this paper, we pay attention to constructing EAQEC codes of length $n = \frac{q-1}{a}(q+1)$ from cyclic codes and negacyclic codes, where $a \mid (q-1)$ and $q \geq 2a+1$. By deeply investigating properties of q^2-cyclotomic cosets modulo rn, where $r = 1$ or $r = 2$, we clarify that the number of entanglement bits can take almost all possible values. That is to say, our construction can produce series of new EAQEC codes with large minimum distance and generalize almost all known results with the same length in [11–19,23,26,28–30]. In particular, all our codes are EAQMDS codes if their minimum distance $d \leq \frac{n+2}{2}$.

The paper is organized as follows. In Sect. 2, some basic notions and preliminaries are recalled. In Sects. 3 and 4, EAQEC codes of length $n = \frac{q-1}{a}(q+1)$ are constructed from cyclic codes and negacyclic codes, respectively. In Sect. 5, some remarks and comparisons are made finally.

2 Preliminaries

In this section, we recall some basic concepts on constacyclic codes, cyclotomic cosets and EAQEC codes. For more details, we may refer to Refs. [20,21,31,32].

Let q be a prime power and $\mathbb{F}_{q^2}$ be a finite field with q^2 elements. For any $\alpha \in \mathbb{F}_{q^2}$, $\overline{\alpha} = \alpha^q$ is denoted as the conjugation of α. Given two vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ in $\mathbb{F}_{q^2}^n$, their Hermitian inner product is defined by

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

A linear code $\mathcal{C}$ with length n over $\mathbb{F}_{q^2}$ is said to be a k-dimension subspace of $\mathbb{F}_{q^2}^n$, which is denoted by $[n, k]_{q^2}$. Hermitian dual code of $\mathcal{C}$ is defined as

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

For any codeword $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, if $(\lambda c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is still a codeword in $\mathcal{C}$, then $\mathcal{C}$ is called a λ-constacyclic code, where $\lambda \in \mathbb{F}_{q^2} \backslash \{0\}$. Particularly, if $\lambda = 1$, then $\mathcal{C}$ is a cyclic code; if $\lambda = -1$, then $\mathcal{C}$ is a negacyclic code. Denote that $r = \mathrm{ord}_{q^2}(\lambda)$, then one can get that $\mathcal{C}$ is a cyclic code if $r = 1$ and $\mathcal{C}$ is a negacyclic code if $r = 2$ by definition.

Define a mapping φ from $\mathbb{F}_{q^2}^n$ to $\mathcal{R}_n = \frac{\mathbb{F}_{q^2}[x]}{\langle x^n - \lambda \rangle}$ as follows:

$$(c_0, c_1, \ldots, c_{n-1}) \mapsto c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}.$$

One can check that $\mathcal{C}$ is a λ-constacyclic code with length n over $\mathbb{F}_{q^2}$ if and only if $\varphi(\mathcal{C})$ is an ideal of quotient ring $\mathcal{R}_n$. Thus, there exists a monic polynomial divisor $g(x)$ of $x^n - \lambda$ with the least degree such that $g(x)$ generates $\mathcal{C}$, i.e., $\mathcal{C} = \langle g(x) \rangle$. It is well known that $\mathcal{C}$ has dimension $k = n - \deg(g(x))$. Let $\gcd(q, n) = 1$, $\Omega_{r,n} = \{1 + ir \mid 0 \leq i \leq n-1\}$ and ζ be a primitive rnth root of unity in some extension field of $\mathbb{F}_{q^2}$ such that $\zeta^n = \lambda$. For any $j \in \Omega_{r,n}$, q^2-cyclotomic coset C_j modulo rn containing j is defined by

$$C_j = \{j, jq^2, j(q^2)^2, \ldots, j(q^2)^{l-1}\} \bmod rn,$$

where l is the smallest positive integer such that $j(q^2)^l \equiv j \bmod rn$. The defining set of $\mathcal{C}$ is the set $T = \{j \in \Omega_{r,n} | g(\zeta^j) = 0\}$. Obviously, we can see that T is a union of some q^2-cyclotomic cosets modulo rn and the dimension of $\mathcal{C}$ is $k = n - |T|$.

The following lemma can be used to determine minimum distance of a λ-constacyclic code.

Lemma 2 (The BCH bound for λ-constacyclic codes, [34,35]) *Let $\mathcal{C}$ be a q^2-ary λ-constacyclic code of length n with generator polynomial $g(x)$. If $g(x)$ has its elements $\{\zeta^{1+ir} | 0 \le i \le \delta - 2\}$ as roots, where ζ is a primitive rnth root of unity, then the minimum distance of $\mathcal{C}$ is at least δ.*

As to compute the parameters of EAQEC codes constructed from a linear code $\mathcal{C}$, we need to determine the optimal number of required entanglement bits c. Wilde et al. [21] provided a formula that $c = rank(HH^\dagger)$, where H is a parity check matrix of $\mathcal{C}$ and $H^\dagger$ is conjugate transpose of H. Further, for EAQEC codes obtained from constacyclic codes (including cyclic codes and negacyclic codes), the authors in [24,29,33] proposed decomposition of their defining set to count the value of c instead of calculating $rank(HH^\dagger)$ as follows.

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

Using the definition above, parameters of the EAQEC codes constructed from constacyclic codes can be confirmed readily.

Theorem 1 ([29], Theorem 1) *Let $\mathcal{C}$ be an $[n, k, d]_{q^2}$ λ-constacyclic code with defining set T. Suppose decomposition of T is $T = T_{ss} \bigcup T_{sas}$. Then there exists an $[[n, n - 2|T| + |T_{ss}|, d; |T_{ss}|]]_q$ EAQEC code.*

From now on till the end of this paper, we give some notations beforehand to make the discussions in the sequel simple.

Notation 1 Set $n = \frac{q-1}{a}(q+1) = a'(q+1)$, where $q \ge 2a+1$ is a prime power and $aa' = q - 1$. Given a symbol $\mathcal{S}$, $|\mathcal{S}|$ is defined as its cardinality if $\mathcal{S}$ is a set and its absolute value if $\mathcal{S}$ is an integer. Denote the sequence $\{b, b+1, \ldots, e\}$ by $[b, e]$, where $b < e$. For $\mu \in [b, e]$, denote that $\underline{\mu} = [b, e]$.

Throughout this paper, we study EAQEC codes derived from cyclic codes or negacyclic codes with length n, i.e., $r = 1$ or $r = 2$. Note that $i(q^2 - 1) \equiv 0 \bmod rn$ holds for all $1 \le i \le n - 1$. Thus, it is easy to see that any q^2-cyclotomic coset modulo rn has only one element.

3 Construction of EAQEC codes from cyclic codes with length n

In this section, we investigate the properties of q^2-cyclotomic cosets modulo n first of all. Then, by decomposition of defining set, the number of entanglement bits can be determined precisely. Consequently, series of EAQEC codes could be obtained from these cyclic codes.

Lemma 3 *Let n, q, a, a' be given as above.*

(1) *For $i \equiv 0 \bmod a'$, any C_i is a skew symmetric coset.*
(2) *For $i \in [1, n-1]$, let $i = ua' + v$, where $v \in [1, a']$ if $u \in [0, q-1]$ and $v \in [1, a'-1]$ if $u = q$. Then,*

$$-qC_{ua'+v} = \begin{cases} C_{(u-1-va)a'+a'-v} & \text{if } u-1-va \geq 0; \\ C_{(q+u-va)a'+a'-v} & \text{if } u-1-va < 0. \end{cases}$$

Proof (1) Assume that there exists a skew symmetric coset C_i, then there holds $i(q+1) \equiv 0 \bmod n \Leftrightarrow i \equiv 0 \bmod a'$. Clearly, our desired result has been clarified.
(2) Note that any q^2-cyclotomic coset C_i contains one element. From $-q(ua'+v) = -ua'(q+1) + ua' - v(q-1) - v = -ua'(q+1) + (u-1-va)a' + a' - v$, one can see that $-q(ua'+v) \equiv (u-1-va)a' + a' - v \bmod n$ if $u-1-va \geq 0$ and $-q(ua'+v) \equiv (q+u-va)a' + a' - v \bmod n$ if $u-1-va < 0$. Thus, (2) holds.

□

Lemma 4 *Let n, q, a, a' be given as above. Denote that $f \in [1, a'-1]$ if $e = 0$ and $f \in [\lceil \frac{e}{a} \rceil, a'-1]$ if $e \in [1, a(a'-1)]$. Set $T_1 = \bigcup C_{ea'+f}$, there holds $T_1 \bigcap -qT_1 = \emptyset$.*

Proof From Lemma 3 (2), one needs to verify firstly that if $e-1-fa < 0$ or not. Indeed, $e-1-fa < 0$ holds when $e = 0$. When $e \in [1, a(a'-1)]$, $f \in [\lceil \frac{e}{a} \rceil, a'-1]$, it is easy to check that $e-1-fa \leq e - \lceil \frac{e}{a} \rceil a - 1 < 0$ as well. Thus, we have that $-qT_1 = \bigcup C_{(q+e-fa)a'+a'-f}$.

Suppose that $T_1 \bigcap -qT_1 \neq \emptyset$, from $T_1 = \bigcup C_{ea'+f}$ and the range of e, f, there are two cases as below.

Case 1: When $e = 0$, one can see that $\underline{q+e-fa} \subseteq \underline{e}\setminus\{0\}$ then $a'-f \geq \lceil \frac{q+e-fa}{a} \rceil = \lceil \frac{q-fa}{a} \rceil > a'-f$, a contradiction.

Case 2: When $e \in [1, a(a'-1)]$, we also have that $\underline{q+e-fa} \subseteq \underline{e}\setminus\{0\}$. Note that $a'-f \geq \lceil \frac{q+e-fa}{a} \rceil > a'-f$, a contradiction.

Till now, our claim holds. □

As shown in Theorem 1, one could know the number of entanglement bits by calculating the cardinality of T_{ss}.

Theorem 2 *Let n, q, a, a' be given as above. Keep the notations defined in* Lemma 4. *If $\mathcal{C}$ is a cyclic code with defining set $T = C_1 \bigcup C_2 \bigcup \cdots \bigcup C_{\beta a'+a'-1}$, where $\beta \in [0, q]$,* *then*

$$|T_{ss}| = \begin{cases} \beta & \textit{for } \beta \in [0, a]; \\ \beta + \sum\limits_{k=a+1}^{\beta} 2\left(\left\lceil \frac{k}{a} \right\rceil - 1\right) & \textit{for } \beta \in [a+1, q-1]; \\ n-1 & \textit{for } \beta = q. \end{cases}$$

Proof See in "Appendix 1". □

After the detailed analysis on cyclotomic cosets modulo n and defining set of certain cyclic codes of length n, one can construct EAQEC codes from these cyclic codes naturally.

Theorem 3 *Let n, q, a, a' be given as above. Keep the notations defined in* Lemma 4 *and* Theorem 2. *There exist EAQEC codes with parameters* $[[n, n-2(d-1)+c, d; c]]_q$.

(1) *If $q = 2a + 1$, then*

$$\begin{cases} d \in [2, a'], c = 0 & \textit{for } \beta = 0; \\ d \in [\beta a' + 1, (\beta+1)a'], c = \beta & \textit{for } \beta \in [1, a]; \\ d = n, c = n-1 & \textit{for } \beta = q. \end{cases}$$

(2) *If $q \geq 3a + 1$, then*

$$\begin{cases} d \in [2, a'], c = 0 & \textit{for } \beta = 0; \\ d \in [\beta a' + 1, (\beta+1)a'], c = \beta & \textit{for } \beta \in [1, a]; \\ d \in [\beta a' + \left\lceil \frac{\beta}{a} \right\rceil, (\beta+1)a'], c = \beta + \sum\limits_{k=a+1}^{\beta} 2\left(\left\lceil \frac{k}{a} \right\rceil - 1\right) & \textit{for } \beta \in [a+1, q-a-1]; \\ d = n, c = n-1 & \textit{for } \beta = q. \end{cases}$$

Particularly, for $\beta \in [0, \frac{q-1}{2}]$, these EAQEC codes are EAQMDS codes.

Proof According to different q, we can calculate the exact parameters of EAQEC codes with length n for given minimum distance.

Note that any q^2-cyclotomic coset contains only one element. It is clear that the cyclic code $\mathcal{C}$ with defining set $T = C_1 \bigcup C_2 \bigcup \cdots \bigcup C_{d-1}$ is an MDS code with parameters $[n, n-d+1, d]_{q^2}$. From Theorems 1 and 2, one can obtain series of $[[n, n-2(d-1)+c, d; c]]_q$ EAQEC codes easily.

For $\beta \in [0, \frac{q-1}{2}]$, there holds $d \leq (\beta+1)a' = \frac{n}{2}$. Then, one can conclude that the constructed EAQEC codes above are EAQMDS codes since all of them saturate the EA-Singleton bound when $\beta \in [0, \frac{q-1}{2}]$. □

4 Construction of EAQEC codes from negacyclic codes with length *n*

In this section, the properties of q^2-cyclotomic cosets modulo $2n$ are investigated in detail. From these results, many EAQEC codes with length n could be constructed from negacyclic codes. Set $r = 2$, $r \mid a$ qnd $aa' = q - 1$, then, a is an even positive integer and q is an odd prime power.

Table 1 New EAQEC codes with length $n = q^2 - 1$

q	Paras.	d	From	Paras.	d	Refs.
3	$[[8, 10 - 2d, d; 0]]_3$	$d = 2$	Th.3(1)	$[[8, 10 - 2d, d]]_3$	$d \leq 2$	[11,14,19]
	$[[8, 11 - 2d, d; 1]]_3$	$d = 3$		$[[8, 5, 3; 1]]_3$	$d = 3$	[30]
	$*[[8, 11 - 2d, d; 1]]_3$	$d = 4$				
	$[[8, 17 - 2d, d; 7]]_3$	$d = 8$		$[[8, 1, 8; 7]]_3$	$d = 8$	
4	$[[15, 17 - 2d, d; 0]]_4$	$2 \leq d \leq 3$	Th.3 (2)	$[[15, 17 - 2d, d]]_4$	$d \leq 3$	[11,14,19]
	$[[15, 18 - 2d, d; 1]]_4$	$d = 4$		$[[15, 10, 4; 1]]_4$	$d = 4$	[30]
	$*[[15, 18 - 2d, d; 1]]_4$	$5 \leq d \leq 6$				
	$\diamond[[15, 21 - 2d, d; 4]]_4$	$8 \leq d \leq 9$				
	$[[15, 31 - 2d, d; 14]]_4$	$d = 15$		$[[15, 1, 15; 14]]_4$	$d = 15$	
5	$[[24, 26 - 2d, d; 0]]_5$	$2 \leq d \leq 4$	Th.3(2)	$[[24, 26 - 2d, d]]_5$	$d \leq 4$	[11,14,19]
	$[[24, 27 - 2d, d; 1]]_5$	$d = 5$		$[[24, 17, 5; 1]]_5$	$d = 5$	[30]
	$*[[24, 27 - 2d, d; 1]]_5$	$6 \leq d \leq 8$				
	$*[[24, 30 - 2d, d; 4]]_5$	$10 \leq d \leq 12$				
	$\diamond[[24, 35 - 2d, d; 9]]_5$	$15 \leq d \leq 16$				
	$[[24, 49 - 2d, d; 23]]_5$	$d = 24$		$[[24, 1, 24; 23]]_5$	$d = 24$	
7	$[[48, 50 - 2d, d; 0]]_7$	$2 \leq d \leq 6$	Th.3(2)	$[[48, 50 - 2d, d]]_7$	$d \leq 6$	[11,14,19]
	$[[48, 51 - 2d, d; 1]]_7$	$d = 7$		$[[48, 37, 7; 1]]_7$	$d = 7$	[30]
	$*[[48, 51 - 2d, d; 1]]_7$	$8 \leq d \leq 12$				
	$*[[48, 54 - 2d, d; 4]]_7$	$14 \leq d \leq 18$				
	$*[[48, 59 - 2d, d; 9]]_7$	$21 \leq d \leq 24$				
	$\diamond[[48, 66 - 2d, d; 16]]_7$	$28 \leq d \leq 30$				
	$\diamond[[48, 75 - 2d, d; 25]]_7$	$35 \leq d \leq 36$				
	$[[48, 97 - 2d, d; 47]]_7$	$d = 48$		$[[48, 1, 48; 47]]_7$	$d = 48$	

Lemma 5 *Let n, q, a, a' be given as above. Denote that $i \in [0, n - 1]$.*

(1) *Any C_{1+2i} is a skew asymmetric coset.*

(2) *Let $i = ua' + v$, where $u \in [0, q]$, $v \in [0, a' - 1]$. Then,*

$$-qC_{1+2(ua'+v)} = \begin{cases} C_{1+2((u-va-\frac{a}{2}-1)a'+a'-1-v)} & \text{if } u - va - \frac{a}{2} - 1 \geq 0; \\ C_{1+2((q+u-va-\frac{a}{2})a'+a'-1-v)} & \text{if } u - va - \frac{a}{2} - 1 < 0. \end{cases}$$

Proof (1) Suppose that C_{1+2i} is skew symmetric, one can derive that $(1+2i)(q+1) \equiv 0 \bmod 2n = 2a'(q+1) \Leftrightarrow 1+2i \equiv 0 \bmod 2a'$. Actually, $1+2i$ is an odd integer, so this congruence cannot hold. Then, (1) follows.

(2) If $i = ua' + v$, then $C_{1+2i} = C_{1+2(ua'+v)} = \{1 + 2(ua' + v)\}$. Thus, from $-q(1+2(ua'+v)) = -q-2(q+1)ua'+2ua'-2qv = -(q-1)-2(q-1)v+2ua'-2(q+1)ua'-1-2v \equiv 1+2((u-va-\frac{a}{2}-1)a'+a'-1-v) \bmod 2n$, it follows that $-q(1+2(ua'+v)) \equiv 1+2((u-va-\frac{a}{2}-1)a'+a'-1-v) \bmod 2n$ if $u - va - \frac{a}{2} - 1 \geq 0$ and $-q(1+2(ua'+v)) \equiv 1+2((q+u-va-\frac{a}{2})a'+a'-1-v) \bmod 2n$ if $u - va - \frac{a}{2} - 1 < 0$. □

Table 2 New EAQEC codes with length $n = \frac{q-1}{2}(q+1)$

q	Paras.	d	From	Paras.	d	Refs.
(a)						
5	$[[12, 14-2d, d; 0]]_5$	$d = 2$	Th.3(1)			
	$[[12, 15-2d, d; 1]]_5$	$d = 3$		$[[12, 9, 3; 1]]_5$	$d = 3$	[30]
	$*[[12, 15-2d, d; 1]]_5$	$d = 4$				
	$[[12, 16-2d, d; 2]]_5$	$5 \le d \le 6$				
	$[[12, 25-2d, d; 11]]_5$	$d = 12$		$[[12, 1, 12; 11]]_5$	$d = 12$	
7	$[[24, 26-2d, d; 0]]_7$	$2 \le d \le 3$	Th.3(2)			
	$[[24, 27-2d, d; 1]]_7$	$d = 4$		$[[24, 19, 4; 1]]_7$	$d = 4$	[30]
	$*[[24, 27-2d, d; 1]]_7$	$5 \le d \le 6$				
	$[[24, 28-2d, d; 2]]_7$	$7 \le d \le 9$				
	$*[[24, 31-2d, d; 5]]_7$	$11 \le d \le 12$				
	$\diamond[[24, 34-2d, d; 8]]_7$	$14 \le d \le 15$				
	$[[24, 49-2d, d; 23]]_7$	$d = 24$		$[[24, 1, 24; 23]]_7$	$d = 24$	
9	$[[40, 42-2d, d; 0]]_9$	$2 \le d \le 4$	Th.3(2)	$[[40, 42-2d, d]]_9$	$2 \le d \le 4$	[19]
	$[[40, 43-2d, d; 1]]_9$	$d = 5$		$[[40, 33, 5; 1]]_9$	$d = 5$	[30]
	$*[[40, 43-2d, d; 1]]_9$	$6 \le d \le 8$				
	$[[40, 44-2d, d; 2]]_9$	$9 \le d \le 12$				
	$*[[40, 47-2d, d; 5]]_9$	$14 \le d \le 16$				
	$*[[40, 50-2d, d; 8]]_9$	$18 \le d \le 20$				
	$\diamond[[40, 55-2d, d; 13]]_9$	$23 \le d \le 24$				
	$\diamond[[40, 60-2d, d; 18]]_9$	$27 \le d \le 28$				
	$[[40, 81-2d, d; 39]]_9$	$d = 40$		$[[40, 1, 40; 39]]_9$	$d = 40$	
(b)						
5	$[[12, 14-2d, d; 0]]_5$	$2 \le d \le 5$	Th.5	$[[12, 14-2d, d]]_5$	$2 \le d \le 5$	[13,15–18,26]
	$[[12, 16-2d, d; 2]]_5$	$6 \le d \le 7$		$[[12, 16-2d, d; 2]]_5$	$5 \le d \le 7$	[23]
				$[[12, 16-2d, d; 2]]_5$	$6 \le d \le 7$	[26]
	$[[12, 18-2d, d; 4]]_5$	$8 \le d \le 9$		$[[12, 18-2d, d; 4]]_5$	$8 \le d \le 9$	
	$\diamond[[12, 26-2d, d; 12]]_5$	$d = 13$				
7	$[[24, 26-2d, d; 0]]_7$	$2 \le d \le 7$	Th.5	$[[24, 26-2d, d]]_7$	$2 \le d \le 7$	[13,15–18,26]
	$[[24, 28-2d, d; 2]]_7$	$8 \le d \le 10$		$[[24, 28-2d, d; 2]]_7$	$6 \le d \le 10$	[23]
				$[[24, 28-2d, d; 2]]_7$	$8 \le d \le 10$	[26]
	$[[24, 30-2d, d; 4]]_7$	$11 \le d \le 13$		$[[24, 30-2d, d; 4]]_7$	$11 \le d \le 13$	
	$\diamond[[24, 34-2d, d; 8]]_7$	$15 \le d \le 16$				
	$\diamond[[24, 38-2d, d; 12]]_7$	$18 \le d \le 19$				
	$\diamond[[24, 50-2d, d; 24]]_7$	$d = 25$				

Table 2 continued

q	Paras.	d	From	Paras.	d	Refs.
9	$[[40, 42-2d, d; 0]]_9$	$2 \le d \le 9$	Th.5	$[[40, 42-2d, d]]_9$	$2 \le d \le 9$	[13,15–18,26]
	$[[40, 44-2d, d; 2]]_9$	$10 \le d \le 13$		$[[40, 44-2d, d; 2]]_9$	$7 \le d \le 13$	[23]
				$[[40, 44-2d, d; 2]]_9$	$10 \le d \le 13$	[26]
	$[[40, 46-2d, d; 4]]_9$	$14 \le d \le 17$		$[[40, 46-2d, d; 4]]_9$	$14 \le d \le 17$	
	$*[[40, 50-2d, d; 8]]_9$	$19 \le d \le 21$				
	$\diamond[[40, 54-2d, d; 12]]_9$	$23 \le d \le 26$				
	$\diamond[[40, 60-2d, d; 18]]_9$	$28 \le d \le 29$				
	$\diamond[[40, 66-2d, d; 24]]_9$	$32 \le d \le 33$				
	$\diamond[[40, 82-2d, d; 40]]_9$	$d = 41$				

Table 3 New EAQEC codes with length $n = \frac{q-1}{3}(q+1)$

q	Paras.	d	From	Paras.	d	Refs.
7	$*[[16, 18-2d, d; 0]]_7$	$d = 2$	Th.3(1)			
	$[[16, 19-2d, d; 1]]_7$	$d = 3$		$[[16, 13, 3; 1]]_7$	$d = 3$	[30]
	$*[[16, 19-2d, d; 1]]_7$	$d = 4$				
	$*[[16, 20-2d, d; 2]]_7$	$5 \le d \le 6$				
	$*[[16, 21-2d, d; 3]]_7$	$7 \le d \le 8$				
	$[[16, 33-2d, d; 15]]_7$	$d = 16$		$[[16, 1, 16; 15]]_7$	$d = 16$	
13	$[[56, 58-2d, d; 0]]_{13}$	$2 \le d \le 4$	Th.3(2)	$[[56, 58-2d, d]]_{13}$	$2 \le d \le 4$	[19]
	$[[56, 59-2d, d; 1]]_{13}$	$d = 5$		$[[56, 49, 5; 1]]_{13}$	$d = 5$	[30]
	$*[[56, 59-2d, d; 1]]_{13}$	$6 \le d \le 8$				
	$*[[56, 60-2d, d; 2]]_{13}$	$9 \le d \le 12$				
	$*[[56, 61-2d, d; 3]]_{13}$	$13 \le d \le 16$				
	$*[[56, 64-2d, d; 6]]_{13}$	$18 \le d \le 20$				
	$*[[56, 67-2d, d; 9]]_{13}$	$22 \le d \le 24$				
	$*[[56, 70-2d, d; 12]]_{13}$	$26 \le d \le 28$				
	$\diamond[[56, 75-2d, d; 17]]_{13}$	$31 \le d \le 32$				
	$\diamond[[56, 80-2d, d; 22]]_{13}$	$35 \le d \le 36$				
	$\diamond[[56, 85-2d, d; 27]]_{13}$	$39 \le d \le 40$				
	$[[56, 113-2d, d; 55]]_{13}$	$d = 56$		$[[56, 1, 56; 55]]_{13}$	$d = 56$	

Lemma 6 *Let n, q, a, a' be given as above. Denote that $f \in [0, a'-1]$ if $e \in [0, \frac{a}{2}]$ and $f \in [\lceil\frac{e-\frac{a}{2}}{a}\rceil, a'-1]$ if $e \in [\frac{a+2}{2}, q-\frac{a+2}{2}]$. Set $T_2 = \bigcup C_{1+2(ea'+f)}$, there holds $T_2 \bigcap -qT_2 = \emptyset$.*

Proof According to the value of e, our discussions are divided into the following two cases.

Case 1: If $e \in [0, \frac{a}{2}]$ and $f \in [0, a'-1]$, it is easy to check that $e - fa - \frac{a}{2} - 1 < 0$. Then, $-qT_2 = \bigcup C_{1+2((q+e-fa-\frac{a}{2})a'+a'-1-f)}$. Note that $\underline{q+e-fa-\frac{a}{2}} \cap \underline{e} \neq \emptyset$

Table 4 New EAQEC codes with length $n = \frac{q-1}{4}(q+1)$

q	Paras.	d	From	Paras.	d	Refs.
(a)						
9	$[[20, 22-2d, d; 0]]_9$	$d = 2$	Th.3(1)			
	$[[20, 23-2d, d; 1]]_9$	$d = 3$		$[[20, 17, 3; 1]]_9$	$d = 3$	[30]
	$*[[20, 23-2d, d; 1]]_9$	$d = 4$				
	$*[[20, 24-2d, d; 2]]_9$	$5 \le d \le 6$				
	$*[[20, 25-2d, d; 3]]_9$	$7 \le d \le 8$				
	$*[[20, 26-2d, d; 4]]_9$	$d = 9$				
	$[[20, 26-2d, d; 4]]_9$	$d = 10$				
	$[[20, 41-2d, d; 19]]_9$	$d = 20$		$[[20, 1, 20; 19]]_9$	$d = 20$	
13	$[[42, 44-2d, d; 0]]_{13}$	$2 \le d \le 3$	Th.3(2)			
	$[[42, 45-2d, d; 1]]_{13}$	$d = 4$		$[[42, 37, 4; 1]]_{13}$	$d = 4$	[30]
	$*[[42, 45-2d, d; 1]]_{13}$	$5 \le d \le 6$				
	$*[[42, 46-2d, d; 2]]_{13}$	$7 \le d \le 9$				
	$*[[42, 47-2d, d; 3]]_{13}$	$10 \le d \le 12$				
	$*[[42, 48-2d, d; 4]]_{13}$	$d = 13$				
	$[[42, 48-2d, d; 4]]_{13}$	$14 \le d \le 15$				
	$*[[42, 51-2d, d; 7]]_{13}$	$17 \le d \le 18$				
	$*[[42, 54-2d, d; 10]]_{13}$	$20 \le d \le 21$				
	$\diamond[[42, 57-2d, d; 13]]_{13}$	$23 \le d \le 24$				
	$\diamond[[42, 60-2d, d; 16]]_{13}$	$26 \le d \le 27$				
	$[[42, 85-2d, d; 41]]_{13}$	$d = 42$		$[[42, 1, 42; 41]]_{13}$	$d = 42$	
(b)						
9	$[[20, 22-2d, d; 0]]_9$	$2 \le d \le 7$	Th.5	$[[20, 22-2d, d]]_9$	$2 \le d \le 7$	[15–17,26]
	$[[20, 24-2d, d; 2]]_9$	$8 \le d \le 9$		$[[20, 24-2d, d; 2]]_9$	$8 \le d \le 9$	[26]
	$[[20, 26-2d, d; 4]]_9$	$10 \le d \le 11$		$[[20, 26-2d, d; 4]]_9$	$10 \le d \le 11$	
	$\diamond[[20, 28-2d, d; 6]]_9$	$12 \le d \le 13$				
	$\diamond[[20, 30-2d, d; 8]]_9$	$14 \le d \le 15$				
	$\diamond[[20, 42-2d, d; 20]]_9$	$d = 21$				
13	$[[42, 44-2d, d; 0]]_{13}$	$2 \le d \le 10$	Th.5	$[[42, 44-2d, d; 0]]_{13}$	$2 \le d \le 10$	[13,16,26]
	$[[42, 46-2d, d; 2]]_{13}$	$11 \le d \le 13$		$[[42, 46-2d, d; 2]]_{13}$	$11 \le d \le 13$	
	$[[42, 48-2d, d; 4]]_{13}$	$14 \le d \le 15$		$[[42, 48-2d, d; 4]]_{13}$	$14 \le d \le 15$	
	$*[[42, 50-2d, d; 6]]_{13}$	$16 \le d \le 19$				
	$*[[42, 52-2d, d; 8]]_{13}$	$20 \le d \le 22$				
	$\diamond[[42, 56-2d, d; 12]]_{13}$	$24 \le d \le 25$				
	$\diamond[[42, 60-2d, d; 16]]_{13}$	$27 \le d \le 28$				
	$\diamond[[42, 64-2d, d; 20]]_{13}$	$30 \le d \le 31$				
	$\diamond[[42, 68-2d, d; 24]]_{13}$	$33 \le d \le 34$				
	$\diamond[[42, 86-2d, d; 42]]_{13}$	$d = 43$				

Table 5 New EAQEC codes with length $n = \frac{q-1}{5}(q+1)$

q	Paras.	d	From	Paras.	d	Refs.
11	$*[[24, 26-2d, d; 0]]_{11}$	$d=2$	Th.3(1)			
	$[[24, 27-2d, d; 1]]_{11}$	$d=3$		$[[24, 21, 3; 1]]_{11}$	$d=3$	[30]
	$*[[24, 27-2d, d; 1]]_{11}$	$d=4$				
	$*[[24, 28-2d, d; 2]]_{11}$	$5 \leq d \leq 6$				
	$*[[24, 29-2d, d; 3]]_{11}$	$7 \leq d \leq 8$				
	$*[[24, 30-2d, d; 4]]_{11}$	$9 \leq d \leq 10$				
	$*[[24, 31-2d, d; 5]]_{11}$	$11 \leq d \leq 12$				
	$[[24, 49-2d, d; 23]]_{11}$	$d=24$		$[[24, 1, 24; 23]]_{11}$	$d=24$	
16	$*[[51, 53-2d, d; 0]]_{16}$	$2 \leq d \leq 3$	Th.3(2)			
	$[[51, 54-2d, d; 1]]_{16}$	$d=4$		$[[51, 46, 4; 1]]_{16}$	$d=4$	[30]
	$*[[51, 54-2d, d; 1]]_{16}$	$5 \leq d \leq 6$				
	$*[[51, 55-2d, d; 2]]_{16}$	$7 \leq d \leq 9$				
	$*[[51, 56-2d, d; 3]]_{16}$	$10 \leq d \leq 12$				
	$*[[51, 57-2d, d; 4]]_{16}$	$13 \leq d \leq 15$				
	$*[[51, 58-2d, d; 5]]_{16}$	$16 \leq d \leq 18$				
	$*[[51, 61-2d, d; 8]]_{16}$	$20 \leq d \leq 21$				
	$*[[51, 64-2d, d; 11]]_{16}$	$23 \leq d \leq 24$				
	$\diamond[[51, 67-2d, d; 14]]_{16}$	$26 \leq d \leq 27$				
	$\diamond[[51, 70-2d, d; 17]]_{16}$	$29 \leq d \leq 30$				
	$\diamond[[51, 73-2d, d; 20]]_{16}$	$32 \leq d \leq 33$				
	$[[51, 103-2d, d; 50]]_{16}$	$d=51$		$[[51, 1, 51; 50]]_{16}$	$d=51$	

and $[0, a'-1] = \underline{a'-1-f} \cap \underline{f} \neq \emptyset$. Suppose that $T_2 \bigcap -qT_2 \neq \emptyset$, there must hold that $a'-1-f \geq \lceil \frac{q+e-fa-\frac{a}{2}-\frac{a}{2}}{a} \rceil > a'-1-f$, a contradiction.

Case 2: If $e \in [\frac{a+2}{2}, q-\frac{a+2}{2}]$ and $f \in [\lceil \frac{e-\frac{a}{2}}{a} \rceil, a'-1]$, then denote that $e' = e-\frac{a}{2} \in [1, a(a'-1)]$ and $f' \in [\lceil \frac{e'}{a} \rceil, a'-1]$. Similar to Case 2 of Lemma 3, one can seek a contradiction to $T_2 \bigcap -qT_2 \neq \emptyset$ readily.

The proof is complete. □

The following theorem shows value of $|T_{ss}|$, which is useful to confirm the number of entanglement bits.

Theorem 4 *Let n, q, a, a' be given as above. Keep the notations defined in* Lemma 6. *If $\mathcal{C}$ is a negacyclic code with defining set $T = C_1 \bigcup C_3 \bigcup \cdots \bigcup C_{1+2(\beta a'+a'-1)}$, where $\beta \in [0, q]$, then*

$$|T_{ss}| = \begin{cases} 0 & \text{for } \beta \in \left[0, \frac{a}{2}\right]; \\ \sum_{k=\frac{a+2}{2}}^{\beta} 2\left\lceil \frac{k-\frac{a}{2}}{a} \right\rceil & \text{for } \beta \in \left[\frac{a+2}{2}, q\right]. \end{cases}$$

Table 6 New EAQEC codes with length $n = \frac{q-1}{6}(q+1)$

q	Paras.	d	From	Paras.	d	Refs.
(a)						
13	$[[28, 30 - 2d, d; 0]]_{13}$	$d = 2$	Th.3(1)			
	$[[28, 31 - 2d, d; 1]]_{13}$	$d = 3$		$[[28, 25, 3; 1]]_{13}$	$d = 3$	[30]
	$*[[28, 31 - 2d, d; 1]]_{13}$	$d = 4$				
	$*[[28, 32 - 2d, d; 2]]_{13}$	$5 \leq d \leq 6$				
	$*[[28, 33 - 2d, d; 3]]_{13}$	$7 \leq d \leq 8$				
	$*[[28, 34 - 2d, d; 4]]_{13}$	$9 \leq d \leq 10$				
	$*[[28, 35 - 2d, d; 5]]_{13}$	$11 \leq d \leq 12$				
	$*[[28, 36 - 2d, d; 6]]_{13}$	$d = 13$				
	$[[28, 36 - 2d, d; 6]]_{13}$	$d = 14$				
	$[[28, 57 - 2d, d; 27]]_{13}$	$d = 28$		$[[28, 1, 28; 27]]_{13}$	$d = 28$	
19	$[[60, 62 - 2d, d; 0]]_{19}$	$2 \leq d \leq 3$	Th.3(2)			
	$[[60, 63 - 2d, d; 1]]_{19}$	$d = 4$		$[[60, 55, 4; 1]]_{19}$	$d = 4$	[30]
	$*[[60, 63 - 2d, d; 1]]_{19}$	$5 \leq d \leq 6$				
	$*[[60, 64 - 2d, d; 2]]_{19}$	$7 \leq d \leq 9$				
	$*[[60, 65 - 2d, d; 3]]_{19}$	$10 \leq d \leq 12$				
	$*[[60, 66 - 2d, d; 4]]_{19}$	$13 \leq d \leq 15$				
	$*[[60, 67 - 2d, d; 5]]_{19}$	$16 \leq d \leq 18$				
	$*[[60, 68 - 2d, d; 6]]_{19}$	$d = 19$				
	$[[60, 68 - 2d, d; 6]]_{19}$	$20 \leq d \leq 21$				
	$*[[60, 71 - 2d, d; 9]]_{19}$	$23 \leq d \leq 24$				
	$*[[60, 74 - 2d, d; 12]]_{19}$	$26 \leq d \leq 27$				
	$*[[60, 77 - 2d, d; 15]]_{19}$	$29 \leq d \leq 30$				
	$\diamond[[60, 80 - 2d, d; 18]]_{19}$	$32 \leq d \leq 33$				
	$\diamond[[60, 83 - 2d, d; 21]]_{19}$	$35 \leq d \leq 36$				
	$\diamond[[60, 86 - 2d, d; 24]]_{19}$	$38 \leq d \leq 39$				
	$[[60, 121 - 2d, d; 59]]_{19}$	$d = 60$		$[[60, 1, 60; 59]]_{19}$	$d = 60$	
(b)						
13	$[[28, 30 - 2d, d; 0]]_{13}$	$2 \leq d \leq 9$	Th.5	$[[28, 30 - 2d, d; 0]]_{13}$	$2 \leq d \leq 9$	[15–17,26]
	$[[28, 32 - 2d, d; 2]]_{13}$	$10 \leq d \leq 11$		$[[28, 32 - 2d, d; 2]]_{13}$	$10 \leq d \leq 11$	[26,28]
	$[[28, 34 - 2d, d; 4]]_{13}$	$12 \leq d \leq 13$		$[[28, 34 - 2d, d; 4]]_{13}$	$12 \leq d \leq 13$	
	$[[28, 36 - 2d, d; 6]]_{13}$	$14 \leq d \leq 15$		$[[28, 36 - 2d, d; 6]]_{13}$	$14 \leq d \leq 15$	[28]
	$\diamond[[28, 38 - 2d, d; 8]]_{13}$	$16 \leq d \leq 17$				
	$\diamond[[28, 40 - 2d, d; 10]]_{13}$	$18 \leq d \leq 19$				
	$\diamond[[28, 42 - 2d, d; 12]]_{13}$	$20 \leq d \leq 21$				
	$\diamond[[28, 58 - 2d, d; 28]]_{13}$	$d = 29$				
19	$[[60, 62 - 2d, d; 0]]_{19}$	$2 \leq d \leq 13$	Th.5	$[[60, 62 - 2d, d; 0]]_{19}$	$2 \leq d \leq 13$	[13,15–17,26]
	$[[60, 64 - 2d, d; 2]]_{19}$	$14 \leq d \leq 16$		$[[60, 64 - 2d, d; 2]]_{19}$	$14 \leq d \leq 16$	[26,28]
	$[[60, 66 - 2d, d; 4]]_{19}$	$17 \leq d \leq 19$		$[[60, 66 - 2d, d; 4]]_{19}$	$17 \leq d \leq 19$	
	$[[60, 68 - 2d, d; 6]]_{19}$	$20 \leq d \leq 22$		$[[60, 68 - 2d, d; 6]]_{19}$	$20 \leq d \leq 22$	[28]

Table 6 continued

q	Paras.	d	From	Paras.	d	Refs.
	$*[[60, 70-2d, d; 8]]_{19}$	$23 \le d \le 25$				
	$*[[60, 72-2d, d; 10]]_{19}$	$26 \le d \le 28$				
	$*[[60, 74-2d, d; 12]]_{19}$	$29 \le d \le 31$				
	$\diamond[[60, 78-2d, d; 16]]_{19}$	$33 \le d \le 34$				
	$\diamond[[60, 82-2d, d; 20]]_{19}$	$36 \le d \le 37$				
	$\diamond[[60, 86-2d, d; 24]]_{19}$	$39 \le d \le 40$				
	$\diamond[[60, 90-2d, d; 28]]_{19}$	$42 \le d \le 43$				
	$\diamond[[60, 94-2d, d; 32]]_{19}$	$45 \le d \le 46$				
	$\diamond[[60, 98-2d, d; 36]]_{19}$	$48 \le d \le 49$				
	$\diamond[[60, 122-2d, d; 60]]_{19}$	$d = 61$				

Proof See in "Appendix 2". □

Summarizing those observations above, we can finish this section with the following theorem, which is helpful to construct EAQEC codes of length n with large minimum distance from negacyclic codes.

Theorem 5 *Let n, q, a, a' be given as above. Keep the notations defined in* Lemma 6 *and* Theorem 4. *There exist EAQEC codes with parameters $[[n, n-2(d-1)+c, d; c]]_q$, where*

$$\begin{cases} d \in \left[2, \frac{(a+2)a'}{2}+1\right], \quad c = 0 \\ d \in \left[\beta a' + \left\lceil \frac{\beta - \frac{a}{2}}{a} \right\rceil + 1, (\beta+1)a'+1\right], \quad c = \sum\limits_{k=\frac{a+2}{2}}^{\beta} 2\left\lceil \frac{k-\frac{a}{2}}{a} \right\rceil \ \textit{for } \beta \in \left[\frac{a+2}{2}, q-\frac{a}{2}-1\right]; \\ d = n+1, \quad c = n \qquad \textit{for } \beta = q. \end{cases}$$

Particularly, for $\beta \in [0, \frac{q-1}{2}]$, these EAQEC codes are EAQMDS codes.

Proof From those consequences of Lemma 6 and Theorem 4, one can construct series of EAQEC codes based on Theorem 1 directly. When $d \le \frac{n+2}{2}$, these codes are optimal. The process of proof is similar to that of Theorem 3 and is omitted here. □

5 Code comparisons and conclusions

In this paper, by investigating q^2-cyclotomic cosets modulo rn, we construct a family of EAQEC codes with length n, where q is a prime power, $n = \frac{q-1}{a}(q+1)$, $a \mid (q-1)$ and $r = 1$ or 2. Note that each coset contains only one element. Naturally, any EAQEC code derived in this paper achieves EA-Singleton bound and is optimal if its minimum distance $d \le \frac{n+2}{2}$. Furthermore, our construction could produce many new EAQEC codes with large minimum distance that are not covered in the literature.

In order to obtain QMDS or EAQMDS codes with big minimum distance, many scholars restricted their attention to studying constacyclic codes or GRS codes of length $n \leq q^2+1$. Indeed, lots of consequences on codes with length $n \mid (q^2-1)$ have been made, see Refs. [11–19,23,26,28–30]. However, most of conclusions in those above researches required many corresponding conditions, such as an odd prime power q, $n = \lambda(q+1)$ with λ an odd divisor of $q-1$ in [13], an odd prime power $q = 2tm+1$, $n = \frac{q^2-1}{2t}$ in [16] and an odd prime power $q \equiv 1 \bmod 2a$ with $a \geq 3, n = \frac{q-1}{2a}(q+1)$ in [28] and so on. Our construction comes into existence under only one condition, i.e., $a \mid (q-1)$. Clearly, given the same length n, our conclusions generalize those results in [11–19,23,26,28–30] evidently.

To make comparisons with the known codes clearly, we enumerate examples of EAQEC codes of length $n = \frac{q-1}{a}(q+1)$ in Tables 1, 2, 3, 4, 5, 6, where $a \in [1, 6]$. For even a, EAQEC codes in part (a) of Table a are obtained from cyclic codes by Theorem 3, while EAQEC codes in part (b) of Table a are derived from negacyclic codes by Theorem 5. Symbols $*$ and $\diamondsuit$ in the tables denote that those corresponding codes are new EAQMDS codes and new EAQEC codes, respectively.

As shown in Tables 1, 2, 3, 4, 5, 6, for given length n, our construction is prior to those already known ones. Specifically, many known constructions of EAQEC codes are applicable for big and specific q, which might be empty of practicality. Nevertheless, those codes produced by their construction have shorter minimum distance than ours. In other words, the bigger q is, the larger minimum distance of our EAQEC codes could have. Moreover, quite a lot of known results can be seemed as some special cases of ours in Theorems 3 and 5.

Practically, it is difficult to construct EAQEC codes with flexible good parameters. Whereas, we present a family of EAQEC codes whose required number of entanglement bits is flexible. We believe that our method of studying EAQEC codes employed in this paper can facilitate more good results in the future.

Appendix 1: Proof of Theorem 2

Proof Let $T_1 = \bigcup C_{ea'+f}$, where $f \in [1, a'-1]$ if $e = 0$ and $f \in [\lceil \frac{e}{a} \rceil, a'-1]$ if $e \in [1, a(a'-1)]$. Then, one can get that $T_1 \bigcap -qT_1 = \emptyset$ by Lemma 4.

Denote that $T_1^c = \bigcup C_{ka'+l} \bigcup C_{wa'}$, where $l \in [1, \lceil \frac{k}{a} \rceil - 1]$ if $k \in [a+1, q-1]$, $l \in [1, \lceil \frac{k}{a} \rceil - 2]$ if $k = q$ and $w \in [1, q]$. From Lemma 3, it is easy to obtain that $-qT_1^c = \bigcup C_{(k-1-la)a'+a'-l} \bigcup C_{wa'}$ since $k-1-la \geq 0$ and $-qC_{wa'} = C_{wa'}$. Next, we verify that $T_1^c \bigcap -qT_1^c = C_{wa'}$.

Suppose that $(\bigcup C_{ka'+l}) \bigcap (\bigcup C_{(k-1-la)a'+a'-l}) \neq \emptyset$, there are two cases according to k.

Case 1: If $k \in [a+1, q-1]$, then there holds that $l \leq \lceil \frac{k}{a} \rceil - 1 \Rightarrow a'-l \leq \lceil \frac{k-1-la}{a} \rceil - 1 \leq \lceil \frac{q-2-la}{a} \rceil - 1 < a'-l-1$, a contradiction.

Case 2: If $k = q$, then from $l \leq \lceil \frac{k}{a} \rceil - 2$, one can derive that $a'-l \leq \lceil \frac{k-1-la}{a} \rceil - 2 \leq \lceil \frac{q-1-la}{a} \rceil - 2 < a'-l-2$, which yields also a contradiction.

From Case 1, Case 2 and $(\bigcup C_{ka'+l}) \bigcap C_{wa'} = \emptyset$, one can conclude that $T_1^c \bigcap -qT_1^c = C_{wa'}$.

Note that $T = C_1 \bigcup C_2 \bigcup \cdots \bigcup C_{\beta a'+a'-1}$ for some β. Then, it is not difficult to check that $T = T_1 \bigcup T_1^c$. Hence, $T_{ss} = T \bigcap -qT = (T_1 \bigcup T_1^c) \bigcap -q(T_1 \bigcup T_1^c) = (T_1^c \bigcap -qT_1) \bigcup (T_1 \bigcap -qT_1^c) \bigcup C_{wa'}$. Obviously, $T_1 \bigcap -qT_1^c = -q(T_1^c \bigcap -qT_1)$, which indicates that $|T_{ss}| = 2|T_1 \bigcap -qT_1^c| + |C_{wa'}|$.

As discussed above, $-qT_1^c = \bigcup C_{(k-1-la)a'+a'-l} \bigcup C_{wa'}$. Clearly, from $0 \notin \underline{f}$, it follows that $T_1 \bigcap (\bigcup C_{wa'}) = \emptyset$. According to different e, f, k, l, we prove that $(\bigcup C_{(k-1-la)a'+a'-l}) \subseteq T_1$ below.

Case 1: If $k-1-la = 0 = e$, then we have that $\underline{a'-l} = \underline{a' - \frac{k-1}{a}} = [1, a'-1] \subseteq \underline{f}$, which implies that $(\bigcup C_{(k-1-la)a'+a'-l}) \subseteq T_1$

Case 2: If $k-1-la \neq 0$, then $\underline{k-1-la} \subseteq \underline{e} \backslash \{0\}$ clearly. Note that $a'-l \geq \lceil \frac{k-1-la}{a} \rceil$ and $a'-l \leq a'-1$. Thus, one can gain that $\underline{a'-l} \subseteq \underline{f}$ for any $k-1-la$ and $a-l'$, implying that $(\bigcup C_{(k-1-la)a'+a'-l}) \subseteq T_1$.

Overall, it is easy to see that $T_1 \bigcap -qT_1^c = \bigcup C_{(k-1-la)a'+a'-l}$. Therefore, $|T_{ss}| = 2|T_1 \bigcap -qT_1^c| + |C_{wa'}| = 2|\bigcup C_{(k-1-la)a'+a'-l}| + |C_{wa'}| = 2|\bigcup C_{ka'+l}| + |C_{wa'}|$.

For $\beta = 0$ and $T = C_1 \bigcup C_2 \bigcup \cdots \bigcup C_{a'-1}$, then $T_1^c = \emptyset$.

For $\beta = 1$ and $T = C_1 \bigcup C_2 \bigcup \cdots \bigcup C_{2a'-1}$, then $T_1^c = C_{a'}$. Thus, $|T_{ss}| = 1$.

For $\beta = 2$ and $T = C_1 \bigcup C_2 \bigcup \cdots \bigcup C_{3a'-1}$, then $T_1^c = \bigcup C_{wa'}$, where $w \in [1, 2]$. Naturally, $|T_{ss}| = 2$.

…

For $\beta = a+1$ and $T = C_1 \bigcup C_2 \bigcup \cdots \bigcup C_{(a+1)a'+a'-1}$, then $T_1^c = \bigcup C_{ka'+l} \bigcup C_{wa'}$, where $k = a+1, l \in [1, \lceil \frac{k}{a} \rceil - 1], w \in [1, a+1]$. Hence, $|T_{ss}| = a + 1 + 2(\lceil \frac{k}{a} \rceil - 1)$.

…

For $\beta = 2a+1$ and $T = C_1 \bigcup C_2 \bigcup \cdots \bigcup C_{(2a+1)a'+a'-1}$, then $T_1^c = \bigcup C_{ka'+l} \bigcup C_{wa'}$, where $k \in [a+1, 2a+1], l \in [1, \lceil \frac{k}{a} \rceil - 1], w \in [1, 2a+1]$. It is easy to calculate that $|T_{ss}| = 2a + 1 + \sum\limits_{k=a+1}^{2a+1} 2(\lceil \frac{k}{a} \rceil - 1)$.

According to the analysis above, one can derive universal consequences as below.

For $\beta \in [0, a]$ and $T = C_1 \bigcup C_2 \bigcup \cdots \bigcup C_{\beta a'-1}$, then $T_1^c = \bigcup C_{wa'}$, where $w \in [1, \beta]$. Hence, $|T_{ss}| = \beta$.

For $\beta \in [a+1, q-1]$ and $T = C_1 \bigcup C_2 \bigcup \cdots \bigcup C_{\beta a'-1}$, then $T_1^c = \bigcup C_{ka'+l} \bigcup C_{wa'}$, where $k \in [a+1, \beta], l \in [1, \lceil \frac{k}{a} \rceil - 1], w \in [1, \beta]$. Clearly, $|T_{ss}| = \beta + \sum\limits_{k=a+1}^{\beta} 2(\lceil \frac{k}{a} \rceil - 1)$.

For $\beta = q$ and $T = C_1 \bigcup C_2 \bigcup \cdots \bigcup C_{qa'+a'-1}$, then $T_1^c = \bigcup C_{ka'+l} \bigcup C_{wa'}$, where $l \in [1, \lceil \frac{k}{a} \rceil - 1]$ if $k \in [a+1, q-1], l \in [1, \lceil \frac{k}{a} \rceil - 2]$ if $k = q$ and $w \in [1, q]$. One can obtain that $|T_{ss}| = q + \sum\limits_{k=a+1}^{q-1} 2(\lceil \frac{k}{a} \rceil - 1) + a' - 1 = n - 1$. □

Appendix 2: Proof of Theorem 4

Proof By Lemma 6, one knows that $T_2 \bigcap -qT_2 = \emptyset$, where T_2 is defined as $T_2 = \bigcup C_{1+2(ea'+f)}$, $f \in [0, a'-1]$ if $e \in [0, \frac{a}{2}]$ and $f \in [\lceil \frac{e-\frac{a}{2}}{a} \rceil, a'-1]$ if $e \in [\frac{a+2}{2}, q - \frac{a+2}{2}]$.

Denote that $T_2^c = \bigcup C_{1+2(ka'+l)}$, where $k \in [\frac{a+2}{2}, q]$, $l \in [0, \lceil \frac{k-\frac{a}{2}}{a} \rceil - 1]$. In the sequel, we clarify that $T_2^c \bigcap -qT_2^c = \emptyset$.

From $l \leq (\lceil \frac{k-\frac{a}{2}}{a} \rceil - 1) \Rightarrow la \leq (\lceil \frac{k-\frac{a}{2}}{a} \rceil - 1)a \leq k - \frac{a}{2} - 1$, it follows that $k - la - \frac{a}{2} - 1 \geq 0$ and $-qT_2^c = \bigcup C_{1+2((k-la-\frac{a}{2}-1)a'+a'-1-l)}$ by Lemma 5 (2). Suppose that $T_2^c \bigcap -qT_2^c \neq \emptyset$, then one can obtain that $l \leq \lceil \frac{k-\frac{a}{2}}{a} \rceil - 1 \Rightarrow a' - 1 - l \leq \lceil \frac{k-la-\frac{a}{2}-1-\frac{a}{2}}{a} \rceil - 1 \leq \lceil \frac{q-1-la-a}{a} \rceil - 1 = a' - l - 2$, a contradiction. Thus, one can conclude that $T_2^c \bigcap -qT_2^c = \emptyset$.

Clearly, there holds $T = T_2 \bigcup T_2^c$. By definition, one knows that $T_{ss} = T \bigcap -qT = (T_2^c \bigcap -qT_2) \bigcup (T_2 \bigcap -qT_2^c)$ and $|T_{ss}| = 2|T_2 \bigcap -qT_2^c|$. Actually, $-qT_2^c \subseteq T_2$ holds and we give its proof as below. As to different range of e, f, we need to split our discussions of $-qT_2^c$ with different range of k, l as well.

Case 1: For $e \in [0, \frac{a}{2}]$, $f \in [0, a'-1]$. Set $k = \frac{a+2}{2} + \mu a + \nu$, $l = \lceil \frac{k-\frac{a}{2}}{a} \rceil - 1 = \mu$, where $\mu \in [0, a'-1]$ and $\nu \in [0, \frac{a}{2}]$. Obviously, one can deduce that $\underline{k - la - \frac{a}{2} - 1} = \underline{\nu} = [0, \frac{a}{2}] \subseteq \underline{e}$, $\underline{a' - 1 - l} = [0, a'-1] \subseteq \underline{f}$. Hence, it is not difficult to check that $-qT_2^c \subseteq T_2$ for any combination of k and l given as above.

Case 2: For $e \in [\frac{a+2}{2}, q - \frac{a+2}{2}]$, $f \in [\lceil \frac{e-\frac{a}{2}}{a} \rceil, a'-1]$. Set $k = \frac{a+2}{2} + \mu a + \nu$, $l \in [0, \lceil \frac{k-\frac{a}{2}}{a} \rceil - 2] = [0, \mu - 1]$, where $\nu \in [0, \frac{a}{2}]$ if $\mu \in [1, a'-1]$. Then, we have that $\underline{k - la - \frac{a}{2} - 1} = \underline{\mu a + \nu - la} \subseteq \underline{e}$. From $a' - 1 - l \geq \lceil \frac{k-la-\frac{a}{2}-1-\frac{a}{2}}{a} \rceil = \lceil \frac{\mu a+\nu-la-\frac{a}{2}}{a} \rceil$ and $a' - 1 - l \leq a' - 1$, it follows that $\underline{a' - 1 - l} = [a' - \mu, a' - 1] \subseteq \underline{f}$ for any $k - la - \frac{a}{2} - 1, a' - 1 - l$. So we can derive that $-qT_2^c \subseteq T_2$ with given e, f, k, l above.

Case 3: For $e \in [\frac{a+2}{2}, q - \frac{a+2}{2}]$, $f \in [\lceil \frac{e-\frac{a}{2}}{a} \rceil, a'-1]$. Set $k = \frac{a+2}{2} + \mu a + \nu$, $l \in [0, \lceil \frac{k-\frac{a}{2}}{a} \rceil - 1] = [0, \mu]$, where $\nu \in [\frac{a+2}{2}, a-1]$ if $\mu \in [0, a'-2]$. Then, one can get that $\underline{k - la - \frac{a}{2} - 1} = \underline{\mu a + \nu - la} \subseteq \underline{e}$ easily. Similar to the Case 2, there also holds that $-qT_2^c \subseteq T_2$ for any $a' - 1 - l, k - la - \frac{a}{2} - 1$ since $\underline{a' - 1 - l} \subseteq \underline{f}$.

Utilizing the results of Cases 1–3, we can calculate the precise value of $|T_{ss}| = 2|T_2 \bigcap -qT_2^c| = 2|-qT_2^c| = 2|T_2^c|$ simply.

For $\beta \in [0, \frac{a}{2}]$ and $T = C_1 \bigcup C_3 \bigcup \cdots \bigcup C_{1+2(\beta a'+a'-1)}$, then $T_2^c = \emptyset$.

For $\beta = \frac{a+2}{2}$ and $T = C_1 \bigcup C_3 \bigcup \cdots \bigcup C_{1+2(\beta a'+a'-1)}$, then $T_2^c = C_{1+2(\frac{a+2}{2}a')}$. Thus, $|T_{ss}| = 2$.

For $\beta = \frac{a+4}{2}$ and $T = C_1 \bigcup C_3 \bigcup \cdots \bigcup C_{1+2(\beta a'+a'-1)}$, then $T_2^c = \bigcup C_{1+2(ka')}$, where $k \in [\frac{a+2}{2}, \frac{a+4}{2}]$. Obviously, $|T_{ss}| = 2 + 2 = 4$.

$\ldots$

For $\beta \in [\frac{a+2}{2}, q]$ and $T = C_1 \bigcup C_3 \bigcup \cdots \bigcup C_{1+2(\beta a'+a'-1)}$, then $T_2^c = \bigcup C_{1+2(ka'+l)}$, where $k \in [\frac{a+2}{2}, q], l \in [0, \lceil\frac{k-\frac{a}{2}}{a}\rceil - 1]$. Then, it is easy to see that $|T_{ss}| = 2|T_2^c| = \sum\limits_{k=\frac{a+2}{2}}^{\beta} 2\lceil\frac{k-\frac{a}{2}}{a}\rceil$. □

References

1. Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A **52**, 2493–2496 (1995)
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**, 1369–1387 (1998)
3. Grassl, M., Beth, T.: Quantum BCH codes. In: Proceedings of X. International Symposium on Theoretical Electrical Engineering Magdeburg, 207–212 (1999)
4. Ashikhim, A., Knill, E.: Non-binary quantum stabilizer codes. IEEE Trans. Inf. Theory **47**, 3065–3072 (2001)
5. Ketkar, A., Klappenecker, A., Kumar, S.: Nonbinary stablizer codes over finite fields. IEEE Trans. Inf. Theory **52**, 4892–4914 (2006)
6. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: On quantum and classical BCH codes. IEEE Trans. Inf. Theory **53**, 1183–1188 (2007)
7. 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)
8. Liu, Y., Li, R., Lv, L., Ma, Y.: A class of constacyclic BCH codes and new quantum codes. Quantum Inf. Process. **16**(66), 1–16 (2017)
9. Wang, J., Li, R., Liu, Y., Guo, G.: Two families of BCH codes and new quantum codes. Int. J. Theor. Phys. **58**, 2293–2302 (2019)
10. Li, R., Wang, J., Liu, Y., Guo, G.: New quantum constacyclic codes. Quantum Inf. Process. **18**(127), 1–23 (2019)
11. Grassl, M., Beth, T., Rtteler, M.: Qn optimal quantum codes. Int. J. Quantum Inf. **2**(1), 55–64 (2004)
12. 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**, 4735–4740 (2010)
13. Kai, X., Zhu, S., Li, P.: Constacyclic codes and some new quantum MDS codes. IEEE Trans. Inf. Theory **60**, 2080–2086 (2014)
14. Jin, L., Xing, C.: A construction of new quantum MDS codes. IEEE Trans. Inf. Theory **60**, 2921–2925 (2014)
15. Chen, B., Ling, S., Zhang, G.: Application of constacyclic codes to quantum MDS codes. IEEE Trans. Inf. Theory **61**, 1474–1484 (2015)
16. Zhang, T., Ge, G.: Some new classes of quantum MDS codes from constacyclic codes. IEEE Trans. Inf. Theory **61**, 5224–5228 (2015)
17. Zhang, T., Ge, G.: Quantum MDS codes with large minimum distance. Des. Codes Cryptogr. **83**(3), 503–517 (2016)
18. Shi, X., Yue, Q., Chang, Y.: Some quantum MDS codes with large minimum distance from generalized Reed–Solomon codes. Cryptogr. Commun. **10**(6), 1118–1165 (2018). 2
19. Shi, X., Yue, Q., Zhu, X.: Construction of some new quantum MDS codes. Finite Fields Appl. **46**, 347–362 (2017)
20. Burn, T., Devetak, I., Hsieh, M.: Correcting quantum errors with entanglement. Science **314**, 436–439 (2006)
21. Wilde, M., Burn, T.: Optimal entanglement formulas for entanglement-assisted quantum coding. Phys. Rev. A **77**, 064302 (2008)
22. Grassl, M.: Entanglement-assisted quantum communication beating the quantum singleton bound. In: AQIS, Taiwan(2016)
23. 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**, 423–434 (2016)

24. Chen, J., Huang, Y., Feng, C., Chen, R.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. Quantum Inf. Process. **16**(303), 1–22 (2017)
25. Lu, L., Ma, W., Li, R., Ma, Y., Liu, Y., Cao, H.: Entanglement-assisted quantum MDS codes from constacyclic codes with large minimum distance. Finite Fields Appl. **53**, 309–325 (2018)
26. Lu, L., Li, R., Guo, L., Ma, Y., Liu, Y.: Entanglement-assisted quantum MDS codes from negacyclic codes. Quantum Inf. Process. **17**(69), 1–23 (2018)
27. Qian, J., Zhang, L.: Constructions of new entanglement-assisted quantum MDS codes and almost MDS codes. Quantum Inf. Process. **18**(71), 1–12 (2019)
28. Li, R., Guo, G., Song, H., Liu, Y.: New constructions of entanglement-assisted quantum MDS codes from negacyclic codes. Int. J. Quantum Inf. **17**(1), 1950022 (2019)
29. Liu, Y., Li, R., Lv, L., Ma, Y.: Application of constacyclic codes to entanglement-assisted quantum maximum diatance separable codes. Quantum Inf. Process. **17**(210), 1–19 (2018)
30. Fang, W., Fu, F., Li, L., Zhu, S.: Euclidean and Hermitian hulls of MDS codes and their applications to EAQECCs. arXiv:1812.09019v3
31. Macwilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, Amsterdam (1977)
32. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
33. Lü, L., Li, R.: Entanglement-assisted quantum codes constructed from primitive quaternary BCH codes. Int. J. Quantum Inf. **12**(03), 1450015 (2014)
34. Aydin, N., Siap, I., Ray-Chaudhuri, D.K.: The structure of 1-generator quasi-twisted codes and new linear codes. Des. Codes Cryptogr. **24**, 313–326 (2001)
35. Krishna, A., Sarwate, D.V.: Pseudo-cyclic maximum-distance separable codes. IEEE Trans. Inf. Theory **36**, 880–884 (1990)

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