Quantum Information Processing (2019) 18:292
https://doi.org/10.1007/s11128-019-2409-0

Entanglement-assisted quantum error correction codes with length $n = q^2 + 1$

Junli Wang[1] · Ruihu Li[1] · Jingjie Lv[1] · Guanmin Guo[1] · Yang Liu[1]

Received: 18 April 2019 / Accepted: 7 August 2019 / Published online: 13 August 2019

Abstract
In this paper, by investigating q^2-cyclotomic coset modulo rn in detail, where q is a prime power, $n = q^2+1$ and $r \mid (q+1)$, series of entanglement-assisted quantum error correction (EAQEC) codes with flexible parameters of length n are constructed from constacyclic codes (including cyclic codes). Most of our EAQEC codes are new and have large minimum distance. As to EAQEC codes constructed from cyclic codes, their all possible parameters are determined completely. When minimum distance $d \leq \frac{n+2}{2}$, all of our constructed EAQEC codes are entanglement-assisted quantum MDS (EAQMDS) codes. Those previously known EAQMDS codes with the same length in Fan et al. (Quantum Inf Comput 16:423–434, 2016), Chen et al. (Quantum Inf Process 16(303):1–22, 2017), Lu et al. (Finite Fields Their Appl 53:309–325, 2018), Mustafa and Emre (Comput Appl Math 38(75):1–13, 2019) and Qian and Zhang (Quantum Inf Process 18(71):1–12, 2019) are special cases of ours. Besides, some maximum entanglement EAQEC codes and maximum entanglement EAQMDS codes are derived as well.

Keywords Constacyclic code · Cyclotomic coset · EAQEC code · EAQMDS code

1 Introduction

Quantum error correction (QEC) codes play an important role in the field of fighting against decoherence and quantum noise. For the security of quantum information and quantum communication, many QEC codes with good parameters were obtained from dual-containing classical linear codes concerning Euclidean inner product or

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

Hermitian inner product; see Refs. [1–10]. A q-ary QEC code, denoted as $[[n, k, d]]_q$, achieves the quantum singleton bound $k \leq n - 2d + 2$. When $k = n - 2d + 2$, the QEC code is called a quantum maximum-distance separable (QMDS) code, whose parameters are optimal. In recent years, many scholars have devoted their attention to constructing QMDS codes from constacyclic codes (including cyclic codes); see Refs. [11–15]. However, it is still very hard to construct QMDS codes with large distance. The dual-containing condition for constructing QEC codes forms a limitation and induces that many classical linear codes cannot be used fully. Thus, new ideas need to be employed to improve the ability of error correction of QEC codes.

In [16], Brun et al. proposed entanglement-assisted stabilizer formalism. They proved that any classical linear code can be used to construct QEC code if pre-shared entanglement bits are available between the sender and receiver. Such q-ary QEC codes are called EAQEC codes and denoted as $[[n, k, d; c]]_q$, where c is the number of entanglement bits. Clearly, if $c = 0$, then the EAQEC code is a standard QEC code. If $c = n - k$, then the EAQEC code is called a maximal entanglement EAQEC code. They also gave EA-singleton bound for EAQEC codes as follows. An EAQEC code that saturates such bound is called an EAQMDS code, whose parameters are optimal.

Lemma 1 (EA-singleton bound [16,17]) *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* $0 \leq c \leq n - 1$.

Until now, almost all known nontrivial q-ary QMDS codes have minimum distance less than or equal to $q + 1$, whereas with the help of entanglement bits, it is possible to obtain EAQMDS codes from classical MDS codes with minimum distance lager than $q + 1$; see Refs. [18–26]. Among those existing results, there were some about EAQMDS codes with length $n = q^2 + 1$. In [18], Fan et al. proposed a family of q-ary EAQMDS codes with parameters $[[n, n - 2d + 3, d; 1]]_q$, where $2 \leq d \leq 2q$. From constacyclic codes, Chen et al. and Lu et al. constructed new EAQMDS codes with larger minimum distance and consumed 4 entanglement bits in [19,20], respectively. Let $c = 5$ and $c = 9$, Mustafa and Emre improved the parameters of EAQMDS codes with length n further in [21]. In [22,23], based on MDS linear complementary dual codes and cyclic codes, Qian et al. obtained new maximal entanglement EAQMDS codes and EAQMDS codes, respectively. In particular, all of their codes had flexible parameters.

Actually, the larger the minimum distances of EAQEC codes are, the more the entanglement bits will be employed. However, it is not an easy task to analyze the accurate parameters if the value of c is too large or flexible. Inspired by the above work, we discuss EAQEC codes obtained from constacyclic codes (including cyclic codes) with length $n = q^2 + 1$ in this paper, where q is a prime power. By investigating q^2-cyclotomic coset modulo rn, where $r \mid (q + 1)$, we can determine their properties and analyze parameters of corresponding EAQEC codes accurately. Further, many EAQMDS codes with minimum distance $d \leq \frac{n+2}{2}$ can be obtained. Almost all of those known results mentioned above are some special cases of ours. Our constructed EAQEC codes also have flexible parameters, indicating that the minimum distances of such codes are larger. As to EAQEC codes gained from cyclic codes, their parameters are calculated exactly for $2 \leq d \leq n$. Moreover, some maximal entanglement EAQEC codes and maximal entanglement EAQMDS codes are derived as well.

The paper is organized as follows. In Sect. 2, some basic knowledge on constacyclic codes, cyclotomic cosets and EAQEC codes is reviewed. In Sects. 3 and 4, EAQEC codes with length $n = q^2 + 1$ are discussed when q is an odd prime power and q is an even prime power, respectively. Finally, some comparisons of codes and conclusions are made.

2 Preliminaries

In this section, some basic concepts on constacyclic codes, cyclotomic cosets and EAQEC codes are reviewed. For more details, we may refer to Refs. [16,27–29].

Let q be a prime power and $\mathbb{F}_{q^2}$ be a finite field with q^2 elements. For any $\alpha \in \mathbb{F}_{q^2}$, the conjugation of α is $\overline{\alpha} = \alpha^q$. 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 k-dimensional subspace of $\mathbb{F}_{q^2}^n$ is said to be a linear code with length n, denoted as $\mathcal{C}$. Hermitian dual code of a linear code $\mathcal{C}$ with length n is

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

If $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$, then $\mathcal{C}$ is called a Hermitian dual-containing code and could be adopted to construct standard QEC codes.

Let $\mathcal{C}$ be a linear code over $\mathbb{F}_{q^2}$ with length n and $\gcd(q, n) = 1$. If for any codeword $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, we have $(\lambda c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$, then $\mathcal{C}$ is said to be 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. Under the correspondence of codes with polynomials, we know that a λ-constacyclic code $\mathcal{C}$ is an ideal of quotient ring $\mathcal{R}_n = \frac{\mathbb{F}_{q^2}[x]}{\langle x^n - \lambda \rangle}$ and $xc(x)$ corresponds to an λ-constacyclic shift of $c(x)$ in $\mathcal{R}_n$, where $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$. Thus, $\mathcal{C}$ can be generated by a monic polynomial divisor $g(x)$ of $x^n - \lambda$, i.e., $\mathcal{C} = \langle g(x) \rangle$. It is well known that $\mathcal{C}$ has dimension $k = n - \deg(g(x))$.

Denote that $r = \mathrm{ord}_{q^2}(\lambda)$ and $\Omega_{r,n} = \{1 + ir \mid 0 \leq i \leq n - 1\}$. By definition, one can get that a λ-constacyclic code $\mathcal{C}$ is a cyclic code if $r = 1$ and $\mathcal{C}$ is a negacyclic code if $r = 2$. Let ζ be a primitive rnth root of unity in some extension field of $\mathbb{F}_{q^2}$ such that $\zeta^n = \lambda$. Then, $T = \{j \in \Omega_{r,n} | g(\zeta^j) = 0\}$ is called defining set of $\mathcal{C}$. For any $j \in \Omega_{r,n}$, q^2-cyclotomic coset C_j modulo rn containing j is

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

where l is the smallest positive integer such that $j(q^2)^l \equiv j \bmod rn$. It is known that $\Omega_{r,n}$ can be divided into several q^2-cyclotomic coset modulo rn that are disjoint with

each other. For $b + (\delta - 2)r \in \Omega_{r,n}$, if $\mathcal{C}$ has defining set $T_\delta = C_b \cup C_{b+r} \cup \cdots \cup C_{b+(\delta-2)r}$, then it is called a constacyclic BCH code with designed distance δ.

According to the following BCH bound for λ-constacyclic codes, a constacyclic BCH code $\mathcal{C}$ with designed distance δ has minimum distance at least δ.

Lemma 2 (The BCH bound for λ-constacyclic codes, [30,31]) *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 $\{\zeta^{1+ir} | 0 \leq i \leq \delta - 2\}$ as roots, where ζ is a primitive rnth root of unity, then the minimum distance of $\mathcal{C}$ is at least δ.*

As mentioned above, over $\mathbb{F}_{q^2}$, EAQEC codes could be obtained from any linear codes $\mathcal{C}$ by consuming some entanglement bits. According to [27], one needs to know the value of $\text{rank}(HH^\dagger)$ to determine the number of entanglement bits c, where H is a parity check matrix of $\mathcal{C}$ and $H^\dagger$ is conjugate transpose of H. However, it is not easy to compute $\text{rank}(HH^\dagger)$ exactly. Then, some researchers proposed the definition for decomposition of defining set of some special linear codes $\mathcal{C}$ to calculate c in [19,25,32], such as constacyclic codes (including cyclic codes and negacyclic codes).

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

Using decomposition of a defining set T, one can calculate $c = \text{rank}(HH^\dagger) = |T_{\text{ss}}|$ as shown in [25]. Naturally, some EAQEC codes with good parameters can be constructed from these special classes of linear codes readily.

Theorem 1 [25, Theorem 1] *Let $\mathcal{C}$ be an $[n, k, d]_{q^2}$ λ-constacyclic code with defining set T. Suppose decomposition of T is $T = T_{\text{ss}} \bigcup T_{\text{sas}}$. Then there exists an $[[n, n - 2|T| + |T_{\text{ss}}|, d; |T_{\text{ss}}|]]_q$ 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 Set $n = q^2 + 1$, where q is a prime power. Given a symbol $\mathcal{S}$, $|\mathcal{S}|$ is defined as its cardinality if $\mathcal{S}$ is a set. If $\mathcal{S}$ is an integer, then $|\mathcal{S}|$ is denoted by the absolute value of $\mathcal{S}$. Denote the set $\{b, b+1, \ldots, e\}$ by $[b, e]$ for $b < e$.

3 q is an odd prime power

Throughout this section, we construct EAQEC codes from constacyclic codes (including cyclic codes) with length n. Note that q is an odd prime power and $r \mid (q+1)$. If $r = 1$, then let $s = \frac{q^2+1}{2}$; if $r \neq 1$, then denote that $rr' = q + 1$ and $s = \frac{(q^2+1)(r+1)}{2}$. Firstly, properties of corresponding q^2-cyclotomic coset modulo rn are given as follows.

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

1. *If $r = 1$, then $C_s = \{s\}$ is a skew symmetric coset and $C_{s+i} = \{s + i, s - i\}$.*

2. *If $r \neq 1$, then $C_s = \{s\}$ and $C_{s+ir} = \{s+ir, s-ir\}$. If r' is odd, then $-qC_s = C_{\frac{q^2+1}{2}}$; if r' is even, then C_s is a skew symmetric coset.*

Proof It is not difficult to obtain that any C_{s+ir} has at most two elements since $\mathrm{ord}_{rn}(q^2) = 2$.

1. If $r = 1$, from $sq^2 = \frac{q^2+1}{2}(q^2-1+1) \equiv \frac{q^2+1}{2} \bmod n$ and $-qs = (-q-1+1)\frac{q^2+1}{2} \equiv s \bmod n$, one can conclude that $C_s = \{s\}$ is a skew symmetric coset. Moreover, there holds $(s+i)q^2 = \left(\frac{q^2+1}{2}+i\right)(q^2-1+1) \equiv \frac{q^2+1}{2} - i \bmod n$. Hence, $C_{s+i} = \{s+i, s-i\}$.
2. If $r \neq 1$, it is easy to check that $C_s = \{s\}$ since $sq^2 = \frac{(q^2+1)(r+1)}{2}(q^2-1+1) \equiv s \bmod rn$.

   Note that $(s+ir)q^2 \equiv s - ir \bmod rn$. Clearly, $C_{s+ir} = \{s+ir, s-ir\}$.

   Set r' is odd. Then, $-qs = -\frac{q+1}{2}(q^2+1) - \frac{q+1}{2}(q^2+1)r + \frac{(q^2+1)(r+1)}{2} \equiv -\frac{rr'-r}{2}(q^2+1) + \frac{q^2+1}{2} \equiv \frac{q^2+1}{2} \bmod rn$. Hence, $-qC_s = C_{\frac{q^2+1}{2}}$.

   Set r' is even. From $-qs = -\frac{q+1}{2}(r+1)(q^2+1) + \frac{(q^2+1)(r+1)}{2} \equiv -\frac{rr'}{2}(q^2+1) + \frac{(q^2+1)(r+1)}{2} \equiv s \bmod rn$, it follows that C_s is a skew symmetric coset. □

Lemma 4 *Let n, q, r, r', s be given as above.*

1. *If $r = 1$, for $1 \leq i \leq \frac{q^2-1}{2}$, let $i = uq + v$, where $v \in [1, \frac{q-1}{2}]$ if $u = 0$ and $v \in [-\frac{q-1}{2}, \frac{q-1}{2}]$ if $u \in [1, \frac{q-1}{2}]$. Then, $-qC_{s+uq+v} = C_{s+vq-u}$.*
2. *If r' is odd, for $1 \leq i \leq \frac{(q-1)(r-1)r'}{2}$, let $i = uq + v$, where $v \in [1, \frac{r'-1}{2}]$ if $u = 0$ and $v \in [\frac{-(2q-1)+r'}{2}, \frac{r'-1}{2}]$ if $u \in [1, \frac{q-r'}{2}]$. Then, $-qC_{s+(uq+v)r} = C_{\frac{q^2+1}{2}+(vq-u)r}$.*
3. *If r' is even, for $1 \leq i \leq \frac{(q-1)(r-1)r'}{2}$, let $i = uq + v$, where $v \in [1, \frac{q-1+r'}{2}]$ if $u = 0$ and $v \in [\frac{-(q-1)+r'}{2}, \frac{q-1+r'}{2}]$ if $u \in [1, \frac{q-1-r'}{2}]$. Then, $-qC_{s+(uq+v)r} = C_{s+(vq-u)r}$.*

Proof 1. By Lemma 3 (1), one can get that $C_{s+i} = \{s+i, s-i\}$. Hence, $-q(s+i) = -q(s+uq+v) \equiv s - vq + u \bmod n$, i.e., $-qC_{s+uq+v} = C_{s-vq+u} = \{s-vq+u, s+vq-u\}$.

2. If r' is odd, note that $-qs \equiv \frac{q^2+1}{2} \bmod rn$ from Lemma 3 (3). Thus, (2) follows.
3. Note that $C_{s+ir} = \{s+ir, s-ir\}$. Similar to (1), the results are easy to see.

Lemma 5 *Let n, q, r, r', s be given as above.*

1. *If $r = 1$, then denote that $0 \leq e \leq \frac{q-3}{2}, e+1 \leq f \leq \frac{q-1}{2}$ and $1 \leq g \leq \frac{q-1}{2}, -\frac{q-1}{2} \leq h \leq -g$. Set*

$$T_1 = \bigcup C_{s+eq+f} \bigcup C_{s+gq+h},$$

there holds $T_1 \bigcap -qT_1 = \emptyset$.

2. *If r' is odd, then denote that $e = 0, 0 \le f \le \frac{r'-1}{2}, 1 \le g \le \frac{q-r'}{2}, -\frac{q-1}{2} + g \le h \le \frac{r'-1}{2}$ and $1 \le k \le \frac{q-r'}{2}, \frac{-(2q-1)+r'}{2} \le l \le -\frac{q-1}{2} - k$. Set*

$$T_2 = \bigcup C_{s+(eq+f)r} \bigcup C_{s+(gq+h)r} \bigcup C_{s+(kq+l)r},$$

there holds $T_2 \bigcap -qT_2 = \emptyset$.

3. *If r' is even, then denote that $0 \le e \le \frac{q-1-r'}{2}, e+1 \le f \le \frac{q-1+r'}{2}$ and $1 \le g \le \frac{q-1-r'}{2}, \frac{-(q-1)+r'}{2} \le h \le -g$. Set*

$$T_3 = \bigcup C_{s+(eq+f)r} \bigcup C_{s+(gq+h)r},$$

there holds $T_3 \bigcap -qT_3 = \emptyset$.

Proof 1. By Lemma 4 (1), one can get that

$$-qT_1 = \bigcup C_{s+fq-e} \bigcup C_{s+hq-g}.$$

Note that $C_{s+i} = \{s+i, s-i\}$ for $|i| \le \frac{q^2-1}{2}$. From the range of e, f, g and h, it is easy to see that $|fq - e| < \frac{q^2-1}{2}$ and $|hq - g| < \frac{q^2-1}{2}$. Suppose that $T_1 \bigcap -qT_1 \neq \emptyset$, naturally, one can get that some of the following equations hold.

(1.1) $s + eq + f = s + fq - e \Leftrightarrow e(q+1) - f(q-1) = 0$;
(1.2) $s + eq + f = s - fq + e \Leftrightarrow e(q-1) + f(q+1) = 0$;
(1.3) $s + gq + h = s + fq - e \Leftrightarrow fq - e = gq + h$;
(1.4) $s + gq + h = s - fq + e \Leftrightarrow -fq + e = gq + h$;
(2.1) $s + eq + f = s + hq - g \Leftrightarrow hq - g = eq + f$;
(2.2) $s + eq + f = s - hq + g \Leftrightarrow -hq + g = eq + f$;
(2.3) $s + gq + h = s + hq - g \Leftrightarrow g(q+1) - h(q-1) = 0$;
(2.4) $s + gq + h = s - hq + g \Leftrightarrow g(q-1) + h(q+1) = 0$.

From $0 \le e \le \frac{q-3}{2}, e+1 \le f \le \frac{q-1}{2}$, it follows that
$e(q+1) - f(q-1) \le e(q+1) - (e+1)(q-1) < 0$
and $e(q-1) + f(q+1) \ge e(q-1) + (e+1)(q+1) > 0$, which contradicts to (1.1) and (1.2).
From $1 \le g \le \frac{q-1}{2}, -\frac{q-1}{2} \le h \le -g$, we have
$g(q+1) - h(q-1) \ge g(q+1) + g(q-1) > 0$
and $g(q-1) + h(q+1) \le g(q-1) - g(q+1) < 0$. Hence, (2.3) and (2.4) do not hold, either.
Note the range of e, f, g and h, one can get that $hq - g \le -gq - g < 0 < eq + f$ and $-fq + e \le -(e+1)q + e < 0 < gq + h$, which contradicts to (2.1) and (1.4), respectively.
It is clear that $-hq + g = eq + f$ if and only if $-h = e$ and $g = f$. If $g = f$, then $e + 1 \le g = f \le \frac{q-1}{2}$. From $-h \ge g \ge e + 1$, it is easy to derive that $-h \neq e$, implying that (2.2) does not hold. Analogously, one can deduce that (1.3) cannot hold.

Summarizing all the cases above, (1) holds.

2. From Lemma 4 (2), if r' is odd, one can derive that

$$-qT_2 = \bigcup C_{\frac{q^2+1}{2}+(fq-e)r} \bigcup C_{\frac{q^2+1}{2}+(hq-g)r} \bigcup C_{\frac{q^2+1}{2}+(lq-k)r}.$$

Note that $C_{s+ir} = \{s+ir, s-ir\}$. For $1 \leq |i| \leq \frac{(q-1)r'}{2}$, it is not difficult to derive that $C_{\frac{q^2+1}{2}+ir} = \{\frac{q^2+1}{2}+ir, \frac{q^2+1}{2}-ir\}$. However, for $|i| > \frac{(q-1)r'}{2}$, from $\frac{q^2+1}{2}-|i|r < 0$, one can deduce that $C_{\frac{q^2+1}{2}+ir} = \{\frac{q^2+1}{2}+|i|r, \frac{q^2+1}{2}-|i|r+rn\} = \{\frac{q^2+1}{2}+|i|r, \frac{q^2+1}{2}+(n-|i|)r\}$. Hence, assume that $T_2 \bigcap -qT_2 \neq \emptyset$, one can confirm that some of the following equations hold and we need to split discussions according to the range of $|i|$.

1. Note that $0 \leq fq-e \leq \frac{q(r'-1)}{2} < \frac{(q-1)r'}{2}$.

(1.1) $s+(eq+f)r = \frac{q^2+1}{2}+(fq-e)r \Leftrightarrow e(q+1)-f(q-1)+\frac{q^2+1}{2} = 0$;
(1.2) $s+(eq+f)r = \frac{q^2+1}{2}-(fq-e)r \Leftrightarrow e(q-1)+f(q+1)+\frac{q^2+1}{2} = 0$;
(1.3) $s+(gq+h)r = \frac{q^2+1}{2}+(fq-e)r \Leftrightarrow \left(\frac{q}{2}+g\right)q+\frac{1}{2}+h = fq-e$;
(1.4) $s+(gq+h)r = \frac{q^2+1}{2}-(fq-e)r \Leftrightarrow \left(\frac{q}{2}+g\right)q+\frac{1}{2}+h = -fq+e$;
(1.5) $s+(kq+l)r = \frac{q^2+1}{2}+(fq-e)r \Leftrightarrow \left(\frac{q}{2}+k\right)q+\frac{1}{2}+l = fq-e$;
(1.6) $s+(kq+l)r = \frac{q^2+1}{2}-(fq-e)r \Leftrightarrow \left(\frac{q}{2}+k\right)q+\frac{1}{2}+l = -fq+e$.

2. Note that $-\frac{(q-1)(q-2)}{2} \leq (-\frac{q-1}{2}+g)q-g \leq hq-g \leq \frac{q(r'-1)}{2}-1 < \frac{(q-1)r'}{2}$.

(2.1) if $hq-g \geq -\frac{(q-1)r'}{2}$, then $s+(eq+f)r = \frac{q^2+1}{2}+(hq-g)r \Leftrightarrow \left(\frac{q}{2}+e\right)q+\frac{1}{2}+f = hq-g$;
(2.2) if $hq-g < -\frac{(q-1)r'}{2}$, then $s+(eq+f)r = \frac{q^2+1}{2}+(n+hq-g)r \Leftrightarrow eq+f = \left(\frac{q}{2}+h\right)q+\frac{1}{2}-g$;
(2.3) $s+(eq+f)r = \frac{q^2+1}{2}-(hq-g)r \Leftrightarrow \left(\frac{q}{2}+e\right)q+\frac{1}{2}+f = -hq+g$;
(2.4) if $hq-g \geq -\frac{(q-1)r'}{2}$, then $s+(gq+h)r = \frac{q^2+1}{2}+(hq-g)r \Leftrightarrow gq+h+\frac{q^2+1}{2} = hq-g$;
(2.5) if $hq-g < -\frac{(q-1)r'}{2}$, then $s+(gq+h)r = \frac{q^2+1}{2}+(n+hq-g)r \Leftrightarrow gq+h = \left(\frac{q}{2}+h\right)q+\frac{1}{2}-g$;
(2.6) $s+(gq+h)r = \frac{q^2+1}{2}-(hq-g)r \Leftrightarrow \left(\frac{q}{2}+g\right)q+\frac{1}{2}+h = -hq+g$;
(2.7) if $hq-g \geq -\frac{(q-1)r'}{2}$, then $s+(kq+l)r = \frac{q^2+1}{2}+(hq-g)r \Leftrightarrow \left(\frac{q}{2}+k\right)q+\frac{1}{2}+l = hq-g$;
(2.8) if $hq-g < \frac{(q-1)r'}{2}$, then $s+(kq+l)r = \frac{q^2+1}{2}+(n+hq-g)r \Leftrightarrow kq+l = (\frac{q}{2}+h)q+\frac{1}{2}-g$;
(2.9) $s+(kq+l)r = \frac{q^2+1}{2}-(hq-g)r \Leftrightarrow \left(\frac{q}{2}+k\right)q+\frac{1}{2}+l = -hq+g$.

3. Note that $-q^2+\frac{(q+1)r'}{2}=\frac{-(2q-1)+r'}{2}q-\frac{q-r'}{2}\le lq-k\le(-\frac{q-1}{2}-k)q-k\le -\frac{(q-1)(q+2)}{2}-2<-\frac{(q-1)r'}{2}$.

(3.1) $s+(eq+f)r=\frac{q^2+1}{2}+(n+lq-k)r\Leftrightarrow eq+f=\left(\frac{q}{2}+l\right)q+\frac{1}{2}-k$;
(3.2) $s+(eq+f)r=\frac{q^2+1}{2}-(lq-k)r\Leftrightarrow\left(\frac{q}{2}+e\right)q+\frac{1}{2}+f=-lq+k$;
(3.3) $s+(gq+h)r=\frac{q^2+1}{2}+(n+lq-k)r\Leftrightarrow gq+h=\left(\frac{q}{2}+l\right)q+\frac{1}{2}-k$;
(3.4) $s+(gq+h)r=\frac{q^2+1}{2}-(lq-k)r\Leftrightarrow\left(\frac{q-1}{2}+g\right)q+\frac{q+1}{2}+h=-lq+k$.
(3.5) $s+(kq+l)r=\frac{q^2+1}{2}+(n+lq-k)r\Leftrightarrow k(q+1)-l(q-1)-\frac{q^2+1}{2}=0$;
(3.6) $s+(kq+l)r=\frac{q^2+1}{2}-(lq-k)r\Leftrightarrow k(q-1)+l(q+1)+\frac{q^2+1}{2}=0$;

Similar to the proof in (1), all of the equations in (1) and (3) do not hold indeed. We just select (2.4)–(2.9) in (2) and (3.4) in (3) to illustrate our claim. From the range of g and h, it is not difficult to derive the following important results:

for $1\le g\le\frac{q-r'}{2}-1$ and $-\frac{q-1}{2}+g\le h\le-\frac{r'+1}{2}$, one can get that $hq-g\le-\frac{r'+1}{2}q-1<-\frac{(q-1)r'}{2}$;

for $1\le g\le\frac{q-r'}{2}$ and $-\frac{r'-1}{2}\le h\le\frac{r'-1}{2}$, one can get that $hq-g\ge-\frac{r'-1}{2}q-1>-\frac{(q-1)r'}{2}$.

Seeking a contradiction to (2.4), if $1\le g\le\frac{q-r'}{2}$ and $-\frac{r'-1}{2}\le h\le\frac{r'-1}{2}$, then $gq+h+\frac{q^2+1}{2}\ge\frac{q^2+2q-r'+2}{2}>\frac{(q-1)r'}{2}>hq-g$, a contradiction.

Seeking a contradiction to (2.5), if $-\frac{q-1}{2}+g\le h\le-\frac{r'+1}{2}$, from $\frac{q}{2}+h\ge-\frac{q-1}{2}+\frac{q}{2}+g=g+\frac{1}{2}$, it is easy to derive a contradiction that $\frac{q}{2}+h>g$, implying that 2.5) does not hold.

Seeking a contradiction to (2.6), note that $\left(\frac{q}{2}+g\right)q+\frac{1}{2}+h=-hq+g$ if and only if $\frac{q}{2}+g=-h$ and $\frac{1}{2}+h=g$. From $-h\le\frac{q-1}{2}+g=\frac{q}{2}+g-\frac{1}{2}$, clearly, we have $-h<\frac{q}{2}+g$, which yields a contradiction.

Seeking a contradiction to (2.7), if $-\frac{r'-1}{2}\le h\le\frac{r'-1}{2}$, from $1\le k\le\frac{q-r'}{2}$, it follows that $\frac{q}{2}+k>h$, which implies that (2.7) cannot hold.

Seeking a contradiction to (2.8), similarly, suppose that (2.8) holds, thus, one can get that $k=\frac{q}{2}+h$ and $l=\frac{1}{2}-g$. If $-\frac{q-1}{2}+g\le h\le-\frac{r'+1}{2}$, then $k=\frac{q}{2}+h\ge\frac{1}{2}+g$. Considering that $-l\ge\frac{q-1}{2}+k\ge\frac{q-1}{2}+\frac{1}{2}+g$, we have $l\le\frac{1}{2}-g-\frac{q+1}{2}$, a contradiction.

Seeking a contradiction to (2.9), from $\left(\frac{q}{2}+k\right)q+\frac{1}{2}+l=-hq+g$, one can obtain that $\frac{q}{2}+k=-h$ and $\frac{1}{2}+l=g$. However, it is obvious that $\frac{1}{2}+l\le-\frac{q-2}{2}-k<0<g$, a contradiction.

Seeking a contradiction to (3.4), from $\left(\frac{q-1}{2}+g\right)q+\frac{q+1}{2}+h=-lq+k$, one can get that $\frac{q-1}{2}+g=-l\ge\frac{q-1}{2}+k$ and $\frac{q+1}{2}+h=k$. Note that $-\frac{q-1}{2}+g\le h\le\frac{r'-1}{2}$. Then, $\frac{q+1}{2}+h\ge g+1\ge k+1$, a contradiction.

Considering that all of those equations in (1), (2) and (3) could not hold, we can conclude that our assumption is impossible and $T_2\bigcap-qT_2=\emptyset$.

(3) By Lemma 4 (3), if r' is even, then it is easy to see that

$$-qT_3 = \bigcup C_{s+(fq-e)r} \bigcup C_{s+(hq-g)r}.$$

Note that $C_{s+ir} = \{s+ir, s-ir\}$. For $1 \le |i| \le \frac{(q-1)(r-1)r'}{2}$, there holds $C_{s+ir} = \{s+ir, s-ir\}$. For $|i| > \frac{(q-1)(r-1)r'}{2}$, it follows that $C_{s+ir} = \{s+|i|r-rn, s-|i|r\} = \{s+(|i|-n)r, s-|i|r\}$ since $s+|i|r > rn$. Similar to the proof in (2), (3) follows. □

According to the definition of decomposition of a defining set T, we could calculate the number of entanglement bits $c = |T_{\mathrm{ss}}| = |T \bigcap -qT|$ in the following theorem.

Theorem 2 *Let n, q, r, r', s be given as above. Keep the notations defined in Lemma 5.*

1. *If $r = 1$ or r' is even, denote a constacyclic code $\mathcal{C}$ (including cyclic code) with defining set $T = C_s \bigcup C_{s+r} \bigcup \cdots \bigcup C_{s+\alpha(q-1)r}$, then $|T_{\mathrm{ss}}| = 1 + 4\alpha(\alpha-1)$, where $\alpha \in [1, \frac{q+1}{2}]$ if $r = 1$ and $\alpha \in [1, \frac{q+1-r'}{2}]$ if r' is even.*
2. *If r' is odd, denote a constacyclic code $\mathcal{C}$ with defining set $T = C_s \bigcup C_{s+r} \bigcup \cdots \bigcup C_{s+\frac{2\alpha+1}{2}(q-1)r}$, then $|T_{\mathrm{ss}}| = 4\alpha^2$, where $\alpha \in [1, \frac{q-r'}{2}]$.*

Proof 1. We divide our discussions into two subcases as to r and r'.

(1.1) If $r = 1$, let $T_1 = \bigcup C_{s+eq+f} \bigcup C_{s+gq+h}$, where $0 \le e \le \frac{q-3}{2}$, $e+1 \le f \le \frac{q-1}{2}$ and $1 \le g \le \frac{q-1}{2}$, $-\frac{q-1}{2} \le h \le -g$, then it follows that $T_1 \bigcap -qT_1 = \emptyset$ by Lemma 5 (1).

Set $\overline{T_1} = C_s \bigcup C_{s+uq+v}$, where $1 \le u \le \frac{q-1}{2}$, $-u+1 \le v \le u$. Analogous to the proof in Lemma 5, it is easy to deduce that $(\bigcup C_{s+uq+v}) \bigcap -q(\bigcup C_{s+uq+v}) = \emptyset$. Then, $\overline{T_1} \bigcap -q\overline{T_1} = C_s$ since $-qC_s = C_s$ and $(\bigcup C_{s+uq+v}) \bigcap -qC_s = \emptyset$.

From the range of e, f, g, h, u and v, let $\alpha = \frac{q+1}{2}$, it is not difficult to check that $T = C_s \bigcup C_{s+eq+f} \bigcup C_{s+gq+h} \bigcup C_{s+uq+v} = T_1 \bigcup \overline{T_1}$. Thus, $T_{\mathrm{ss}} = T \bigcap -qT = (T_1 \bigcup \overline{T_1}) \bigcap -q(T_1 \bigcup \overline{T_1}) = (T_1 \bigcap -qT_1) \bigcup (T_1 \bigcap -q\overline{T_1}) \bigcup (\overline{T_1} \bigcap -qT_1) \bigcup (\overline{T_1} \bigcap -q\overline{T_1}) = C_s \bigcup (T_1 \bigcap -q\overline{T_1}) \bigcup (\overline{T_1} \bigcap -qT_1)$.

According to Lemma 4 (1), there holds $-q\overline{T_1} = C_s \bigcup C_{s+vq-u}$. Note that $C_{s+i} = \{s+i, s-i\}$ for $|i| \le \frac{q^2-1}{2}$. We split our discussions into the following two cases in view of $vq-u > 0$ and $vq-u < 0$.

Case 1 If $vq-u > 0$, then one can obtain that $1 \le v \le u \le \frac{q-1}{2}$. Combining that $-\frac{q-1}{2} \le -u \le -1$, we have $(\bigcup C_{s+vq-u}) \subseteq (\bigcup C_{s+gq+h})$, which means that $T_1 \bigcap -q\overline{T_1} = \bigcup C_{s+vq-u}$. Note that $\overline{T_1} \bigcap -qT_1 = -q(T_1 \bigcap -q\overline{T_1}) = -q(\bigcup C_{s+vq-u}) = \bigcup C_{s+uq+v}$. Therefore, one can get that $T_{\mathrm{ss}} = C_s \bigcup C_{s+vq-u} \bigcup C_{s+uq+v}$.

Case 2 If $vq-u < 0$, then one can obtain that $-u+1 \le v \le 0$. Note that $C_{s+vq-u} = \{s+vq-u, s-vq+u\} = C_{s-vq+u}$. Thus, from $0 \le -v \le u-1 \le \frac{q-3}{2}$ and $1 \le u \le \frac{q-1}{2}$, one can conclude that $(\bigcup C_{s+vq-u}) = (\bigcup C_{s-vq+u}) \subseteq (\bigcup C_{s+eq+f})$, implying that $T_1 \bigcap -q\overline{T_1} = \bigcup C_{s+vq-u}$. Then, it follows that $T_{\mathrm{ss}} = C_s \bigcup C_{s+vq-u} \bigcup C_{s+uq+v}$ similarly.

Combining both Case 1 and Case 2, one can derive that $T_{ss} = C_s \bigcup C_{s+vq-u} \bigcup C_{s+uq+v}$. Next, we discuss the value of $|T_{ss}|$. As given above, it is clear that $|C_{s+i}| = 2$ for $i \neq 0$.

If $\alpha = 1$ and $T = C_s \bigcup C_{s+1} \bigcup \cdots \bigcup C_{s+q-1}$, then $\overline{T_1} = C_s$. Obviously, $|T_{ss}| = |C_s| = 1$.

If $\alpha = 2$ and $T = C_s \bigcup C_{s+1} \bigcup \cdots \bigcup C_{s+2q-2}$, then $\overline{T_1} = C_s \bigcup C_{s+uq+v}$, where $u = 1$. $|T_{ss}| = |C_s \bigcup C_{s+vq-u} \bigcup C_{s+uq+v}| = |C_s| + 2|\bigcup C_{s+uq+v}| = 1 + 8 \times 1$.

If $\alpha = 3$ and $T = C_s \bigcup C_{s+1} \bigcup \cdots \bigcup C_{s+3q-3}$, then $\overline{T_1} = C_s \bigcup C_{s+uq+v}$, where $1 \leq u \leq 2$. $|T_{ss}| = |C_s \bigcup C_{s+vq-u} \bigcup C_{s+uq+v}| = |C_s| + 2|\bigcup C_{s+uq+v}| = 1 + 8 \times 1 + 8 \times 2$.

$\cdots$

If $T = C_s \bigcup C_{s+1} \bigcup \cdots \bigcup C_{s+\alpha(q-1)}$, then $\overline{T_1} = C_s \bigcup C_{s+uq+v}$, where $1 \leq \alpha \leq \frac{q+1}{2}$ and $1 \leq u \leq \alpha - 1$. Thus, $|T_{ss}| = |C_s \bigcup C_{s+vq-u} \bigcup C_{s+uq+v}| = |C_s| + 2|\bigcup C_{s+uq+v}| = 1 + 8 \times 1 + 8 \times 2 + \cdots + 8 \times (\alpha - 1) = 1 + 4\alpha(\alpha - 1)$.

(1.2) If r' is even, as given in Lemma 5 (3), let $T_3 = \bigcup C_{s+(eq+f)r} \bigcup C_{s+(gq+h)r}$, where $0 \leq e \leq \frac{q-1-r'}{2}$, $e+1 \leq f \leq \frac{q-1+r'}{2}$ and $1 \leq g \leq \frac{q-1-r'}{2}$, $\frac{-(q-1)+r'}{2} \leq h \leq -g$, then $T_3 \bigcap -qT_3 = \emptyset$. Denote that $\overline{T_3} = C_s \bigcup C_{s+(uq+v)r}$, where $1 \leq u \leq \frac{q-1}{2}$, $-u+1 \leq v \leq u$, similar to the discussion in (1.1), the desired results are easy to obtain.

(2) If r' is odd, let $T_2 = \bigcup C_{s+(eq+f)r} \bigcup C_{s+(gq+h)r} \bigcup C_{s+(kq+l)r}$, where $e = 0, 0 \leq f \leq \frac{r'-1}{2}, 1 \leq g \leq \frac{q-r'}{2}, -\frac{q-1}{2} + g \leq h \leq \frac{r'-1}{2}$ and $1 \leq k \leq \frac{q-r'}{2}$, $\frac{-(2q-1)+r'}{2} \leq l \leq -\frac{q-1}{2} - k$, then $T_2 \bigcap -qT_2 = \emptyset$ by Lemma 5 (2).

Denote that $\overline{T_2} = \bigcup C_{s+(uq+v)r}$, where $1 \leq u \leq \frac{q-r'}{2}$, $-\frac{q-3}{2} - u \leq v \leq -\frac{q+1}{2} + u$. Then, $-q\overline{T_2} = \bigcup C_{\frac{q^2+1}{2}+(vq-u)r}$ from Lemma 4 (2). According to the method used in the proof of Lemma 5, one can know that $\overline{T_2} \bigcap -q\overline{T_2} = \emptyset$. Let $\alpha = \frac{q-r'}{2}$, it is easy to see that $T = T_2 \bigcup \overline{T_2}$. Hence, there holds $T_{ss} = T \bigcap -qT = (T_2 \bigcap -q\overline{T_2}) \bigcup (\overline{T_2} \bigcap -qT_2)$.

From the range of u and v, it is clear that $-\frac{2q^2-2q-r'(q+1)}{2} \leq (-\frac{q-3}{2} - u)q - u \leq vq - u \leq (-\frac{q+1}{2} + u)q - u \leq -\frac{r'(q-1)+2q}{2} < -\frac{(q-1)r'}{2}$. As discussed in Lemma 5 (2), we know that $C_{\frac{q^2+1}{2}+(vq-u)r} = \{\frac{q^2+1}{2} - (vq-u)r, \frac{q^2+1}{2} + (n+vq-u)r\} = \{\frac{q^2+1}{2} - (vq-u)r, s + (\frac{q^2+1}{2} + vq - u)r\}$. Note that $\frac{q^2+1}{2} - \frac{2q^2-2q-r'(q+1)}{2} \leq \frac{q^2+1}{2} + vq - u \leq \frac{q^2+1}{2} - \frac{r'(q-1)+2q}{2} = \frac{(q-1)(q-1-r')}{2} < \frac{(q-1)(r-1)r'}{2}$. Therefore, one can know that $C_{\frac{q^2+1}{2}+(vq-u)r} = C_{s+(\frac{q^2+1}{2}+vq-u)r} = \{s-((\frac{q-1}{2}+v)q+\frac{q+1}{2}-u)r, s+((\frac{q-1}{2}+v)q+\frac{q+1}{2}-u)r\} = \{s-((\frac{q+1}{2}+v)q-\frac{q-1}{2}-u)r, s+((\frac{q+1}{2}+v)q-\frac{q-1}{2}-u)r\}$.

Next, our discussions are divided into two cases according to u, v.

Case 1 Note that $C_{\frac{q^2+1}{2}+(vq-u)r} = \{s-((\frac{q-1}{2}+v)q+\frac{q+1}{2}-u)r, s+((\frac{q-1}{2}+v)q+\frac{q+1}{2}-u)r\}$. If $1 \leq u \leq \frac{q-r'}{2}$, $-\frac{q-3}{2} - u \leq v \leq -\frac{q+1}{2}$, then $1 \leq -(\frac{q-1}{2}+v) \leq u-1 < \frac{q-r'}{2}$, $-\frac{q-1}{2} \leq -(\frac{q+1}{2} - u) \leq -\frac{r'+1}{2}$. It is easy to see that $(\bigcup C_{\frac{q^2+1}{2}+(vq-u)r}) \subseteq$

$(\bigcup C_{s+(gq+h)r})$, implying that $T_2 \bigcap -q\overline{T_2} = -q\overline{T_2} = \bigcup C_{\frac{q^2+1}{2}+(vq-u)r}$. Naturally, one can deduce that $\overline{T_2} \bigcap -qT_2 = \overline{T_2} = \bigcup C_{s+(uq+v)r}$. Hence, $T_{ss} = -q\overline{T_2} \bigcup \overline{T_2}$.

Case 2 Note that $C_{\frac{q^2+1}{2}+(vq-u)r} = \{s - ((\frac{q+1}{2}+v)q - \frac{q-1}{2} - u)r, s + ((\frac{q+1}{2}+v)q - \frac{q-1}{2} - u)r\}$. If $1 \le u \le \frac{q-r'}{2}$, $-\frac{q-1}{2} \le v \le -\frac{q+1}{2} + u$, then $1 \le \frac{q+1}{2} + v \le u \le \frac{q-r'}{2}$, $\frac{-(2q-1)+r'}{2} \le -\frac{q-1}{2} - u \le -\frac{q+1}{2}$. It is not difficult to check that $(\bigcup C_{\frac{q^2+1}{2}+(vq-u)r}) \subseteq (\bigcup C_{s+(kq+k)r})$, which means that $T_2 \bigcap -q\overline{T_2} = -q\overline{T_2} = \bigcup C_{\frac{q^2+1}{2}+(vq-u)r}$. Similar to Case 1, we have $T_{ss} = -q\overline{T_2} \bigcup \overline{T_2}$.

Combining Case 1 and Case 2, we could conclude that $T_{ss} = -q\overline{T_2} \bigcup \overline{T_2}$ and compute $|T_{ss}|$ as follows.

If $\alpha = 1$ and $T = C_s \bigcup C_{s+r} \bigcup \cdots \bigcup C_{s+\frac{3}{2}(q-1)r}$, then $\overline{T_2} = \bigcup C_{s+(uq+v)r}$, where $u = 1$. Thus, $|T_{ss}| = |-q\overline{T_2} \bigcup \overline{T_2}| = 2|\overline{T_2}| = 4$.

If $\alpha = 2$ and $T = C_s \bigcup C_{s+r} \bigcup \cdots \bigcup C_{s+\frac{5}{2}(q-1)r}$, then $\overline{T_2} = \bigcup C_{s+(uq+v)r}$, where $1 \le u \le 2$, it follows that $|T_{ss}| = |-q\overline{T_2} \bigcup \overline{T_2}| = 2|\overline{T_2}| = 4 + 12$.

If $\alpha = 3$ and $T = C_s \bigcup C_{s+r} \bigcup \cdots \bigcup C_{s+\frac{7}{2}(q-1)r}$, then $\overline{T_2} = \bigcup C_{s+(uq+v)r}$, where $1 \le u \le 3$, it follows that $|T_{ss}| = |-q\overline{T_2} \bigcup \overline{T_2}| = 2|\overline{T_2}| = 4 + 12 + 20$.

...

From the above analysis, if $T = C_s \bigcup C_{s+r} \bigcup \cdots \bigcup C_{s+\frac{2\alpha+1}{2}(q-1)r}$, then $\overline{T_2} = \bigcup C_{s+(uq+v)r}$, where $1 \le \alpha \le \frac{q-r'}{2}$ and $1 \le u \le \alpha$, one can deduce that $|T_{ss}| = |-q\overline{T_2} \bigcup \overline{T_2}| = 2|\overline{T_2}| = 4 + 12 + 20 + \cdots + (8\alpha - 4) = 4\alpha^2$. □

Example 1 Let $q = 5$, then $n = q^2 + 1 = 26$. From $rr' = (q+1)$, it follows that $r = 1, 2, 3$ and 6. Next, we illustrate our conclusions mentioned above when $r = 1$, $r = 2$ and $r = 3$.

(1) For $r = 1$, by Theorem 2 (1), one can get that $T = C_{13} \bigcup C_{14} \bigcup \cdots \bigcup C_{13+4\alpha}$, where $\alpha \in [1, 3]$.
If $\alpha = 1$, then $T = C_{13} \bigcup C_{14} \bigcup \cdots \bigcup C_{17}$. From Lemma 5, one knows that $T_1 = C_{14} \bigcup \cdots \bigcup C_{17}$ and $\overline{T_1} = C_{13}$. It is easy to see that $T_{ss} = C_{13} \bigcup (T_1 \bigcap -q\overline{T_1}) \bigcup (\overline{T_1} \bigcap -qT_1) = C_{13}$, implying that $|T_{ss}| = 1$.
If $\alpha = 2$, then $T = C_{13} \bigcup C_{14} \bigcup \cdots \bigcup C_{21}$. From Lemma 5, one can obtain that $T_1 = C_{14} \bigcup C_{15} \bigcup C_{16} \bigcup C_{17} \bigcup C_{20} \bigcup C_{21}$ and $\overline{T_1} = C_{13} \bigcup C_{18} \bigcup C_{19}$. It is not difficult to check that $T_{ss} = C_{13} \bigcup C_{18} \bigcup C_{19} \bigcup C_{14} \bigcup C_{17}$, implying that $|T_{ss}| = 9$.
If $\alpha = 3$, then $T = C_{13} \bigcup C_{14} \bigcup \cdots \bigcup C_{25}$. From Lemma 5, one knows that $T_1 = C_{14} \bigcup C_{15} \bigcup C_{16} \bigcup C_{17} \bigcup C_{20} \bigcup C_{21}$ and $\overline{T_1} = C_{13} \bigcup C_{18} \bigcup C_{19} \bigcup C_{22} \bigcup C_{23} \bigcup C_{24} \bigcup C_{25}$. Hence, $T_{ss} = C_{13} \bigcup C_{14} \cdots \bigcup C_{25}$, implying that $|T_{ss}| = 26$.

(2) For $r = 2$, then $r' = 3$ is odd. By Theorem 2 (2), one can get that $T = C_{39} \bigcup C_{41} \bigcup \cdots \bigcup C_{51}$.
From Lemma 5, one knows that $T_1 = C_{39} \bigcup C_{41} \bigcup C_{43} \bigcup C_{47} \bigcup C_{49} \bigcup C_{51}$ and $\overline{T_1} = C_{45}$. Then, there holds that $T_{ss} = (T_1 \bigcap -q\overline{T_1}) \bigcup (\overline{T_1} \bigcap -qT_1) = C_{43} \bigcup C_{45}$, implying that $|T_{ss}| = 4$.

(3) For $r = 3$, one can deduce that $r' = 2$ is even. From Theorem 2 (1), it is clear that $T = C_{52} \bigcup C_{55} \bigcup \cdots \bigcup C_{52+4\alpha r}$, where $\alpha \in [1, 2]$.
If $\alpha = 1$, then $T = C_{52} \bigcup C_{55} \bigcup C_{58} \bigcup C_{61} \bigcup C_{64}$. By Lemma 5, one can also obtain that $T_1 = C_{55} \bigcup C_{58} \bigcup C_{61} \bigcup C_{64}$ and $\overline{T_1} = C_{52}$. Hence, there holds that $T_{ss} = C_{52} \bigcup (T_1 \bigcap -q\overline{T_1}) \bigcup (\overline{T_1} \bigcap -qT_1) = C_{52}$, which means that $|T_{ss}| = 1$.
If $\alpha = 2$, then $T = C_{52} \bigcup C_{55} \bigcup \cdots \bigcup C_{76}$. It is easy to derive that $T_1 = C_{55} \bigcup C_{58} \bigcup C_{61} \bigcup C_{64} \bigcup C_{73} \bigcup C_{76}$ and $\overline{T_1} = C_{52} \bigcup C_{67} \bigcup C_{70}$. Similarly, one knows that $T_{ss} = C_{52} \bigcup C_{55} \bigcup C_{64} \bigcup C_{67} \bigcup C_{70}$. Therefore, $|T_{ss}| = 9$.

From the above detailed analysis, one can calculate precise parameters of EAQEC codes readily.

Theorem 3 *Let n, q, r, r', s be given as above. Keep the notations defined in Theorem 2.*

1. *If $r = 1$ or r' is even, let $2 + 2(\alpha - 1)(q + 1) \leq d \leq 2 + 2\alpha(q - 1)$ and d be even, then there exist $[[n, n - 2d + 4\alpha(\alpha - 1) + 3, d; 1 + 4\alpha(\alpha - 1)]]_q$ EAQEC codes, where $\alpha \in [1, \frac{q+1}{2}]$ if $r = 1$ and $\alpha \in [1, \frac{q+1-r'}{2}]$ if r' is even.*
   Particularly, for $\alpha \in [1, \frac{q+1}{4}]$, these EAQEC codes are EAQMDS codes.
2. *If r' is odd, let $2 + (2\alpha - 1)(q + 1) \leq d \leq 2 + (2\alpha + 1)(q - 1)$ and d be even, then there exist $[[n, n - 2d + 4\alpha^2 + 2, d; 4\alpha^2]]_q$ EAQEC codes, where $\alpha \in [1, \frac{q-r'}{2}]$.*
   Particularly, for $\alpha \in [1, \frac{q-1}{4}]$, these EAQEC codes are EAQMDS codes.

Proof (1) If $r = 1$ or r' is even, for $2 + 2(\alpha - 1)(q + 1) \leq d \leq 2 + 2\alpha(q - 1)$, let $\mathcal{C}$ be the constacyclic codes (including cyclic codes) with defining set $T = C_s \bigcup C_{s+r} \bigcup \cdots \bigcup C_{s+\frac{d-2}{2}r}$. It is easy to see that $\mathcal{C}$ are MDS codes with parameters $[n, n - d + 1, d]_{q^2}$. From Theorem 2, one can get that $|T_{ss}| = 1 + 4\alpha(\alpha - 1)$. By Theorem 1,

$$[[n, n - 2d + 4\alpha(\alpha - 1) + 3, d; 1 + 4\alpha(\alpha - 1)]]_q,$$

EAQEC codes.

If $\alpha \in [1, \frac{q+1}{4}]$, then there holds $d \leq 2+2\alpha(q-1) = \frac{n+2}{2}$. Note that $n-k+c+2 = 2d$ saturates EA-singleton bound. Obviously, for $\alpha \in [1, \frac{q+1}{4}]$, these constructed EAQEC codes are EAQMDS codes.

(2) Similar to the proof of (1), our desired results are not difficult to obtain. □

From the above theorem, one can derive some maximal entanglement EAQEC codes as below.

Corollary 4 *Let n, q, r, r', s be given as above.*

1. *If $r = 1$, then there exist an $[[n, n - 1, 2; 1]]_q$ maximal entanglement EAQMDS code and an $[[n, 1, n; n - 1]]_q$ maximal entanglement EAQEC code.*
2. *If r' is even, then there exist an $[[n, n-1, 2; 1]]_q$ maximal entanglement EAQMDS code.*

Proof (1) If $r = 1$, let the defining set of a cyclic code be $T = C_s$, then $|T_{ss}| = 1$. From Theorem 1, it follows that there exists an EAQEC code with parameter $[[n, n-1, 2; 1]]_q$. According to the singleton bound for EAQEC codes, this code is an EAQMDS code. Moreover, note that $c = 1 = n-k$, then such code is a maximal entanglement EAQMDS code.

Set $\alpha = \frac{q+1}{2}$, one can get a maximal entanglement EAQEC code with parameter $[[n, 1, n; n-1]]_q$ readily.

(2) Similar to (1), (2) is an immediate consequence. □

4 *q* is an even prime power

In this section, let q be an even prime power. Similarly, before our specific work, we make some notations as well. If $r = 1$, then let $s = \frac{q^2+2}{2}$; if $r \neq 1$, then denote that $rr' = q+1$ and $s = \frac{(q^2+1)(r+1)}{2}$. Clearly, both r and r' are odd integers since q is an even prime power. Next, we discuss the properties of q^2-cyclotomic coset modulo rn in the sequel.

Lemma 6 *Let n, q, r, r', s be given as above.*

1. *If $r = 1$, then $C_{s+i} = \{s+i, s-(i+1)\}$. For $0 \le i \le \frac{q^2-2}{2}$, let $i = uq + v$, where $u \in [0, \frac{q-2}{2}]$, $v \in [0, q-1]$, there holds $-qC_{s+uq+v} = C_{s+\left(\frac{q-1}{2}-v\right)q+u}$.*
2. *If $r \neq 1$, then $C_s = \{s\}$ is a skew symmetric cosets and $C_{s+ir} = \{s+ir, s-ir\}$. For $1 \le i \le \frac{(q-1)(r-1)r'}{2}$, let $i = uq + v$, where $v \in [1, \frac{q-1+r'}{2}]$ if $u = 0$ and $v \in [\frac{-(q-1)+r'}{2}, \frac{q-1+r'}{2}]$ if $u \in [1, \frac{q-1-r'}{2}]$, there holds $-qC_{s+(uq+v)r} = C_{s+(vq-u)r}$.*

Proof (1) Note that q is an even prime power. If $r = 1$, then $sq^2 = \frac{q^4-1+1}{2} + q^2 = \frac{(q^2+1)(q^2-1)+1}{2} + q^2 + 1 - 1 \equiv \frac{q^2}{2} = s - 1 \bmod n$. Hence, there holds $(s+i)q^2 = s - 1 + iq^2 \equiv s - (i+1) \bmod n$, i.e., $C_{s+i} = \{s+i, s-(i+1)\}$. Moreover, $-q(s+i) = -q(s+uq+v) \equiv \frac{2q^2-q+2}{2} - vq + u = s + \left(\frac{q-1}{2} - v\right)q + u \bmod n$, which means that $-qC_{s+uq+v} = C_{s+\left(\frac{q-1}{2}-v\right)q+u}$.

(2) If $r \neq 1$, it is easy to check that $C_s = \{s\}$ since $sq^2 = \frac{(q^2+1)(r+1)}{2}(q^2-1+1) \equiv s \bmod rn$. From $-qs = -\frac{q}{2}(r+1)(q^2+1) \equiv \frac{2r-q}{2}(q^2+1) = \frac{r(2-r')+1}{2}(q^2+1) \equiv s \bmod rn$, it follows that C_s is a skew symmetric coset.

Note that $(s+ir)q^2 \equiv s - ir \bmod rn$. Clearly, $C_{s+ir} = \{s+ir, s-ir\}$. Moreover, it is not difficult to deduce that $-qC_{s+(uq+v)r} = C_{s+(vq-u)r}$. □

Lemma 7 *Let n, q, r, r', s be given as above.*

1. *If $r = 1$, then denote that $0 \le e \le \frac{q-2}{2}$, $0 \le f \le -e + \frac{q-2}{2}$ and $1 \le g \le \frac{q-2}{2}$, $-\frac{q}{2} + g \le h \le -1$. Set*

$$T_1 = \bigcup C_{s+eq+f} \bigcup C_{s+gq+h},$$

there holds $T_1 \bigcap -qT_1 = \emptyset$.

2. *If* $r \neq 1$, *then denote that* $0 \leq e \leq \frac{q-1-r'}{2}, e+1 \leq f \leq \frac{q-1+r'}{2}$ *and* $1 \leq g \leq \frac{q-1-r'}{2}, \frac{-(q-1)+r'}{2} \leq h \leq -g$. *Set*

$$T_2 = \bigcup C_{s+(eq+f)r} \bigcup C_{s+(gq+h)r},$$

there holds $T_2 \bigcap -qT_2 = \emptyset$.

Proof (1) By Lemma 6 (1), it is easy to see that

$$-qT_1 = \bigcup C_{s+\left(\frac{q-1}{2}-f\right)q+e} \bigcup C_{s+\left(\frac{q-1}{2}-h\right)q+g}.$$

Note that $C_{s+i} = \{s+i, s-(i+1)\}$ for $|i| \leq \frac{q^2-2}{2}$. Considering the range of e, f, g and h, we can conclude that $|\left(\frac{q-1}{2} - f\right)q + e| \leq \frac{q^2-2}{2}$ and $\frac{q^2-2}{2} + \frac{q+4}{2} \leq \left(\frac{q-1}{2} - h\right)q + g \leq \left(\frac{2q-1}{2} - g\right)q + g \leq \frac{q^2-2}{2} + \frac{q^2-3q+4}{2}$. Thus, there holds $C_{s+\left(\frac{q-1}{2}-f\right)q+e} = \left\{s + \left(\frac{q-1}{2} - f\right)q + e, s - \left(\left(\frac{q-1}{2} - f\right)q + e + 1\right)\right\}$ and $C_{s+\left(\frac{q-1}{2}-h\right)q+g} = \left\{s + \left(\frac{q-1}{2} - h\right)q + g - q^2, s - \left(\left(\frac{q-1}{2} - h\right)q + g + 1\right) + q^2\right\}$. With the method used in the proof of Lemma 5 (1), our results are easy to obtain.

(2) Also, the proof is analogous to that of Lemma 5, and they are omitted here. □

Theorem 5 *Let* n, q, r, r', s *be given as above. Keep the notations defined in Lemma 7.*

1. *If* $r = 1$, *denote a cyclic code* $\mathcal{C}$ *with defining set* $T = C_s \bigcup C_{s+1} \bigcup \cdots \bigcup C_{s+\frac{q-2}{2}+\alpha(q-1)}$, *then* $|T_{ss}| = 4\alpha^2$, *where* $\alpha \in [1, \frac{q}{2}]$.
2. *If* $r \neq 1$, *denote a constacyclic code* $\mathcal{C}$ *with defining set* $T = C_s \bigcup C_{s+r} \bigcup \cdots \bigcup C_{s+\alpha(q-1)r}$, *then* $|T_{ss}| = 1 + 4\alpha(\alpha-1)$, *where* $\alpha \in [1, \frac{q+1-r'}{2}]$.

Proof Similar to the proof in Theorem 2, it is not difficult to check this theorem. □

Example 2 Let $q = 4$, then $n = q^2 + 1 = 17$. It is easy to see that $r = 1$ and $r = 5$.

1. For $r = 1$, from Theorem 5, it follows that $T = C_9 \bigcup C_{10} \bigcup \cdots \bigcup C_{10+3\alpha}$, where $\alpha \in [1, 2]$.
   If $\alpha = 1$, then $T = C_9 \bigcup C_{10} \bigcup C_{11} \bigcup C_{12} \bigcup C_{13}$. One can obtain that $T_1 = C_9 \bigcup C_{10} \bigcup C_{12} \bigcup C_{13}$ and $\overline{T_1} = C_{11}$ by Lemma 7. Hence, it is not difficult to check that $T_{ss} = (T_1 \bigcap -q\overline{T_1}) \bigcup (\overline{T_1} \bigcap -qT_1) = C_{10} \bigcup C_{11}$, implying that $T_{ss} = 4$.
   If $\alpha = 2$, then $T = C_9 \bigcup C_{10} \bigcup \cdots \bigcup C_{16}$. By Lemma 7, one can get that $T_1 = C_9 \bigcup C_{10} \bigcup C_{12} \bigcup C_{13}$ and $\overline{T_1} = C_{11} \bigcup C_{14} \bigcup C_{15} \bigcup C_{16}$. Thus, $T_{ss} = C_9 \bigcup C_{10} \bigcup \cdots \bigcup C_{16}$ and $|T_{ss}| = 16$.
2. For $r = 5$, one knows that $T = C_{51} \bigcup C_{56} \bigcup \cdots \bigcup C_{51+3\alpha r}$, where $\alpha \in [1, 2]$.
   If $\alpha = 1$, then $T = C_{51} \bigcup C_{56} \bigcup C_{61} \bigcup C_{66}$. From Lemma 7, there holds that $T_1 = C_{56} \bigcup C_{61} \bigcup C_{66}$ and $\overline{T_1} = C_{51}$. Similarly, one can deduce that $T_{ss} = C_{51} \bigcup (T_1 \bigcap -q\overline{T_1}) \bigcup (\overline{T_1} \bigcap -qT_1) = C_{51}$.
   If $\alpha = 2$, then $T = C_{51} \bigcup C_{56} \bigcup C_{61} \bigcup C_{66} \bigcup C_{71} \bigcup C_{76} \bigcup C_{81}$. Thereinto, $T_1 = C_{56} \bigcup C_{61} \bigcup C_{66} \bigcup C_{81}$ and $\overline{T_1} = C_{51} \bigcup C_{71} \bigcup C_{76}$. It is easy to see that $T_{ss} = C_{51} \bigcup C_{56} \bigcup C_{66} \bigcup C_{71} \bigcup C_{76}$, which indicates that $|T_{ss}| = 9$.

From the above consequences, we can obtain some EAQEC codes naturally.

Theorem 6 *Let n, q, r, r', s be given as above. Keep the notations defined in Theorem 5.*

1. *If $r = 1$, let $2 + (2\alpha - 1)(q + 1) \leq d \leq 2 + (2\alpha + 1)(q - 1)$ and d be odd, then there exist $[[n, n - 2d + 4\alpha^2 + 2, d; 4\alpha^2]]_q$ EAQEC codes, where $\alpha \in [1, \frac{q}{2}]$. For $\alpha \in [1, \frac{q-4}{4}]$, these EAQEC codes are EAQMDS codes.*
2. *If $r \neq 1$, let $2 + 2(\alpha - 1)(q + 1) \leq d \leq 2 + 2\alpha(q - 1)$ and d be even, then there exist $[[n, n - 2d + 4\alpha(\alpha - 1) + 3, d; 1 + 4\alpha(\alpha - 1)]]_q$ EAQEC codes, where $\alpha \in [1, \frac{q+1-r'}{2}]$. For $\alpha \in [1, \frac{q}{4}]$, these EAQEC codes are EAQMDS codes.*

Proof If $r = 1$, note that $C_s = \{s, s - 1\}$. Hence, minimum distance d is odd. The rest of proof can be clarified with the method of Theorem 3. □

By Theorem 6, some maximal entanglement EAQEC codes can be obtained readily in the following corollary.

Corollary 7 *Let n, q, r, r', s be given as above.*

1. *If $r = 1$, then there exists an $[[n, 1, n; n - 1]]_q$ maximal entanglement EAQEC code.*
2. *If $r \neq 1$, then there exists an $[[n, n - 1, 2; 1]]_q$ maximal entanglement EAQMDS code.*

5 Code comparisons and conclusions

In this paper, we study q^2-cyclotomic coset modulo rn in detail, where $r \mid (q + 1)$ and $n = q^2 + 1$. If $r \neq 1$, then set $rr' = q + 1$; it is interesting to find that the properties of such cosets are consistent for the same parity of r'. Also, if $r = 1$, the properties of relevant cosets are determined absolutely. Finally, we adopt these results to investigate EAQEC codes of length n with flexible parameters, which are constructed from constacyclic codes (including cyclic codes). Set $d \leq \frac{n+2}{2}$, some EAQMDS codes can be obtained from our construction easily. Notably, all of these EAQMDS codes could be seemed as a generalization of the known codes with length n in Refs. [11–15,18–21,23]. As to EAQEC codes obtained from cyclic codes, their possible parameters are completely computed. Meanwhile, those EAQEC codes constructed from constacyclic codes are discussed for given large minimum distance. In addition, some maximal entanglement EAQEC codes could be derived as well. Compared with those literatures about the constructions of EAQEC codes, our construction provides a new idea for future study.

By Theorems 3 and 6, we could obtain series of new EAQEC codes with comparatively large minimum distance. To illustrate the priority of our constructed codes, we list some specific examples and known codes with the same length in Refs. [12,13,18–21,23,26] in Tables 1, 2, 3, 4 and 5, while in Table 6, we give our general conclusions

Table 1 New EAQEC codes with length n over $\mathbb{F}_3$

r	Paras.	Even d	From	Refs.	Paras.	Even d
$r=1$	$[[10, 13-2d, d; 1]]_3$	$2 \le d \le 6$	Th. 3 (1)	[18]	$[[10, 13-2d, d; 1]]_3$	$2 \le d \le 6$
	$[[10, 1, 10; 9]]_3$	$d=10$		[26]	$[[10, 1, 10; 9]]_3$	$d=10$
$r=2$	$[[10, 13-2d, d; 1]]_3$	$2 \le d \le 6$	Th. 3 (1)			
$r=4$	$[[10, 4, 6; 4]]_3$	$d=6$	Th. 3 (2)			
	$[[10, 0, 8; 4]]_3$	$d=8$		[26]	$[[10, 0, 8; 4]]_3$	$d=8$

Table 2 New EAQEC codes with length n over $\mathbb{F}_4$

r	Paras.	d	From	Refs.	Paras.	d
$r=1$				[12]	$[[17, 19-2d, d]]_4$	$3 \le d \le 5$ odd
				[18]	$[[17, 20-2d, d; 1]]_4$	$2 \le d \le 8$ even
	$*[[17, 23-2d, d; 4]]_4$	$7 \le d \le 9$ odd	Th. 6 (1)	[23]	$[[17, 4, 8; 1]]_4$	$d=8$
					$[[17, 4, 10; 5]]_4$	$d=10$
	$\diamond[[17, 1, 11; 4]]_4$	$d=11$				
	$[[17, 1, 17; 16]]_4$	$d=17$		[26]	$[[17, 1, 17; 16]]_4$	$d=17$
$r=5$	$[[17, 20-2d, d; 1]]_4$	$2 \le d \le 8$ even	Th. 6 (2)			
	$\diamond[[17, 4, 12; 9]]_4$	$d=12$				
	$[[17, 0, 14; 9]]_4$	$d=14$		[26]	$[[17, 0, 14; 9]]_4$	$d=14$

Table 3 New EAQEC codes with length n over $\mathbb{F}_5$

r	Paras.	Even d	From	Refs.	Paras.	Even d
$r=1$	$[[26, 29-2d, d; 1]]_5$	$2 \le d \le 10$	Th. 3 (1)	[18]	$[[26, 29-2d, d; 1]]_5$	$2 \le d \le 10$
				[23]	$[[26, 9, 10; 1]]_5$	$d=10$
					$[[26, 9, 12; 5]]_5$	$d=12$
	$*[[26, 9, 14; 9]]_5$	$d=14$				
	$\diamond[[26, 37-2d, d; 9]]_5$	$15 \le d \le 18$				
	$[[26, 1, 26; 25]]_5$	$d=26$		[26]	$[[26, 1, 26; 25]]_5$	$d=26$
$r=2$				[13]	$[[26, 27-2d, d]]_5$	$2 \le d \le 6$
	$[[26, 32-2d, d; 4]]_5$	$8 \le d \le 14$	Th. 3 (2)	[20]	$[[26, 32-2d, d; 4]]_5$	$8 \le d \le 14$
				[19]	$[[26, 12, 10; 4]]_5$	$d=10$
$r=3$	$[[26, 29-2d, d; 1]]_5$	$2 \le d \le 10$	Th. 3 (1)			
	$*[[26, 9, 14; 9]]_5$	$d=14$				
	$\diamond[[26, 37-2d, d; 9]]_5$	$15 \le d \le 18$				
$r=6$	$[[26, 32-2d, d; 4]]_5$	$8 \le d \le 14$	Th. 3 (2)			
	$\diamond[[26, 4, 20; 16]]_5$	$d=20$				
	$[[26, 0, 22; 16]]_5$	$d=22$		[26]	$[[26, 0, 22; 16]]_5$	$d=22$

Table 4 New EAQEC codes with length n over $\mathbb{F}_7$

r	Paras.	Even d	From	Refs.	Paras.	Even d
$r=1$	$[[50, 53-2d, d; 1]]_7$	$2 \le d \le 14$	Th. 3 (1)	[18]	$[[50, 53-2d, d; 1]]_7$	$2 \le d \le 14$
				[23]	$[[50, 25, 14; 1]]_7$	$d = 14$
					$[[50, 25, 16; 5]]_7$	$d = 16$
	$[[50, 61-2d, d; 9]]_7$	$18 \le d \le 26$			$[[50, 9, 26; 9]]_7$	$d = 26$
					$[[50, 9, 28; 13]]_7$	$d = 28$
					$[[50, 9, 30; 17]]_7$	$d = 30$
	$\diamond[[50, 77-2d, d; 25]]_7$	$34 \le d \le 38$				
	$[[50, 1, 50; 25]]_7$	$d = 50$		[26]	$[[50, 1, 50; 25]]_7$	$d = 50$
$r=2$	$[[50, 53-2d, d; 1]]_7$	$2 \le d \le 14$	Th. 3 (1)			
				[21]	$[[50, 25, 16; 5]]_7$	$d = 16$
	$[[50, 61-2d, d; 9]]_7$	$18 \le d \le 26$			$[[50, 61-2d, d; 9]]_7$	$18 \le d \le 26$
$r=4$	$[[50, 53-2d, d; 1]]_7$	$2 \le d \le 14$	Th. 3 (1)			
	$[[50, 61-2d, d; 9]]_7$	$18 \le d \le 26$				
	$\diamond[[50, 77-2d, d; 25]]_7$	$34 \le d \le 38$				
$r=8$	$[[50, 56-2d, d; 4]]_7$	$10 \le d \le 20$	Th. 3 (2)	[20]	$[[50, 56-2d, d; 4]]_7$	$10 \le d \le 20$
	$*[[50, 16, 26; 16]]_7$	$d = 26$				
	$\diamond[[50, 68-2d, d; 16]]_7$	$28 \le d \le 32$				
	$\diamond[[50, 4, 42; 36]]_7$	$d = 42$				
	$[[50, 0, 44; 36]]_7$	$d = 44$		[26]	$[[50, 0, 44; 36]]_7$	$d = 44$

to make comparisons with those known results in Refs. [11–15,18–23,26], where q is denoted as a prime power. The symbol $*$ in the tables denotes that those corresponding codes are new EAQMDS codes. And the symbol $\diamond$ means those new EAQEC codes.

Tables 1, 2, 3, 4 and 5 show that our construction could produce many new EAQEC codes whose minimum distances are bigger than those known QMDS codes or EAQMDS codes with the same length. That is to say, these new EAQEC codes can perform better on error correction. As shown in Table 6, almost all of those known conclusions about EAQMDS codes with length $n = q^2 + 1$ are some special cases of ours, which means that our construction generalizes the corresponding known results remarkably. Moreover, several maximal entanglement EAQMDS codes with $d = 2$ or maximal entanglement EAQEC codes with $d = n$ can be also obtained easily.

At present, most of the EAQEC codes studied in the literatures are consuming fixed entanglement bits. However, the number of entanglement bits of EAQEC codes derived from our construction is very flexible. We hope that our construction may promote more good consequences in the future.

Table 5 New EAQEC codes with length n over $\mathbb{F}_8$

r	Paras.	d	From	Refs.	Paras.	d
$r=1$				[12]	$[[65, 67-2d, d]]_8$	$3 \le d \le 9$ odd
				[18]	$[[65, 68-2d, d; 1]]_8$	$2 \le d \le 16$ even
	$*[[65, 71-2d, d; 4]]_8$	$11 \le d \le 23$ odd	Th. 6 (1)	[23]	$[[65, 36, 16; 1]]_8$	$d=16$
					$[[65, 36, 18; 5]]_8$	$d=18$
	$*[[65, 83-2d, d; 16]]_8$	$29 \le d \le 33$ odd			$[[65, 16, 30; 9]]_8$	$d=30$
					$[[65, 16, 32; 13]]_8$	$d=32$
					$[[65, 16, 34; 17]]_8$	$d=34$
	$\diamond[[65, 83-2d, d; 16]]_8$	$35 \le d \le 37$ odd			$[[65, 4, 44; 25]]_8$	$d=44$
					$[[65, 4, 46; 29]]_8$	$d=46$
	$\diamond[[65, 103-2d, d; 36]]_8$	$47 \le d \le 51$ odd			$[[65, 4, 48; 33]]_8$	$d=48$
					$[[65, 4, 50; 37]]_8$	$d=50$
	$[[65, 1, 65; 64]]_8$	$d=65$		[26]	$[[65, 1, 65; 64]]_8$	$d=65$
$r=3$	$[[65, 68-2d, d; 1]]_8$	$2 \le d \le 16$ even	Th. 6 (2)			
	$*[[65, 76-2d, d; 9]]_8$	$20 \le d \le 28$ even				
	$[[65, 16, 30; 9]]_8$	$d=30$				
	$\diamond[[65, 92-2d, d; 25]]_8$	$38 \le d \le 42$ even				
	$[[65, 4, 44; 25]]_8$	$d=44$				
$r=9$	$[[65, 68-2d, d; 1]]_8$	$2 \le d \le 16$ even	Th. 6 (2)			
	$*[[65, 76-2d, d; 9]]_8$	$20 \le d \le 28$ even				
	$[[65, 16, 30; 9]]_8$	$d=30$				
	$\diamond[[65, 92-2d, d; 25]]_8$	$38 \le d \le 42$ even				
	$[[65, 4, 44; 25]]_8$	$d=44$				
	$\diamond[[65, 4, 56; 49]]_8$	$d=56$				
	$[[65, 0, 58; 49]]_8$	$d=58$		[26]	$[[65, 0, 58; 49]]_8$	$d=58$

Table 6 Comparisons of QMDS codes and EAQMDS codes with length n over $\mathbb{F}_q$

q	Paras.	d	Refs.
q	$[[n, n-2d+2, d]]_q$	$3 \le d \le \frac{q+2}{2}$	[11]
even q	$[[n, n-2d+2, d]]_q$	$3 \le d \le q+1$ odd	[12]
$q \equiv 1 \bmod 4$	$[[n, n-2d+2, d]]_q$	$2 \le d \le q+1$ even	[13]
q	$[[n, n-2d+2, d]]_q$	$3 \le d \le q+1$	[14]
odd q	$[[n, n-2d+2, d]]_q$	$1 \le d \le q+1$	[15]
even q	$[[n, n-2d+2, d]]_q$	$1 \le d \le q+1$ odd	
q	$[[n, n-2d+3, d; 1]]_q$	$2 \le d \le 2q$ even	[18]
$q \equiv 1 \bmod 4$	$[[n, n-2d+6, d; 4]]_q$	$q+5 \le d \le 2q$ even	[19]
odd $q \ge 5$	$[[n, n-2d+6, d; 4]]_q$	$q+3 \le d \le 3q-1$ even	[20]
q	$[[n, n-d+1, d; d-1]]_q$	$2 \le d \le \frac{n(r-1)+2}{r}$ even	[22]
even q	$[[n, n-d+1, d; d-1]]_q$	$3 \le d \le \frac{n-2+2r}{r}$ odd	
q	$[[n, n-4(m-1)(q+1-m)-1, d; 4(m-1)^2+1-4l]]_q$	$d = 2(m-1)q - 2l + 2$	[23]
$q \equiv 3 \bmod 4, q \ge 7$	$[[n, n-2d+7, d; 5]]_q$	$d = 2q+2$	[21]
	$[[n, n-2d+11, d; 9]]_q$	$2q+4 \le d \le 4q-2$ even	
$q > 2$	$[[n, q-l, q^2-q+2; n-q-l]]_q$	$d = q^2-q+2$	[26]
$q > 2$	$[[n, n-q-l, q+1; q-l]]_q$	$d = q+1$	
$q > 2$	$[[n, k-l, n+1-k; n-k-l]]_q$	$d = n+1-k$	
$q > 2$	$[[n, n-k-l, k+1; k-l]]_q$	$d = k+1$	
odd q	$[[n, n-2d+4\alpha(\alpha-1)+3, d; 1+4\alpha(\alpha-1)]]_q, \alpha \in [1, \frac{q+1}{4}]$	$2+2(\alpha-1)(q+1) \le d \le 2+2\alpha(q-1)$ even	Th. 3 (1)
	$[[n, n-2d+4\alpha^2+2, d; 4\alpha^2]]_q, \alpha \in [1, \frac{q-1}{4}]$	$2+(2\alpha-1)(q+1) \le d \le 2+(2\alpha+1)(q-1)$ even	Th. 3 (2)
even q	$[[n, n-2d+4\alpha^2+2, d; 4\alpha^2]]_q, \alpha \in [1, \frac{q-4}{4}]$	$2+(2\alpha-1)(q+1) \le d \le 2+(2\alpha+1)(q-1)$ odd	Th. 6 (1)
	$[[n, n-2d+4\alpha(\alpha-1)+3, d; 1+4\alpha(\alpha-1)]]_q, \alpha \in [1, \frac{q}{4}]$	$2+2(\alpha-1)(q+1) \le d \le 2+2\alpha(q-1)$ even	Th. 6 (2)

References

1. 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)
2. Grassl, M., Beth, T.: Quantum BCH codes. In: Proceedings X. International Symposium on Theoretical Electrical Engineering Magdeburg, pp. 207–212 (1999)
3. Ashikhim, A., Knill, E.: Non-binary quantum stabilizer codes. IEEE. Trans. Inf. Theory **47**, 3065–3072 (2001)
4. Li, R., Li, X.: Binary construction of quantum codes of minimum distance three and four. IEEE. Trans. Inf. Theory **50**, 1331–1336 (2004)
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. Song, H., Li, R., Wang, J., Liu, Y.: Two classes of BCH codes and new quantum codes. Quantum Inf. Process. **17**(270), 1–24 (2018)
10. Li, R., Wang, J., Liu, Y., Guo, G.: New quantum constacyclic codes. Quantum Inf. Process. **18**(127), 1–23 (2019)
11. 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)
12. Guardia, G.G.L.: New quantum MDS codes. IEEE. Trans. Inf. Theory **57**, 5551–5554 (2011)
13. Kai, X., Zhu, S.: New quantum MDS codes from negacyclic codes. IEEE. Trans. Inf. Theory **59**, 1193–1197 (2013)
14. Jin, L., Xing, C.: A construction of new quantum MDS codes. IEEE. Trans. Inf. Theory **60**, 2921–2925 (2014)
15. Grassl, M., Rtteler, M.: Quantum MDS codes over small fields. In: IEEE IEEE International Symposium on Information Theory, pp. 1104–1108(2015)
16. Brun, T., Devetak, I., Hsieh, M.: Correcting quantum errors with entanglement. Science **314**, 436–439 (2006)
17. Grassl, M.: Entanglement-assisted quantum communication beating the quantum singleton bound. In: AQIS, Taiwan (2016)
18. 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)
19. 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)
20. Lu, L., Ma, W., Li, R., Ma, Y., Liu, Y., Cao, H.: Entanglement-assisted quantum MDS codes from constacyclic codes with large minimum distance. Finite Fields Their Appl. **53**, 309–325 (2018)
21. Mustafa, S., Emre, K.: An application of constacyclic codes to entanglement-assisted quantum MDS codes. Comput. Appl. Math. **38**(75), 1–13 (2019)
22. Qian, J., Zhang, L.: On MDS linear complementary dual codes and entanglement-assisted quantum codes. Des. Codes Cryptogr. **86**, 1565–1572 (2018)
23. Qian, J., Zhang, L.: Constructions of new entanglement-assisted quantum MDS codes and almost MDS codes. Quantum Inf. Process. **18**(71), 1–12 (2019)
24. 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)
25. 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)
26. Fang, W., Fu, F., Li, L., Zhu, S.: Euclidean and Hermitian hulls of MDS codes and their applications to EAQECCs (2018)
27. Wilde, M., Burn, T.: Optimal entanglement formulas for entanglement-assisted quantum coding. Phys. Rev. A **77**, 064302 (2008)
28. Macwilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, Amsterdam (1977)

29. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
30. 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)
31. Krishna, A., Sarwate, D.V.: Pseudo-cyclic maximum-distance separable codes. IEEE. Trans. Inf. Theory **36**, 880–884 (1990)
32. Lü, L., Li, R.: Entanglement-assisted quantum codes constructed from primitive quaternary BCH codes. Int. J. Quantum Inf. **12**(3), 1450015 (2014)