IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 20, 2019, accepted August 22, 2019, date of publication September 13, 2019, date of current version October 2, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2941416

Applications of Constacyclic Codes to Some New Entanglement-Assisted Quantum MDS Codes

JIANZHANG CHEN[1,2], YOUQIN CHEN[3], DONG YU[1], CHUNHUI FENG[1], YUANYUAN HUANG[4], AND RIQING CHEN[1]

[1]College of Computer and Information Sciences, Fujian Agriculture and Forestry University, Fuzhou 350002, China
[2]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[3]State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, Wuhan 430079, China
[4]Department of Network Engineering, Chengdu University of Information Technology, Chengdu 610225, China

Corresponding author: Yuanyuan Huang (yyhuangcuit@126.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61802064, in part by the China Postdoctoral Science Foundation under Grant 2018M633354, and in part by the Natural Science Foundation of Fujian Province, China, under Grant 2016J01281 and Grant 2016J01278.

ABSTRACT Generally, it is not easy to construct quantum maximal-distance-separable (MDS) codes with the minimum distance greater than $\frac{q}{2}+1$. The minimum distance of quantum MDS codes can achieve $\frac{q}{2}+1$ or exceed $\frac{q}{2}+1$ by adopting pre-shared entanglement. In this work, some new families of entanglement-assisted quantum MDS codes that satisfy the quantum Singleton bound are constructed and the number of maximally entangled states required is determined to make the minimum distance of some constructed codes achieve $\frac{q}{2}+1$ or exceed $\frac{q}{2}+1$ by utilizing the decomposition of the defining set and q^2-cyclotomic cosets of constacyclic codes with length $\frac{q^2+1}{\gamma}$, where $\gamma=t^2+1$, t is a power of 2 and $q=t^e>4$ with $e\equiv 1 \bmod 4$ or $e\equiv 3 \bmod 4$. Moreover, the parameters of these codes constructed in this paper are more general relative to the ones in the literature and the minimum distance of some codes constructed in this paper is larger than $\frac{q}{2}+1$.

INDEX TERMS Constacyclic codes, entanglement-assisted quantum codes, maximal-distance-separable (MDS) codes.

I. INTRODUCTION

In the area of quantum information and quantum computing, after the work of Shor [37] and Stean [38], [39], much research on quantum error-correcting codes (quantum codes for short) has been done. Construction of good quantum codes via classical codes is very important for quantum information and quantum computing [3], [5], [7], [8], [16], [19], [32], [33], [37], [40], [41], [46]. Let q be a prime power, a q-ary $[[n,k,d]]_q$ quantum code of length n is a q^k-dimensional subspace of the q^n-dimensional Hilbert space which can detect up to $d-1$ quantum errors and correct up to $\lfloor\frac{d-1}{2}\rfloor$ quantum errors. The minimum distance of the code is d. Quantum MDS codes that satisfy the quantum Singleton bound, that is, $2d=n-k+2$, are constructed from the Hermitian construction by most researchers. Some researchers utilized constacyclic codes including negacyclic codes and cyclic codes to construct quantum MDS codes based on the Hermitian construction. Constacyclic codes have been applied to the construction of quantum MDS codes such that the minimum distance of some codes exceeds $\frac{q}{2}+1$. Kai et al. constructed two families of quantum MDS codes by using negacyclic codes in [17]. Since then, some other families of negacyclic codes or constacyclic codes have been studied. More details could be consulted in [4], [18], [26], [35], [42], [44], [45]. Although quantum stabilizer codes can be constructed from dual-containing (or self-orthogonal) classical codes, it is not an easy task to construct quantum MDS codes with relatively large minimum distance. Except for some special codes' length, most of known q-ary quantum MDS codes have minimum distance less than or equal to $\frac{q}{2}+1$. However, the dual-containing condition forms a barrier in the development of quantum coding theory [28].

Recently, the discovery of the theory of entanglement-assisted quantum codes plays an important role in the area of quantum information and quantum computation.

The associate editor coordinating the review of this manuscript and approving it for publication was Abdullah Iliyasu.

Brun et al. proposed the entanglement-assisted stabilizer formalism in [2]. They showed that some entanglement-assisted quantum codes could be constructed without dual-containing classical quaternary codes if the sender and the receiver shared a certain amount of pre-existing entanglement [2]. An entanglement-assisted quantum code can be denoted as $[[n, k, d; c]]_q$. With the help of c pairs of maximally entangled states, it encodes k information qubits into n channel qubits. Some entanglement-assisted quantum codes with good parameters have constructed in [1], [14], [22], [23], [43]. In [27], Li et al. proposed the concept about a decomposition of the defining set of cyclic codes, and then they used this method to construct some entanglement-assisted quantum codes having good parameters. In [34], Qian et al. constructed some families of entanglement-assisted quantum codes by using arbitrary binary linear codes and showed that the existence of asymptotically good entanglement-assisted quantum codes. In [2], Brun et al. proposed the entanglement-assisted Singleton bound for entanglement-assisted quantum codes, which could be called entanglement-assisted quantum maximum-distance-separable (MDS) codes. In [11], with the help of a small amount of pre-shared maximally entanglement, a construction of entanglement-assisted quantum MDS codes was provided by Fan et al. Guenda et al. introduced the hull of the classical codes and constructed some families of entanglement-assisted quantum MDS codes in [13]. We proposed the decomposition of the defining set of negacyclic codes in [6] and then utilized this method to construct some families of entanglement-assisted quantum MDS codes with different lengths based on the results of [24], [27]. In [28], [29], the decomposition of the defining set of negacyclic codes and constacyclic codes was utilized by Lü et al. to construct some families of entanglement-assisted quantum MDS codes respectively, and some of those constructed codes have larger minimum distance with $d \geq q + 1$. In [25], constacyclic codes of length $n = \frac{q^2-1}{r}$ were utilized by Liu et al. to construct some new entanglement-assisted quantum MDS codes, where $r = 3, 5, 6, 7$ and $q \equiv -1 \bmod r$. In fact, pre-shared entanglement can improve the error-correcting ability of quantum codes. Those quantum MDS codes with the minimum distance not exceeding $\frac{q}{2} + 1$ can exceed $\frac{q}{2} + 1$ or even $q + 1$ by using the method of pre-shared entanglement. Therefore, it is necessary for us to consider the construction of entanglement-assisted quantum MDS codes with larger distance. Moreover, how to determine the number of required shared pairs in the quantum coding theory to make the minimum distance of quantum MDS codes larger than $\frac{q}{2} + 1$ or even $q + 1$ is worth discussing. Although Luo et al. used the Euclidean construction to research some families of entanglement-assisted MDS codes from generalized Reed-Solomon codes and the parameters of the codes constructed in [30] are new and flexible compared with the ones from [6], [13], [29], [36], the authors just considered the Euclidean construction not Hermitian construction. Very recently, Fang et al. utilized the Hermitian hull of generalized Reed-Solomon codes to present several families of entanglement-assisted quantum MDS codes in [12], while they did not consider the case of entanglement-assisted quantum MDS codes with general length $\frac{q^2+1}{\gamma}$, where $\gamma = t^2 + 1$ and t is a power of 2. Moreover, the q^2-cyclotomic cosets used in this paper to character the constacyclic codes with length $\frac{q^2+1}{\gamma}$ is different from the ones used in [9] and we obtain some new families of entanglement-assisted quantum MDS that are different from those constructed in [9].

In this paper, we utilize the decomposition of the defining set of constacyclic codes with length $\frac{q^2+1}{\gamma}$ to determine the number of pre-shared entangled states and then to construct some new families of entanglement-assisted quantum MDS codes with length $\frac{q^2+1}{\gamma}$, which is different from the ones used in [12], [30]. Additionally, other entanglement-assisted quantum MDS codes with the number of entangled states that is more than 5 can be obtained by using the same method of this paper in the Hermitian construction. The higher the number of pre-shared entangled states, the more likely it is that the minimum distance of quantum MDS codes will exceed $\frac{q}{2}+1$, but at the same time, entanglement technology needs to consume additional entanglement resources. Therefore, from the perspective of the consumption of entanglement resources, it is not the case that the larger the number of entangled states are the better. In conclusion, we think it is reasonable that the number of pre-shared entangled states is sufficient to make the minimum distance of MDS codes exceed $\frac{q}{2} + 1$. Furthermore, we can obtain more entanglement-assisted quantum MDS codes with minimum distance that is more than $\frac{q}{2} + 1$ relative to the ones of [10], [20] where the length of entanglement-assisted quantum codes is less general. Some classes of entanglement-assisted quantum MDS codes constructed in this paper are listed as follows.

(1) $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma} - 2d + 3, d; 1]]_q$, where $\gamma = t^2 + 1$ with t is a power of 2, $q = t^e > 4$ with $e \equiv 1 \bmod 4$ and $2 \leq d \leq \frac{2tq+2}{\gamma}$ is even.

(2) $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma} - 2d + 6, d; 4]]_q$, where $\gamma = t^2 + 1$ with t is a power of 2, $q = t^e > 4$ with $e \equiv 1 \bmod 4$ and $\frac{(t+1)q-t+1+2\gamma}{\gamma} \leq d \leq \frac{(3t-1)q+t+3}{\gamma}$ is odd.

(3) $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma} - 2d + 7, d; 5]]_q$, where $\gamma = t^2 + 1$ with t is a power of 2, $q = t^e > 4$ with $e \equiv 1 \bmod 4$ and $\frac{2tq+2+2\gamma}{\gamma} \leq d \leq \frac{2(t+1)q-2t+2}{\gamma}$ is even.

(4) $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma} - 2d + 3, d; 1]]_q$, where $\gamma = t^2 + 1$ with t is a power of 2, $q = t^e$ with $e \equiv 3 \bmod 4$ and $2 \leq d \leq \frac{2tq-2}{\gamma}$ is even.

(5) $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma} - 2d + 6, d; 4]]_q$, where $\gamma = t^2 + 1$ with t is a power of 2, $q = t^e$ with $e \equiv 3 \bmod 4$ and $\frac{(t+1)q+2\gamma+t-1}{\gamma} \leq d \leq \frac{(3t-1)q-t-3}{\gamma}$ is odd for $t \geq 4$, or $\frac{3q+11}{5} \leq d \leq \frac{5q+5}{5}$ is odd for $t = 2$.

(6) $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma} - 2d + 7, d; 5]]_q$, where $\gamma = t^2 + 1$ with t is a power of 2, $q = t^e$ with $e \equiv 3 \bmod 4$ and $\frac{2tq+2\gamma-2}{\gamma} \leq d \leq \frac{2(t+1)q+2t-2}{\gamma}$ is even.

The organization of this paper is as follows. In section 2, we present some definitions and basic results of constacyclic codes and entanglement-assisted quantum codes. In Section 3, we give some families of entanglement-assisted quantum MDS codes that are constructed by utilizing constacyclic codes with length $\frac{q^2+1}{\gamma}$, in which some quantum MDS codes have larger minimum distance exceeding $\frac{q}{2}+1$. The conclusion is given in Section 4.

II. PREMILINARIES

In this section, we recall some basic results about constacyclic codes in [4], [15], [17], [18], [21], [26], [31], [35], [42], [44], [45] and some results of entanglement-assisted quantum codes in [2], [6], [25], [27], [28].

Let F_{q^2} be the finite field with q^2 elements, where q is a power of 2. An $[n,k,d]$ linear code over finite field F_{q^2} of length n is a linear subspace of the vector space $F_{q^2}^n$ and its minimum distance is d. Assume that n is a positive integer relatively prime to q, i.e., $gcd(n,q)=1$. Moreover, we have the following result in [15], [31].

Proposition 1 (Singleton Bound [15], [31]): If an $[n,k,d]$ linear code $\mathcal{C}$ over F_{q^2} exists, then

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

If $k=n-d+1$, then $\mathcal{C}$ is called an MDS code.

For a nonzero element $\lambda \in F_{q^2}^*$, a linear code $\mathcal{C}$ of length n over F_{q^2} is said to be λ-constacyclic if $(\lambda c_{n-1}, c_0, c_1, \cdots, c_{n-2}) \in \mathcal{C}$ for every $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$. When $\lambda=-1$, $\mathcal{C}$ is a negacyclic code. When $\lambda=1$, $\mathcal{C}$ is a cyclic code.

From [17], [18], a q^2-ary λ-constacyclic code $\mathcal{C}$ over F_{q^2} of length n is precisely an ideal in $F_{q^2}[x]/\langle x^n-\lambda\rangle$ and $\mathcal{C}$ can be generated by a monic polynomial $g(x)$ which divides $x^n-\lambda$. Assume that $\lambda \in F_{q^2}^*$ is a primitive r-th root of unity, and then exists a primitive rn-th root of unity over some extension field of F_{q^2}, denoted by η, such that $\eta^n=\lambda$. Let $\xi=\eta^r$, then ξ is a primitive n-th root of unity, which implies that the elements $\eta\xi^i=\eta^{1+ri}$ are the roots of $x^n-\lambda$ for $0 \leq i \leq n-1$. We denote the set $\mathcal{O}_{rn}=\{1+ri|0 \leq i \leq n-1\}$. If $\mathcal{C}$ is a λ-constacyclic code over F_{q^2} of length n with generator polynomial $g(x)$, then the defining set of the constacyclic code $\mathcal{C}=\langle g(x)\rangle$ is the set $Z=\{i \in \mathcal{O}_{rn} \mid \eta^i \textit{ is a root of } g(x)\}$. For each $i \in \mathcal{O}_{rn}$, the q^2-cyclotomic coset modulo rn containing i is $C_i=\{i, iq^2, iq^4, \cdots, iq^{2k-2}\}$ mod rn, where k is the smallest positive integer such that $iq^{2k} \equiv i$ mod rn. The defining set Z of constacyclic $\mathcal{C}$ is the union of some q^2-cyclomic cosets modulo rn. The following proposition gives the BCH bound of constacyclic codes.

Proposition 2 (The BCH Bound for Constacyclic Codes [18], [21]): Let $\mathcal{C}$ be a q^2-ary λ-constacyclic code of length n. If the generator polynomial $g(x)$ of $\mathcal{C}$ has the elements $\{\eta^{1+ri} \mid 0 \leq i \leq d-2\}$ as the roots where η is a primitive rn-th root of unity, then the minimum distance of $\mathcal{C}$ is at least d.

Let $a^q=(a_0^q, a_1^q, \cdots, a_{n-1}^q)$ denote the conjugation of the vector $a=(a_0, a_1, \cdots, a_{n-1})$. For $u=(u_0, u_1, \cdots, u_{n-1})$ and $v=(v_0, v_1, \cdots, v_{n-1}) \in F_{q^2}^n$, the Hermitian inner product is defined as

$$\langle u, v\rangle_h = u_0 v_0^q + u_1 v_1^q + \cdots + u_{n-1} v_{n-1}^q.$$

The Hermitian dual code of $\mathcal{C}$ can be defined as

$$\mathcal{C}^{\perp_h} = \{u \in F_{q^2}^n \mid \langle u, v\rangle_h = 0 \textit{ for all } v \in \mathcal{C}\}.$$

If $\mathcal{C} \subseteq \mathcal{C}^{\perp_h}$, then $\mathcal{C}$ is called Hermitian self-orthogonal code. If $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$, then $\mathcal{C}$ is a Hermitian dual-containing code. From [4], [18], we can see that the Hermitian dual $\mathcal{C}^{\perp_h}$ of a λ-constacyclic code over F_{q^2} is a λ^{-q}-constacyclic code. If $\mathcal{C}$ is an $[n,k,d]$ constacyclic code over F_{q^2} with defining set Z, then the Hermitian dual $\mathcal{C}^{\perp_h}$ has a defining set $Z^{\perp_h}=\{z \in \mathcal{O}_{rn}| -qz \text{ mod } rn \notin Z\}$. Furthermore, the following result gives us a sufficient and necessary condition for a constacyclic code to be a Hermitian dual-containing code.

Lemma 1 ([4], [18]): Let $\mathcal{C}$ be a q^2-ary λ-constacyclic code of length n with defining set Z. Then $\mathcal{C}$ contains its Hermitian dual code if and only if $Z \cap -qZ = \emptyset$, where $-qZ=\{-qz \text{ mod } rn \mid z \in Z\}$.

In the following of this section, we recall some results of entanglement-assisted quantum codes in [2], [6], [25], [27], [28].

Theorem 1 ([2], [6], [25], [27], [28]): If $\mathcal{C}=[n,k,d]_{q^2}$ is a classical code and H is its parity check matrix over F_{q^2}, then there exist entanglement-assisted codes with parameters

$$[[n, 2k-n+c, d; c]]_q,$$

where $c=rank(HH^\dagger)$ is the number of maximally entangled states required and $H^\dagger$ is the conjugate transpose matrix of H over F_{q^2}.

Proposition 3 ([2], [6], [25], [27], [28]): If $\mathcal{C}$ is an entanglement-assisted quantum code with parameters $[[n,k,d;c]]_q$, then $\mathcal{C}$ satisfies the entanglement-assisted Singleton bound $n+c-k \leq 2(d-1)$. If $\mathcal{C}$ satisfies the equality

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

then it is called an entanglement-assisted quantum MDS code.

III. CONSTRUCTIONS OF ENTANGLEMENT-ASSISTED QUANTUM MDS CODES

In [25], [28], the authors proposed the definition for the decomposition of the defining set of constacyclic codes that containing cyclic codes and negacyclic codes.

Definition 1 ([25], [28]): Let $\mathcal{C}$ be q^2-ary λ-constacyclic code of length n with defining set Z. Assume that $Z_1=Z \cap (-qZ)$ and $Z_2=Z \setminus Z_1$, where $-qZ=\{rn-qx|x \in Z\}$. Then $Z=Z_1 \cup Z_2$ is called a decomposition of the defining set of $\mathcal{C}$.

Lemma 2 ([25], [28]): Let Z be a defining set of q^2-ary λ-constacyclic code $\mathcal{C}$ with length n, where $gcd(n,q)=1$. Suppose that $Z = Z_1 \cup Z_2$ is a decomposition of Z. Then the number of entangled states required is $c = |Z_1|$.

Similar to Lemma 3.1 in [26], we can obtain Lemma 3 as follows.

Lemma 3: Let $n = \frac{q^2+1}{\gamma}$ and $s = \frac{(q+\gamma+1)n}{2}$, where $\gamma = t^2+1$, t is a power of 2 and $q = t^e > 4$ with $e \equiv 1 \bmod 4$ or $e \equiv 3 \bmod 4$. Then $C_s = \{s\}$, and $C_{s-(q+1)i} = \{s-(q+1)i, s+(q+1)i\}$ for $1 \le i \le \frac{n-1}{2}$.

Theorem 2: Let $n = \frac{q^2+1}{\gamma}$ and $s = \frac{(q+\gamma+1)n}{2}$, where $\gamma = t^2+1$, t is a power of 2 and $q = t^e > 4$ with $e \equiv 1 \bmod 4$. If $\mathcal{C}$ is a q^2-ary λ-constacyclic code whose defining set is given by $Z = \cup_{i=1}^{\delta} C_{s-(q+1)i}$, where $1 \le \delta \le \frac{tq-t^2}{\gamma}$, then $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$.

Proof: We only need to consider that $Z \cap -qZ = \emptyset$ from Lemma 1. If $Z \cap -qZ \ne \emptyset$, then there exist two integers i and j, where $1 \le i,j \le \frac{tq-t^2}{\gamma}$, such that $s-(q+1)i \equiv -q(s-(q+1)j)q^{2k} \bmod (q+1)n$ for $k \in \{0,1\}$. We can seek some contradictions as follows.

(1) If $k=0$, then $s-(q+1)i \equiv -q(s-(q+1)j) \bmod (q+1)n$, which is equivalent to $0 \equiv qj+i \bmod n$. For $1 \le i,j \le \frac{tq-t^2}{\gamma}$, we consider the following cases.

(i) When $1 \le j \le \frac{q-t}{\gamma}$, we have

$$\begin{aligned} q+1 &\le qj+i \\ &\le q\frac{q-t}{\gamma} + \frac{tq-t^2}{\gamma} \\ &= \frac{q^2-t^2}{\gamma} \\ &< n = \frac{q^2+1}{\gamma}. \end{aligned}$$

It is in contradiction with the congruence $0 \equiv qj+i \bmod n$.

(ii) When $\frac{q+\gamma-t}{\gamma} \le j \le \frac{2q-2t}{\gamma}$, let $j' = j - \frac{q-t}{\gamma}$ for $1 \le j' \le \frac{q-t}{\gamma}$. Then we have $0 \equiv q(j' + \frac{q-t}{\gamma}) + i \bmod n$, which is equivalent to $0 \equiv qj' - \frac{tq+1}{\gamma} + i \bmod n$. Moreover,

$$\begin{aligned} 0 &< \frac{(\gamma-t)q+\gamma-1}{\gamma} \\ &= q+1-\frac{tq+1}{\gamma} \\ &\le qj' - \frac{tq+1}{\gamma} + i \\ &\le \frac{q^2-tq-\gamma}{\gamma} < n. \end{aligned}$$

It is in contradiction with the congruence $0 \equiv qj' - \frac{tq+1}{\gamma} + i \bmod n$.

(iii) When $\frac{(\vartheta-1)q+\gamma-(\vartheta-1)t}{\gamma} \le j \le \frac{\vartheta q-\vartheta t}{\gamma}$, where $3 \le \vartheta \le t$ (here, if there exists $t \ge 4$), let $j' = j - \frac{(\vartheta-1)q-(\vartheta-1)t}{\gamma}$ for $1 \le j' \le \frac{q-t}{\gamma}$. Then we have $0 \equiv q(j' + \frac{(\vartheta-1)q-(\vartheta-1)t}{\gamma}) + i \bmod n$, which is equivalent to $0 \equiv qj' - \frac{(\vartheta-1)tq+(\vartheta-1)}{\gamma} + i \bmod n$. Moreover,

$$\begin{aligned} 0 &< \frac{(1+t)q+\gamma-(t-1)}{\gamma} \\ &\le \frac{(\gamma-(\vartheta-1)t)q+\gamma-(\vartheta-1)}{\gamma} \\ &\le qj' - \frac{(\vartheta-1)tq+(\vartheta-1)}{\gamma} + i \\ &\le \frac{q^2-(\vartheta-1)tq-\gamma-\vartheta+2}{\gamma} \\ &\le \frac{q^2-2tq-\gamma-1}{\gamma} < n. \end{aligned}$$

It is in contradiction with the congruence $0 \equiv qj' - \frac{(\vartheta-1)tq+(\vartheta-1)}{\gamma} + i \bmod n$.

(2) If $k=1$, then $s-(q+1)i \equiv -q(s-(q+1)j)q^2 \bmod (q+1)n$, which is equivalent to $qj \equiv i \bmod n$. From $1 \le i,j \le \frac{tq-t^2}{\gamma}$, we consider the following cases.

(i) When $1 \le j \le \frac{q-t}{\gamma}$, we have

$$\begin{aligned} 0 &< \frac{(\gamma-t)q+t^2}{\gamma} \\ &= q - \frac{tq-t^2}{\gamma} \\ &\le \text{qj-i} \\ &\le \frac{q^2-tq-\gamma}{\gamma} < n. \end{aligned}$$

It is in contradiction with $0 \equiv qj-i \bmod n$.

(ii) When $\frac{q+\gamma-t}{\gamma} \le j \le \frac{2q-2t}{\gamma}$, let $j' = j - \frac{q-t}{\gamma}$ for $1 \le j' \le \frac{q-t}{\gamma}$. Then we have $i \equiv q(j' + \frac{q-t}{\gamma}) \bmod n$, which is equivalent to $i \equiv qj' - \frac{tq+1}{\gamma} \bmod n$. Moreover,

$$\begin{aligned} 0 &< \frac{(\gamma-t)q-1}{\gamma} \\ &= q - \frac{tq+1}{\gamma} \\ &\le qj' - \frac{tq+1}{\gamma} \\ &\le \frac{q^2-2tq-1}{\gamma} < n. \end{aligned}$$

It is in contradiction with $1 \le i \le \frac{tq-t^2}{\gamma}$.

(iii) When $\frac{(\vartheta-1)q+\gamma-(\vartheta-1)t}{\gamma} \le j \le \frac{\vartheta q-\vartheta t}{\gamma}$, where $3 \le \vartheta \le t$ (here, if there exists $t \ge 4$), let $j' = j - \frac{(\vartheta-1)q-(\vartheta-1)t}{\gamma}$ for $1 \le j' \le \frac{q-t}{\gamma}$. Then we have $i \equiv q(j' + \frac{(\vartheta-1)q-(\vartheta-1)t}{\gamma}) \bmod n$, which is equivalent to $i \equiv qj' - \frac{(\vartheta-1)tq+(\vartheta-1)}{\gamma} \bmod n$. Moreover,

$$\begin{aligned} 0 &< \frac{(t+1)q-t+1}{\gamma} \\ &\le \frac{(\gamma-(\vartheta-1)t)q-(\vartheta-1)}{\gamma} \end{aligned}$$

$$\leq qj' - \frac{(\vartheta-1)tq+(\vartheta-1)}{\gamma}$$
$$\leq \frac{q^2-\vartheta tq-\vartheta+1}{\gamma}$$
$$\leq \frac{q^2-3\,tq-2}{\gamma} < n.$$

It is in contradiction with $i \equiv qj' - \frac{(\vartheta-1)tq+(\vartheta-1)}{\gamma} \bmod n$.

From the above discussion, the result follows. □

Theorem 3: Let $n = \frac{q^2+1}{\gamma}$ and $s = \frac{(q+\gamma+1)n}{2}$, where $\gamma = t^2+1$, t is a power of 2 and $q = t^e > 4$ with $e \equiv 1 \bmod 4$. If $\mathcal{C}$ is a q^2-ary λ-constacyclic code of length n with defining set $Z = \cup_{i=0}^{\delta} C_{s-(q+1)i}$ for $0 \leq \delta \leq \frac{tq-t^2}{\gamma}$, then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma}-2d+3, d; 1]]_q$, where $2 \leq d \leq \frac{2tq+2}{\gamma}$ is even.

Proof: From Lemma 3, we can assume that the defining set of constacyclic code $\mathcal{C}$ is given by $Z = \cup_{i=0}^{\delta} C_{s-(q+1)i}$ for $0 \leq \delta \leq \frac{tq-t^2}{\gamma}$, and then $\mathcal{C}$ is a constacyclic code with parameters $[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma}-2\delta-1, 2\delta+2]_{q^2}$ from Propositions 1 and 2. If $\delta = 0$, then $-qZ \cap Z = -qC_s \cap C_s = C_s$. From Lemma 2, we have $c = 1$. Then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma}-2d+3, d; 1]]_q$ from Theorem 1 and Proposition 3, where $d = 2$. As for $1 \leq \delta \leq \frac{tq-t^2}{\gamma}$, we assume that the defining set of $\mathcal{C}$ can be divided into two mutually disjoint subsets, i.e., $Z = Z_0 \cup Z_1$, where $Z_0 = C_s$ and $Z_1 = \cup_{i=1}^{\delta} C_{s-(q+1)i}$ and the defining sets Z_0 and Z_1 can generate constacyclic codes $\mathcal{C}_0$ and $\mathcal{C}_1$ respectively. Let the parity check matrices of $\mathcal{C}$, $\mathcal{C}_0$ and $\mathcal{C}_1$ over F_{q^2} be H, H_0 and H_1, respectively. Therefore,

$$H = \begin{pmatrix} H_0 \\ H_1 \end{pmatrix},$$

and

$$HH^\dagger = \begin{pmatrix} H_0H_0^\dagger & H_0H_1^\dagger \\ H_1H_0^\dagger & H_1H_1^\dagger \end{pmatrix}.$$

From Theorem 2, we have $H_1H_1^\dagger = 0$. Moreover, we have $H_0H_1^\dagger = 0$, and $H_1H_0^\dagger = 0$ from

$$C_s \cap -q(\cup_{i=1}^{\delta} C_{s-(q+1)i}) = -q(C_s \cap (\cup_{i=1}^{\delta} C_{s-(q+1)i})) = \emptyset.$$

Hence, we obtain that

$$HH^\dagger = \begin{pmatrix} H_0H_0^\dagger & 0 \\ 0 & 0 \end{pmatrix}.$$

It is easy to see that $Z_0 \cap -qZ_0 = \{s\}$, and then $rank(H_0H_0^\dagger) = 1$. From Lemma 2, $c = 1$. Therefore, there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma}-2d+3, d; 1]]_q$ from Theorem 1 and Proposition 3. □

Example 1: If $t = 4$ and $e = 5$, then $q = 1024$ and $n = 61681$. Therefore, there exist entanglement-assisted quantum MDS codes from Theorem 3 that are listed in Table 1.

TABLE 1. Sample parameters of entanglement-assisted quantum MDS codes constructed from Theorem 3.

q	n	$[[n,k,d;c]]_q$
1024	61681	$[[61681, 61680, 2; 1]]_{1024}$
1024	61681	$[[61681, 61676, 4; 1]]_{1024}$
1024	61681	$[[61681, 61672, 6; 1]]_{1024}$
1024	61681	$[[61681, 61668, 8; 1]]_{1024}$
1024	61681	$[[61681, 61664, 10; 1]]_{1024}$
1024	61681	$[[61681, 61660, 12; 1]]_{1024}$
1024	61681	$[[61681, 61656, 14; 1]]_{1024}$
1024	61681	$[[61681, 61652, 16; 1]]_{1024}$
…	…	…
1024	61681	$[[61681, 60744, 470; 1]]_{1024}$
1024	61681	$[[61681, 60740, 472; 1]]_{1024}$
1024	61681	$[[61681, 60736, 474; 1]]_{1024}$
1024	61681	$[[61681, 60732, 476; 1]]_{1024}$
1024	61681	$[[61681, 60728, 478; 1]]_{1024}$
1024	61681	$[[61681, 60724, 480; 1]]_{1024}$
1024	61681	$[[61681, 60720, 482; 1]]_{1024}$

Lemma 4: Let $n = \frac{q^2+1}{\gamma}$, where $\gamma = t^2+1$, t is a power of 2 and $q = t^e > 4$ with $e \equiv 1 \bmod 4$ or $e \equiv 3 (\bmod 4)$. Assume that $s = \frac{(q+\gamma+1)n}{2}$ and $\beta = \frac{q^2+q}{2}+1$, where $\beta = s - \frac{(q+1)(n-1)}{2}$. Then $C_s = \{s\}$, and $C_{\beta+(q+1)i} = \{\beta+(q+1)i, \beta-(q+1)(i+1)\}$ for $0 \leq i \leq \frac{n-3}{2}$.

Proof: If $j = \frac{q^2+\gamma q-\gamma+1}{2\gamma}$, then $1+(q+1)j = s$. This implies that s must be in $\mathcal{O}_{rn}$ (see Sec.2). Since $sq^2 = s(q^2+1-1) \equiv s \bmod (q+1)n$, it follows that $C_s = \{s\}$. For $0 \leq i \leq \frac{n-3}{2}$, we have $C_{\beta+(q+1)i} = \{\beta+(q+1)i, \beta-(q+1)(i+1)\}$ from

$$\begin{aligned}
&(\beta+(q+1)i)q^2 \\
&\quad= [s-\frac{(q+1)(n-1)}{2}+(q+1)i]q^2 \\
&\quad\equiv s-(q+1)(\frac{n-1}{2}-i)q^2 \\
&\quad\equiv s-(q+1)[\frac{n-1}{2}(q^2+1)-\frac{n-1}{2}-i(q^2+1)+i] \\
&\quad\equiv s+(q+1)(\frac{n-1}{2}-i) \\
&\quad\equiv \beta-(q+1)(i+1) \bmod (q+1)n
\end{aligned}$$

and

$$\begin{aligned}
&(\beta-(q+1)(i+1))q^2 \\
&\quad= [s-\frac{(q+1)(n-1)}{2}-(q+1)(i+1)]q^2 \\
&\quad\equiv s-(q+1)(\frac{n-1}{2}+i+1)q^2 \\
&\quad\equiv s-(q+1)[\frac{n-1}{2}(q^2+1)-\frac{n-1}{2} \\
&\qquad+(i+1)(q^2+1)-i-1] \\
&\quad\equiv s+(q+1)(\frac{n-1}{2}+i+1) \\
&\quad\equiv \beta+(q+1)i \bmod (q+1)n.
\end{aligned}$$

Moreover, we show that $C_{\beta+(q+1)i} = \{\beta+(q+1)i, \beta-(q+1)(i+1)\}$ is disjoint for $0 \leq i \leq \frac{n-3}{2}$. In fact, we assume that there exist two integers i and j, $0 \leq i \neq j \leq \frac{n-3}{2}$ such that

$C_{\beta+(q+1)i} = C_{\beta+(q+1)j}$, and then we have $\beta + (q+1)i \equiv (\beta + (q+1)j)q^{2k} \bmod (q+1)n$ for $k \in \{0, 1\}$.

If $k = 0$, we have $\beta+(q+1)i \equiv \beta+(q+1)j \bmod (q+1)n$, which is equivalent to $i = j$. It is in contradiction with $0 \le i \neq j \le \frac{n-3}{2}$.

If $k = 1$, we have $\beta+(q+1)i \equiv \beta-(q+1)(j+1) \bmod (q+1)n$, which is equivalent to $i + j \equiv n - 1 \bmod n$. It is in contradiction with $0 \le i + j \le n - 3$. Therefore, the result follows. $\square$

Theorem 4: Let $n = \frac{q^2+1}{\gamma}$, where $\gamma = t^2 + 1$, t is a power of 2 and $q = t^e > 4$ with $e \equiv 1 \bmod 4$. Assume that $s = \frac{(q+\gamma+1)n}{2}$ and $\beta = \frac{q^2+q}{2} + 1$, where $\beta = s - \frac{(q+1)(n-1)}{2}$. If $\mathcal{C}$ is a q^2-ary λ-constacyclic code whose defining set is given by $Z = \cup_{i=0}^{\delta} C_{\beta+(q+1)i}$, where $0 \le \delta \le \frac{(t+1)q-3\gamma-t+1}{2\gamma}$, then $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$.

Proof: We only need to consider that $Z \cap -qZ = \emptyset$ from Lemma 1. If $Z \cap -qZ \neq \emptyset$, then there exist two integers i and j, where $1 \le i, j \le \frac{(t+1)q-3\gamma-t+1}{2\gamma}$, such that

$$\beta + (q+1)i \equiv -q(\beta + (q+1)j)q^{2k} \bmod (q+1)n$$

for $k \in \{0, 1\}$. We can seek some contradictions as follows.

(1) If $k = 0$, then $\beta+(q+1)i \equiv -q(\beta+(q+1)j) \bmod (q+1)n$, which is equivalent to $qj + i \equiv \frac{n-q-1}{2} \bmod n$. For $0 \le i, j \le \frac{(t+1)q-3\gamma-t+1}{2\gamma}$, we can consider the following cases.

(i) When $0 \le j \le \frac{q-2\gamma-t}{2\gamma}$, we have

$$\begin{aligned} 0 &\le qj+i \\ &\le q\frac{q-2\gamma-t}{2\gamma} + \frac{(t+1)q-3\gamma-t+1}{2\gamma} \\ &= \frac{q^2-(2\gamma-1)q-3\gamma-t+1}{2\gamma} \\ &< \frac{q^2+1-\gamma q-\gamma}{2\gamma} \\ &= \frac{n-q-1}{2}. \end{aligned}$$

It is in contradiction with the congruence $qj + i \equiv \frac{n-q-1}{2} \bmod n$.

(ii) When $\frac{q-t}{2\gamma} \le j \le \frac{2q-2\gamma-2t}{2\gamma}$, let $j' = j - \frac{q-2\gamma-t}{2\gamma}$ with $1 \le j' \le \frac{q-t}{2\gamma}$. Then we have $\frac{q^2+1-\gamma q-\gamma}{2\gamma} \equiv q(j' + \frac{q-2\gamma-t}{2\gamma}) + i \bmod n$, which is equivalent to $0 \equiv qj' + \frac{-q\gamma-tq+\gamma-1}{2\gamma} + i \bmod n$. Moreover,

$$\begin{aligned} 0 &< \frac{q(\gamma-t)+\gamma-1}{2\gamma} \\ &\le qj' + \frac{-q\gamma-tq+\gamma-1}{2\gamma} + i \\ &\le q\frac{q-t}{2\gamma} + \frac{-q\gamma-tq+\gamma-1}{2\gamma} + \frac{(t+1)q-3\gamma-t+1}{2\gamma} \\ &= \frac{q^2-(\gamma+t-1)q-2\gamma-t}{2\gamma} < n. \end{aligned}$$

It is in contradiction with the congruence $0 \equiv qj' + \frac{-q\gamma-tq+\gamma-1}{2\gamma} + i \bmod n$.

(iii) When $\frac{(\vartheta-1)q-(\vartheta-1)t}{\gamma} \le j \le \frac{\vartheta q-\vartheta t-2\gamma}{2\gamma}$, where $3 \le \vartheta \le t$ (if there exists $t \ge 4$), let $j' = j - \frac{(\vartheta-1)q-(\vartheta-1)t-2\gamma}{2\gamma}$ with $1 \le j' \le \frac{q-t}{2\gamma}$. Then we have $\frac{q^2+1-\gamma q-\gamma}{2\gamma} \equiv q(j' + \frac{(\vartheta-1)q-2\gamma-(\vartheta-1)t}{2\gamma}) + i \bmod n$, which is equivalent to $0 \equiv qj' + \frac{(\vartheta-2)q^2-\gamma q-(\vartheta-1)qt+\gamma-1}{2\gamma} + i \bmod n$.

If ϑ is an even, then we have $0 \equiv qj' + \frac{-\vartheta-\gamma q-(\vartheta-1)qt+\gamma+1}{2\gamma} + i \bmod n$. Moreover,

$$\begin{aligned} 0 &< \frac{(1+t)q-t+\gamma+1}{2\gamma} \\ &\le q + \frac{-\vartheta-\gamma q-(\vartheta-1)qt+\gamma+1}{2\gamma} \\ &\le qj' + \frac{-\vartheta-\gamma q-(\vartheta-1)qt+\gamma+1}{2\gamma} + i \\ &\le q\frac{q-t}{2\gamma} + \frac{-\vartheta-\gamma q-(\vartheta-1)qt+\gamma+1}{2\gamma} \\ &\quad + \frac{(t+1)q-3\gamma-t+1}{2\gamma} \\ &\le \frac{q^2-(\gamma+3t-1)q-2\gamma-t-2}{2\gamma} < n. \end{aligned}$$

It is in contradiction with the congruence $0 \equiv qj' + \frac{-\vartheta-\gamma q-(\vartheta-1)qt+\gamma+1}{2\gamma} + i \bmod n$.

If ϑ is an odd, then we have $\frac{q^2+\gamma q+(\vartheta-1)tq-\gamma+\vartheta}{2\gamma} \equiv qj' + i \bmod n$. Moreover,

$$\begin{aligned} 0 &< q \\ &\le qj' + i \\ &\le q\frac{q-t}{2\gamma} + \frac{(t+1)q-3\gamma-t+1}{2\gamma} \\ &\le \frac{q^2+q-3\gamma-t+1}{2\gamma} < n. \end{aligned}$$

It is in contradiction with $0 < \frac{q^2+\gamma q+2tq-\gamma+3}{2\gamma} \le \frac{q^2+\gamma q+(\vartheta-1)tq-\gamma+\vartheta}{2\gamma} \le \frac{q^2+\gamma q+(t-2)tq-\gamma+t-1}{2\gamma} < n$.

(v) When $\frac{tq-t^2}{2\gamma} \le j \le \frac{(t+1)q-3\gamma-t+1}{2\gamma}$, let $j' = j - \frac{tq-t^2-2\gamma}{2\gamma}$ with $1 \le j' \le \frac{q-t}{2\gamma}$. Then we have $\frac{q^2+1-\gamma q-\gamma}{2\gamma} \equiv q(j' + \frac{tq-t^2-2\gamma}{2\gamma}) + i \bmod n$, which is equivalent to $\frac{q^2+(2\gamma-1)q+t+1-\gamma}{2\gamma} \equiv qj' + i \bmod n$. Moreover,

$$\begin{aligned} 0 &< q \\ &\le qj' + i \\ &\le q\frac{q-t}{2\gamma} + \frac{(t+1)q-3\gamma-t+1}{2\gamma} \\ &\le \frac{q^2+q-3\gamma-t+1}{2\gamma} < n. \end{aligned}$$

It is in contradiction with the congruence

$$\frac{q^2+(2\gamma-1)q+t+1-\gamma}{2\gamma} \equiv qj' + i \bmod n.$$

(2) If $k = 1$, then

$$\beta + (q+1)i \equiv -q(\beta - (q+1)(j+1)) \bmod (q+1)n,$$

which is equivalent to $i \equiv qj + \frac{n+q-1}{2} \bmod n$. From $0 \le i, j \le \frac{(t+1)q-3\gamma-t+1}{2\gamma}$, we can consider the following cases.

(i) When $0 \le j \le \frac{q-2\gamma-t}{2\gamma}$, we have

$$\begin{aligned}0 &< \frac{q^2+\gamma q+1-\gamma}{2\gamma}\\ &\le qj + \frac{q^2+\gamma q+1-\gamma}{2\gamma}\\ &\le q\frac{q-2\gamma-t}{2\gamma} + \frac{q^2+\gamma q+1-\gamma}{2\gamma}\\ &= \frac{2q^2-(\gamma+t)q+1-\gamma}{2\gamma} < n.\end{aligned}$$

It is in contradiction with $0 \le i \le \frac{(t+1)q-3\gamma-t+1}{2\gamma}$.

(ii) When $\frac{q-t}{2\gamma} \le j \le \frac{2q-2\gamma-2t}{2\gamma}$, let $j' = j - \frac{q-2\gamma-t}{2\gamma}$ with $1 \le j' \le \frac{q-t}{2\gamma}$. Then we have $i \equiv q(j' + \frac{q-2\gamma-t}{2\gamma}) + \frac{q^2+\gamma q+1-\gamma}{2\gamma} \bmod n$, which is equivalent to $i \equiv qj' + \frac{-(\gamma+t)q-\gamma-1}{2\gamma} \bmod n$. Moreover,

$$\begin{aligned}0 &< \frac{(\gamma-t)q-\gamma-1}{2\gamma}\\ &\le q + \frac{-(\gamma+t)q-\gamma-1}{2\gamma}\\ &\le qj' + \frac{-(\gamma+t)q-\gamma-1}{2\gamma}\\ &\le q\frac{q-t}{2\gamma} + \frac{-q\gamma-tq-\gamma-1}{2\gamma}\\ &\quad + \frac{(t+1)q-3\gamma-t+1}{2\gamma}\\ &= \frac{q^2-(\gamma+t-1)q-4\gamma-t}{2\gamma} < n.\end{aligned}$$

It is in contradiction with $0 \le i \le \frac{(t+1)q-3\gamma-t+1}{2\gamma}$.

(iii) When $\frac{(\vartheta-1)q-(\vartheta-1)t}{\gamma} \le j \le \frac{\vartheta q-\vartheta t-2\gamma}{2\gamma}$, where $3 \le \vartheta \le t$ (if there exists $t \ge 4$), let $j' = j - \frac{(\vartheta-1)q-(\vartheta-1)t-2\gamma}{2\gamma}$ with $1 \le j' \le \frac{q-t}{2\gamma}$. Then we have $i \equiv q(j' + \frac{(\vartheta-1)q-2\gamma-(\vartheta-1)t}{2\gamma}) + \frac{q^2+\gamma q+1-\gamma}{2\gamma} \bmod n$, which is equivalent to $i \equiv qj' + \frac{\vartheta q^2-\gamma q-(\vartheta-1)qt-\gamma+1}{2\gamma} \bmod n$.

If ϑ is an even, then we have $i \equiv qj' + \frac{-(\gamma+(\vartheta-1)t)q-\gamma-\vartheta+1}{2\gamma} \bmod n$. Moreover, we have

$$\begin{aligned}0 &< \frac{(t+1)q-\gamma-t+1}{2\gamma}\\ &\le \frac{(\gamma-(\vartheta-1)t)q-\gamma-\vartheta+1}{2\gamma}\\ &\le q + \frac{-(\gamma+(\vartheta-1)t)q-\gamma-\vartheta+1}{2\gamma}\\ &\le qj' + \frac{-(\gamma+(\vartheta-1)t)q-\gamma-\vartheta+1}{2\gamma}\\ &\le q\frac{q-t}{2\gamma} + \frac{(\gamma-(\vartheta-1)t)q-\gamma-\vartheta+1}{2\gamma}\\ &= \frac{q^2+(\gamma-\vartheta t)q-\gamma-\vartheta+1}{2\gamma}\\ &\le \frac{q^2+(\gamma-4t)q-\gamma-3}{2\gamma} < n.\end{aligned}$$

It is in contradiction with $0 \le i \le \frac{(t+1)q-3\gamma-t+1}{2\gamma}$.

If ϑ is an odd, then we have $i + \frac{q^2+(\gamma+(\vartheta-1)t)q+\gamma+\vartheta}{2\gamma} \equiv qj' \bmod n$. Moreover,

$$\begin{aligned}0 &< \frac{q^2+(\gamma+2t)q+\gamma+3}{2\gamma}\\ &\le i + \frac{q^2+(\gamma+(\vartheta-1)t)q+\gamma+\vartheta}{2\gamma}\\ &\le \frac{(t+1)q-3\gamma-t+1}{2\gamma}\\ &\quad + \frac{q^2+(\gamma+(\vartheta-1)t)q+\gamma+\vartheta}{2\gamma}\\ &\le \frac{q^2+(2\gamma-t)q-2\gamma}{2\gamma} < n.\end{aligned}$$

It is in contradiction with $q \le qj' \le \frac{q^2-tq}{2\gamma}$.

(v) When $\frac{tq-t^2}{2\gamma} \le j \le \frac{(t+1)q-3\gamma-t+1}{2\gamma}$, let $j' = j - \frac{tq-t^2-2\gamma}{2\gamma}$ with $1 \le j' \le \frac{q-t}{2\gamma}$. Then we have $i \equiv q(j' + \frac{tq-t^2-2\gamma}{2\gamma}) + \frac{q^2+\gamma q+1-\gamma}{2\gamma} \bmod n$, which is equivalent to $i \equiv qj' + \frac{q^2-(2\gamma-1)q-\gamma-t+1}{2\gamma} \bmod n$. Moreover,

$$\begin{aligned}0 &< \frac{q^2+q-\gamma-t+1}{2\gamma}\\ &\le q + \frac{q^2-(2\gamma-1)q-\gamma-t+1}{2\gamma}\\ &\le qj' + \frac{q^2-(2\gamma-1)q-\gamma-t+1}{2\gamma}\\ &\le q\frac{q-t}{2\gamma} + \frac{q^2-(2\gamma-1)q-\gamma-t+1}{2\gamma}\\ &\le \frac{2q^2-(2\gamma+t-1)q-\gamma-t+1}{2\gamma} < n.\end{aligned}$$

It is in contradiction with $0 \le i \le \frac{(t+1)q-3\gamma-t+1}{2\gamma}$.

From the above discussions of (1) and (2), the result follows. □

Theorem 5: Let $n = \frac{q^2+1}{\gamma}$, where $\gamma = t^2+1$, t is a power of 2 and $q = t^e > 4$ with $e \equiv 1 \bmod 4$. Assume that $s = \frac{(q+\gamma+1)n}{2}$ and $\beta = \frac{q^2+q}{2} + 1$, where $\beta = s - \frac{(q+1)(n-1)}{2}$. If $\mathcal{C}$ is a q^2-ary λ-constacyclic of length n with defining set $Z = \cup_{i=0}^{\frac{(t+1)q-3\gamma-t+1}{2\gamma}+\zeta} C_{\beta+(q+1)i}$ for $1 \le \zeta \le \frac{(2t-2)q+2t+2}{2\gamma}$, then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma} - 2d + 6, d; 4]]_q$, where $\frac{(t+1)q-t+1+2\gamma}{\gamma} \le d \le \frac{(3t-1)q+t+3}{\gamma}$ is odd.

Proof: From Lemma 4, we can assume that the defining set of constacyclic code $\mathcal{C}$ is given by $Z = \cup_{i=0}^{\frac{(t+1)q-3\gamma-t+1}{2\gamma}+\zeta} C_{\beta+(q+1)i}$ for $1 \le \zeta \le \frac{(2t-2)q+2t+2}{2\gamma}$, and then

$\mathcal{C}$ is a constacyclic code with parameters $[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma} - \frac{(t+1)q-\gamma-t+1}{\gamma} - 2\zeta, \frac{(t+1)q-t+1}{\gamma} + 2\zeta]_{q^2}$ from Propositions 1 and 2. If $\zeta = 1$, then $Z = \cup_{i=0}^{\frac{(t+1)q-\gamma-t+1}{2\gamma}} C_{\beta+(q+1)i}$. Since $-qC_{\beta+(q+1)\frac{(t+1)q-\gamma-t+1}{2\gamma}} = C_{\beta+(q+1)(\frac{(t-1)(q+1)+2-\gamma}{2\gamma})}$, it follows that

$$\begin{aligned}
&Z \cap -qZ \\
&= (\cup_{i=0}^{\frac{(t+1)q-3\gamma-t+1}{2\gamma}} C_{\beta+(q+1)i} \cup C_{\beta+(q+1)\frac{(t+1)q-\gamma-t+1}{2\gamma}}) \\
&\quad \cap -q(\cup_{i=0}^{\frac{(t+1)q-3\gamma-t+1}{2\gamma}} C_{\beta+(q+1)i} \cup C_{\beta+(q+1)\frac{(t+1)q-\gamma-t+1}{2\gamma}}) \\
&= (\cup_{i=0}^{\frac{(t+1)q-3\gamma-t+1}{2\gamma}} C_{\beta+(q+1)i} \\
&\quad \cap(-q\cup_{i=0}^{\frac{(t+1)q-3\gamma-t+1}{2\gamma}} C_{\beta+(q+1)i})) \\
&\quad \cup(\cup_{i=0}^{\frac{(t+1)q-3\gamma-t+1}{2\gamma}} C_{\beta+(q+1)i} \cap(-qC_{\beta+(q+1)\frac{(t+1)q-\gamma-t+1}{2\gamma}})) \\
&\quad \cup(C_{\beta+(q+1)\frac{(t+1)q-\gamma-t+1}{2\gamma}} \cap(-q\cup_{i=0}^{\frac{(t+1)q-3\gamma-t+1}{2\gamma}} C_{\beta+(q+1)i})) \\
&\quad \cup(-qC_{\beta+(q+1)\frac{(t+1)q-\gamma-t+1}{2\gamma}} \cap C_{\beta+(q+1)\frac{(t+1)q-\gamma-t+1}{2\gamma}}) \\
&= C_{\beta+(q+1)\frac{(t+1)q-\gamma-t+1}{2\gamma}} \cup C_{\beta+(q+1)(\frac{(t-1)(q+1)+2-\gamma}{2\gamma})}.
\end{aligned}$$

From Lemma 2, we have $c = 4$. Therefore, there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma} - 2d + 6, d; 4]]_q$ from Theorem 1 and Proposition 3, where $d = \frac{(t+1)q-t+1+2\gamma}{\gamma}$. If $2 \le \zeta \le \frac{(2t-2)q+2t+2}{2\gamma}$, then the defining set of $\mathcal{C}$ can be divided into three mutually disjoint subsets, i.e., $Z = Z_0 \cup Z_1 \cup Z_2$, where $Z_0 = \cup_{i=0}^{\frac{(t+1)q-3\gamma-t+1}{2\gamma}} C_{\beta+(q+1)i}$, $Z_1 = C_{\beta+(q+1)(\frac{(t+1)q-\gamma-t+1}{2\gamma})}$ and $Z_2 = \cup_{i=\frac{(t+1)q+\gamma-t+1}{2\gamma}}^{\frac{(t+1)q-3\gamma-t+1}{2\gamma}+\zeta} C_{\beta+(q+1)i}$. The defining sets Z_0, Z_1, Z_2 can generate constacyclic codes $\mathcal{C}_0$, $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively. Let the parity check matrices of $\mathcal{C}$, $\mathcal{C}_0$, $\mathcal{C}_1$ and $\mathcal{C}_2$ over F_{q^2} be H, H_0, H_1 and H_2, respectively. Therefore,

$$H = \begin{pmatrix} H_0 \\ H_1 \\ H_2 \end{pmatrix},$$

and

$$HH^\dagger = \begin{pmatrix} H_0H_0^\dagger & H_0H_1^\dagger & H_0H_2^\dagger \\ H_1H_0^\dagger & H_1H_1^\dagger & H_1H_2^\dagger \\ H_2H_0^\dagger & H_2H_1^\dagger & H_2H_2^\dagger \end{pmatrix}.$$

From the proof of Theorem 4, we have $H_0H_0^\dagger = 0$, and then

$$HH^\dagger = \begin{pmatrix} 0 & H_0H_1^\dagger & H_0H_2^\dagger \\ H_1H_0^\dagger & H_1H_1^\dagger & H_1H_2^\dagger \\ H_2H_0^\dagger & H_2H_1^\dagger & H_2H_2^\dagger \end{pmatrix}.$$

Since $-qC_{\beta+(q+1)\frac{(t+1)q-\gamma-t+1}{2\gamma}} = C_{\beta+(q+1)(\frac{(t-1)(q+1)+2-\gamma}{2\gamma})}$, then $rank(H_1H_0^\dagger) = rank(H_0H_1^\dagger) = 2$ and

$$HH^\dagger = \begin{pmatrix} 0 & H_0H_1^\dagger & H_0H_2^\dagger \\ H_1H_0^\dagger & 0 & 0 \\ H_2H_0^\dagger & 0 & H_2H_2^\dagger \end{pmatrix}.$$

In order to obtain

$$HH^\dagger = \begin{pmatrix} 0 & H_0H_1^\dagger & 0 \\ H_1H_0^\dagger & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

we only need to show that $H_0H_2^\dagger = 0$ and $H_2H_2^\dagger = 0$. we disucss two cases as follows.

(1) We have $H_2H_2^\dagger = 0$. In fact, from Lemma 1, it only need to consider that $Z_2 \cap -qZ_2 = \emptyset$. If $Z_2 \cap -qZ_2 \neq \emptyset$, where $Z_2 = \cup_{i=\frac{(t+1)q+\gamma-t+1}{2\gamma}}^{\frac{(t+1)q-3\gamma-t+1}{2\gamma}+\zeta} C_{\beta+(q+1)i}$ for $2 \le \zeta \le \frac{(2t-2)q+2t+2}{2\gamma}$, which is equivalent to $Z_2 = \cup_{i=1}^{\zeta} C_{\beta+(q+1)(\frac{(t+1)q-\gamma-t+1}{2\gamma}+i)}$ for $1 \le \zeta \le \frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$, then there exist two integers i and j, where $1 \le i, j \le \frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$, such that

$$\begin{aligned}
&\beta + (q+1)(\frac{(t+1)q-\gamma-t+1}{2\gamma} + i) \\
&\quad \equiv -q(\beta + (q+1)(\frac{(t+1)q-\gamma-t+1}{2\gamma} + j))q^{2k} \\
&\qquad \bmod (q+1)n
\end{aligned}$$

for $k \in \{0, 1\}$, where $1 \le i, j \le \frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$.

If $k = 0$, then we have $0 \equiv \frac{q-t}{\gamma} + qj + i \bmod n$, and then from $1 \le i, j \le \frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$, we can seek some contradictions by considering the following cases.

(i) When $1 \le j \le \frac{q-t}{2\gamma}$, we have

$$\begin{aligned}
0 &< q + 1 + \frac{q-t}{\gamma} \\
&\le qj + i + \frac{q-t}{\gamma} \\
&\le q\frac{q-t}{2\gamma} \\
&\quad + \frac{(2t-2)q+2t+2-2\gamma}{2\gamma} + \frac{q-t}{\gamma} \\
&= \frac{q^2+tq-2\gamma+2}{2\gamma} < n.
\end{aligned}$$

It is in contradiction with the congruence $0 \equiv \frac{q-t}{\gamma} + qj + i \bmod n$.

(ii) When $\frac{q-t+2\gamma}{2\gamma} \le j \le \frac{2q-2t}{2\gamma}$, let $j' = j - \frac{q-t}{2\gamma}$ for $1 \le j' \le \frac{q-t}{2\gamma}$. Then we have $0 \equiv \frac{q-t}{\gamma} + q(j' + \frac{q-t}{2\gamma}) + i \bmod n$, which is equivalent to $\frac{q^2+(t-2)q+2t+2}{2\gamma} \equiv qj' + i \bmod n$. Moreover, we have

$$\begin{aligned}
0 &< q + 1 \\
&\le qj' + i
\end{aligned}$$

$$\begin{aligned}&\leq q(\frac{q-t}{2\gamma})\\&\quad+\frac{(2t-2)q+2t+2-2\gamma}{2\gamma}\\&=\frac{q^2+(t-2)q+2t+2-2\gamma}{2\gamma}\\&<n,\end{aligned}$$

which is in contradiction with $\frac{q^2+(t-2)q+2t+2}{2\gamma}\equiv qj'+i \bmod n$.

(iii) When $\frac{(\vartheta-1)q-(\vartheta-1)t+2\gamma}{2\gamma}\leq j\leq\frac{\vartheta q-\vartheta t}{2\gamma}$, where $3\leq\vartheta\leq 2t-3$ (here, if there exists the case of $t\geq 4$). Let $j'=j-\frac{(\vartheta-1)q-(\vartheta-1)t}{2\gamma}$ for $1\leq j'\leq\frac{q-t}{2\gamma}$. Then we have $0\equiv\frac{q-t}{\gamma}+q(j'+\frac{(\vartheta-1)q-(\vartheta-1)t}{2\gamma})+i \bmod n$, which is equivalent to $0\equiv\frac{(\vartheta-1)q^2-((\vartheta-1)t-2)q-2t}{2\gamma}+qj'+i \bmod n$.

If ϑ is an odd, then we have $0\equiv\frac{-((\vartheta-1)t-2)q-\vartheta+1-2t}{2\gamma}+qj'+i \bmod n$. Moreover,

$$\begin{aligned}0&<\frac{(4t+4)q+2\gamma+4-4t}{2\gamma}\\&\leq\frac{(2\gamma-(\vartheta-1)t+2)q+2\gamma-\vartheta+1-2t}{2\gamma}\\&\leq q+1-\frac{((\vartheta-1)t-2)q+\vartheta-1+2t}{2\gamma}\\&\leq qj'+i-\frac{((\vartheta-1)t-2)q+\vartheta-1+2t}{2\gamma}\\&\leq q\frac{q-t}{2\gamma}+\frac{(2t-2)q+2t+2-2\gamma}{2\gamma}\\&\quad-\frac{((\vartheta-1)t-2)q+\vartheta-1+2t}{2\gamma}\\&\leq\frac{q^2-tq-2\gamma}{2\gamma}<n,\end{aligned}$$

which is in contradiction with $0\equiv\frac{-((\vartheta-1)t-2)q-\vartheta+1-2t}{2\gamma}+qj'+i \bmod n$.

If ϑ is an even, then we have $0\equiv\frac{q^2-((\vartheta-1)t-2)q-\vartheta+2-2t}{2\gamma}+qj'+i \bmod n$. Moreover,

$$\begin{aligned}0&<\frac{q^2+(5t+4)q+2\gamma+6-4t}{2\gamma}\\&\leq\frac{q^2+(2\gamma-(\vartheta-1)t+2)q+2\gamma-\vartheta+2-2t}{2\gamma}\\&\leq q+1+\frac{q^2-((\vartheta-1)t-2)q-\vartheta+2-2t}{2\gamma}\\&\leq qj'+i+\frac{q^2-((\vartheta-1)t-2)q-\vartheta+2-2t}{2\gamma}\\&\leq q\frac{q-t}{2\gamma}+\frac{(2t-2)q+2t+2-2\gamma}{2\gamma}\\&\quad+\frac{q^2-((\vartheta-1)t-2)q-\vartheta+2-2t}{2\gamma}\\&\leq\frac{2q^2-2tq-2\gamma}{2\gamma}<n,\end{aligned}$$

which is in contradiction with $0\equiv\frac{q^2-((\vartheta-1)t-2)q-\vartheta+2-2t}{2\gamma}+qj'+i \bmod n$.

(iv) When $\frac{(2t-3)q-(2t-3)t+2\gamma}{2\gamma}\leq j\leq\frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$, let $-\frac{(2t-3)q-(2t-3)t}{2\gamma}+j=j'$ for $1\leq j'\leq\frac{q-t}{2\gamma}$. Then we have $0\equiv\frac{q-t}{\gamma}+q(j'+\frac{(2t-3)q-(2t-3)t}{2\gamma})+i \bmod n$, which is equivalent to $0\equiv\frac{q^2-(2t-3)tq+2q-4t+4}{2\gamma}+qj'+i \bmod n$. Moreover, we have

$$\begin{aligned}0&<\frac{q^2+(3t+4)q+2\gamma-4t+4}{2\gamma}\\&\leq q+1+\frac{q^2-(2t-3)tq+2q-4t+4}{2\gamma}\\&\leq\frac{q^2-(2t-3)tq+2q-4t+4}{2\gamma}+qj'+i\\&\leq q\frac{q-t}{2\gamma}+\frac{(2t-2)q+2t+2-2\gamma}{2\gamma}\\&\quad+\frac{q^2-(2t-3)tq+2q-4t+4}{2\gamma}\\&=\frac{2\,q^2-(2t^2-4t)q-2t+6-2\gamma}{2\gamma}<n,\end{aligned}$$

which is in contradiction with then congruence $0\equiv\frac{q^2-(2t-3)tq+2q-4t+4}{2\gamma}+qj'+i \bmod n$.

If $k=1$, then we have $qj\equiv i+\frac{tq+1}{\gamma} \bmod n$, and then from $1\leq i,j\leq\frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$, we can seek some contradictions by considering the following cases.

(i) When $1\leq j\leq\frac{q-t}{2\gamma}$, we have

$$\begin{aligned}0&<\frac{tq+\gamma+1}{\gamma}\\&\leq i+\frac{tq+1}{\gamma}\\&=\frac{(2t-2)q+2t+2-2\gamma}{2\gamma}\\&\quad+\frac{tq+1}{\gamma}\\&<\frac{(4t-2)q+2t+4-2\gamma}{2\gamma}<q,\end{aligned}$$

which is in contradiction with $q\leq qj\leq\frac{q^2-tq}{2\gamma}$.

(ii) When $\frac{q-t+2\gamma}{2\gamma}\leq j\leq\frac{2q-2t}{2\gamma}$, let $j'=j-\frac{q-t}{2\gamma}$ for $1\leq j'\leq\frac{q-t}{2\gamma}$. Then we have $\frac{tq+1}{\gamma}+i\equiv q(j'+\frac{q-t}{2\gamma}) \bmod n$, which is equivalent to $i\equiv qj'+\frac{q^2-3tq-2}{2\gamma} \bmod n$. Moreover,

$$\begin{aligned}0&<\frac{q^2+(2\gamma-3t)q-2}{2\gamma}\\&\leq qj'+\frac{q^2-3tq-2}{2\gamma}\\&\leq q(\frac{q-t}{2\gamma})+\frac{q^2-3tq-2}{2\gamma}\\&=\frac{2q^2-4tq-2}{2\gamma}<n,\end{aligned}$$

which is in contradiction with $1\leq i\leq\frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$.

(iii) When $\frac{(\vartheta-1)q-(\vartheta-1)t+2\gamma}{2\gamma} \le j \le \frac{\vartheta q-\vartheta t}{2\gamma}$, where $3 \le \vartheta \le 2t-3$ (here, if there exists the case of $t \ge 4$), let $j' = j - \frac{(\vartheta-1)q-(\vartheta-1)t}{2\gamma}$ for $1 \le j' \le \frac{q-t}{2\gamma}$. Then we have $\frac{tq+1}{\gamma} + i \equiv q(j' + \frac{(\vartheta-1)q-(\vartheta-1)t}{2\gamma}) \bmod n$, which is equivalent to $i \equiv \frac{(\vartheta-1)q^2-(\vartheta+1)tq-2}{2\gamma} + qj' \bmod n$.

If ϑ is an odd, then we have $i \equiv \frac{-(\vartheta+1)tq-\vartheta-1}{2\gamma} + qj' \bmod n$. Moreover,

$$\begin{aligned}
0 &< \frac{(2t+2)q-2t+2}{2\gamma} \\
&\le \frac{(2\gamma-(\vartheta+1)t)q-\vartheta-1}{2\gamma} \\
&\le q - \frac{(\vartheta+1)tq+\vartheta+1}{2\gamma} \\
&\le qj' - \frac{(\vartheta+1)tq+\vartheta+1}{2\gamma} \\
&\le q\frac{q-t}{2\gamma} - \frac{(\vartheta+1)tq+\vartheta+1}{2\gamma} \\
&= \frac{q^2-(\vartheta+2)tq-1-\vartheta}{2\gamma} \\
&\le \frac{q^2-5tq-4}{2\gamma} < n,
\end{aligned}$$

which is in contradiction with $1 \le i \le \frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$.

If ϑ is an even, then we have $i \equiv \frac{q^2-(\vartheta+1)tq-\vartheta}{2\gamma} + qj' \bmod n$. Moreover,

$$\begin{aligned}
0 &< \frac{q^2+(3t+2)q-2t+4}{2\gamma} \\
&\le \frac{q^2+(2\gamma-\vartheta t-t)q-\vartheta}{2\gamma} \\
&\le q + \frac{q^2-(\vartheta+1)tq-\vartheta}{2\gamma} \\
&\le qj' + \frac{q^2-(\vartheta+1)tq-\vartheta}{2\gamma} \\
&\le q\frac{q-t}{2\gamma} + \frac{q^2-(\vartheta+1)tq-\vartheta}{2\gamma} \\
&\le \frac{2q^2-6tq-4}{2\gamma} < n,
\end{aligned}$$

which is in contradiction with $1 \le i \le \frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$.

(iv) When $\frac{(2t-3)q-(2t-3)t+2\gamma}{2\gamma} \le j \le \frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$, let $-\frac{(2t-3)q-(2t-3)t}{2\gamma} + j = j'$ for $1 \le j' \le \frac{q-t}{2\gamma}$. Then we have $\frac{tq+1}{\gamma} + i \equiv q(j' + \frac{(2t-3)q-(2t-3)t}{2\gamma}) \bmod n$, which is equivalent to $i \equiv \frac{q^2-(2t^2-t)q-2t+2}{2\gamma} + qj' \bmod n$. Moreover, we have

$$\begin{aligned}
0 &< \frac{q^2+(t+2)q-2t+2}{2\gamma} \\
&\le \frac{q^2-(2t^2-t)q-2t+2}{2\gamma} + q \\
&\le \frac{q^2-(2t^2-t)q-2t+2}{2\gamma} + qj' \\
&\le q\frac{q-t}{2\gamma} + \frac{q^2-(2t^2-t)q-2t+2}{2\gamma} \\
&= \frac{2q^2-2t^2q-2t+2}{2\gamma} < n.
\end{aligned}$$

It is in contradiction with $1 \le i \le \frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$.

(2) We have $H_0 H_2^{\dagger} = 0$. In fact, from Lemma 1, it only needs to show that

$$\left(\cup_{i=0}^{\frac{(t+1)q-3\gamma-t+1}{2\gamma}} C_{\beta+(q+1)i}\right) \cap -q\left(\cup_{i=1}^{\zeta} C_{\beta+(q+1)(\frac{(t+1)q-\gamma-t+1}{2\gamma}+i)}\right) = \emptyset,$$

where $1 \le \zeta \le \frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$. Assume that there exist two integers i, j, where $1 \le j \le \frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$ and $0 \le i \le \frac{(t+1)q-3\gamma-t+1}{2\gamma}$, such that $\beta + (q+1)i \equiv -q(\beta + (q+1)(j + \frac{(t+1)q-\gamma-t+1}{2\gamma}))q^{2k} \bmod (q+1)n$.

If $k = 0$, then we have $\beta + (q+1)i \equiv -q(\beta + (q+1)(j + \frac{(t+1)q-\gamma-t+1}{2\gamma})) \bmod (q+1)n$, which is equivalent to $qj + i - \frac{(t-1)q-\gamma+t+1}{2\gamma} \equiv 0 \bmod n$, where $1 \le j \le \frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$ and $0 \le i \le \frac{(t+1)q-3\gamma-t+1}{2\gamma}$.

(i) When $1 \le j \le \frac{q-t}{2\gamma}$, we have

$$\begin{aligned}
0 &< \frac{(2\gamma-t+1)q+\gamma-t-1}{2\gamma} \\
&= q - \frac{(t-1)q-\gamma+t+1}{2\gamma} \\
&\le qj + i - \frac{(t-1)q-\gamma+t+1}{2\gamma} \\
&= \frac{q^2-tq}{2\gamma} + \frac{(t+1)q-3\gamma-t+1}{2\gamma} \\
&\quad - \frac{(t-1)q-\gamma+t+1}{2\gamma} \\
&= \frac{q^2-(t-2)q-2\gamma-2t}{2\gamma} < n,
\end{aligned}$$

which is in contradiction with the congruence $qj + i - \frac{(t-1)q-\gamma+t+1}{2\gamma} \equiv 0 \bmod n$.

(ii) When $\frac{q-t+2\gamma}{2\gamma} \le j \le \frac{2q-2t}{2\gamma}$, let $j' = j - \frac{q-t}{2\gamma}$ for $1 \le j' \le \frac{q-t}{2\gamma}$. Then we have $0 \equiv -\frac{(t-1)q-\gamma+t+1}{2\gamma} + q(j' + \frac{q-t}{2\gamma}) + i \bmod n$, which is equivalent to $0 \equiv \frac{q^2-(2t-1)q+\gamma-t-1}{2\gamma} + qj' + i \bmod n$. Moreover,

$$\begin{aligned}
0 &< \frac{q^2+(\gamma-2t+1)q+\gamma-t-1}{2\gamma} \\
&\le qj' + i + \frac{q^2-(2t-1)q+\gamma-t-1}{2\gamma} \\
&\le q(\frac{q-t}{2\gamma}) + \frac{(t+1)q-3\gamma-t+1}{2\gamma} \\
&\quad + \frac{q^2-(2t-1)q+\gamma-t-1}{2\gamma} \\
&= \frac{2\,q^2-(2t-2)q-2\gamma-2t}{2\gamma} < n.
\end{aligned}$$

It is in contradiction with $0 \equiv \frac{q^2-(2t-1)q+\gamma-t-1}{2\gamma} + qj' + i \bmod n$.

(iii) When $\frac{(\vartheta-1)q-(\vartheta-1)t+2\gamma}{2\gamma} \leq j \leq \frac{\vartheta q-\vartheta t}{2\gamma}$, where $3 \leq \vartheta \leq 2t-3$ (here, if there exists the case of $t \geq 4$), let $j' = j - \frac{(\vartheta-1)q-(\vartheta-1)t}{2\gamma}$ for $1 \leq j' \leq \frac{q-t}{2\gamma}$. Then we have $0 \equiv -\frac{(t-1)q-\gamma+t+1}{2\gamma} + q(j' + \frac{(\vartheta-1)q-(\vartheta-1)t}{2\gamma}) + i \bmod n$, which is equivalent to $0 \equiv \frac{(\vartheta-1)q^2-(\vartheta t-1)q+\gamma-t-1}{2\gamma} + qj' + i \bmod n$.

If ϑ is an odd, we have $0 \equiv \frac{-(\vartheta t-1)q+\gamma-t-\vartheta}{2\gamma} + qj' + i \bmod n$. Moreover,

$$\begin{aligned}
0 &< \frac{(3t+3)q+\gamma-3t+3}{2\gamma} \\
&\leq \frac{(2\gamma-\vartheta t+1)q+\gamma-t-\vartheta}{2\gamma} \\
&\leq \frac{-(\vartheta t-1)q+\gamma-t-\vartheta}{2\gamma} + qj' + i \\
&\leq q(\frac{q-t}{2\gamma}) + \frac{(t+1)q-3\gamma-t+1}{2\gamma} \\
&\quad + \frac{-(\vartheta t-1)q+\gamma-t-\vartheta}{2\gamma} \\
&\leq \frac{q^2-(3t-2)q-2\gamma-2t-2}{2\gamma} < n,
\end{aligned}$$

which is in contradiction with the congruence $0 \equiv \frac{-(\vartheta t-1)q+\gamma-t-1-\vartheta}{2\gamma} + qj' + i \bmod n$.

If ϑ is an even, we have $0 \equiv \frac{q^2-(\vartheta t-1)q+\gamma-t+1-\vartheta}{2\gamma} + qj' + i \bmod n$. Moreover,

$$\begin{aligned}
0 &< \frac{q^2+(4t+3)q+\gamma-3t+5}{2\gamma} \\
&\leq \frac{q^2+(2\gamma-\vartheta t+1)q+\gamma-t+1-\vartheta}{2\gamma} \\
&= \frac{q^2-(\vartheta t-1)q+\gamma-t+1-\vartheta}{2\gamma} + q \\
&\leq \frac{q^2-(\vartheta t-1)q+\gamma-t+1-\vartheta}{2\gamma} + qj' + i \\
&\leq q(\frac{q-t}{2\gamma}) + \frac{(t+1)q-3\gamma-t+1}{2\gamma} \\
&\quad + \frac{q^2-(\vartheta t-1)q+\gamma-t+1-\vartheta}{2\gamma} \\
&= \frac{2q^2-(\vartheta t-2)q-2\gamma-2t+2-\vartheta}{2\gamma} \\
&\leq \frac{2q^2-(4t-2)q-2\gamma-2t-2}{2\gamma} < n,
\end{aligned}$$

which is in contradiction with the congruence $0 \equiv \frac{q^2-(\vartheta t-1)q+\gamma-t+1-\vartheta}{2\gamma} + qj' + i \bmod n$.

(iv) When $\frac{(2t-3)q-(2t-3)t+2\gamma}{2\gamma} \leq j \leq \frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$, let $-\frac{(2t-3)q-(2t-3)t}{2\gamma} + j = j'$ for $1 \leq j' \leq \frac{q-t}{2\gamma}$. Then we have $0 \equiv -\frac{(t-1)q-\gamma+t+1}{2\gamma} + q(j' + \frac{(2t-3)q-(2t-3)t}{2\gamma}) + i \bmod n$, which is equivalent to $0 \equiv \frac{q^2-(2\gamma-2t-3)q+\gamma-3t+3}{2\gamma} + qj' + i \bmod n$. Moreover,

$$\begin{aligned}
0 &< \frac{q^2+(2t+3)q+\gamma-3t+3}{2\gamma} \\
&\leq \frac{q^2-(2\gamma-2t-3)q+\gamma-3t+3}{2\gamma} + q \\
&\leq \frac{q^2-(2\gamma-2t-3)q+\gamma-3t+3}{2\gamma} + qj' + i \\
&\leq q\frac{q-t}{2\gamma} + \frac{(t+1)q-3\gamma-t+1}{2\gamma} \\
&\quad + \frac{q^2-(2\gamma-2t-3)q+\gamma-3t+3}{2\gamma} \\
&= \frac{2q^2-(2\gamma-2t-4)q-2\gamma-4t+4}{2\gamma} < n,
\end{aligned}$$

which is in contradiction with the congruence $0 \equiv \frac{q^2-(\gamma-2t-3)q+\gamma-3t+3}{2\gamma} + qj' + i \bmod n$.

If $k = 1$, then we have $\beta + (q+1)i \equiv -q(\beta - (q+1)(j+1+\frac{(t+1)q-\gamma-t+1}{2\gamma})) \bmod (q+1)n$, which is equivalent to $qj \equiv i + \frac{(t-1)q+\gamma+t+1}{2\gamma} \bmod n$, where $1 \leq j \leq \frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$ and $0 \leq i \leq \frac{(t+1)q-3\gamma-t+1}{2\gamma}$.

(i) When $1 \leq j \leq \frac{q-t}{2\gamma}$, we have

$$\begin{aligned}
0 &< \frac{(t-1)q+\gamma+t+1}{2\gamma} \\
&\leq i + \frac{(t-1)q+\gamma+t+1}{2\gamma} \\
&= \frac{(t+1)q-3\gamma-t+1}{2\gamma} \\
&\quad + \frac{(t-1)q+\gamma+t+1}{2\gamma} \\
&< \frac{2tq-2\gamma+2}{2\gamma} < q,
\end{aligned}$$

which is in contradiction with $q \leq qj \leq \frac{q^2-tq}{2\gamma}$.

(ii) When $\frac{q-t+2\gamma}{2\gamma} \leq j \leq \frac{2q-2t}{2\gamma}$, let $j' = j - \frac{q-t}{2\gamma}$ for $1 \leq j' \leq \frac{q-t}{2\gamma}$. Then we have $\frac{(t-1)q+\gamma+t+1}{2\gamma} + i \equiv q(j' + \frac{q-t}{2\gamma}) \bmod n$, which is equivalent to $i \equiv qj' + \frac{q^2-(2t-1)q-\gamma-t-1}{2\gamma} \bmod n$. Moreover,

$$\begin{aligned}
0 &< \frac{q^2+(2\gamma-2t+1)q-\gamma-t-1}{2\gamma} \\
&\leq qj' + \frac{q^2-(2t-1)q-\gamma-t-1}{2\gamma} \\
&\leq q(\frac{q-t}{2\gamma}) \\
&\quad + \frac{q^2-(2t-1)q-\gamma-t-1}{2\gamma} \\
&= \frac{2q^2-(3t-1)q-\gamma-t-1}{2\gamma} < n.
\end{aligned}$$

It is in contradiction with $0 \leq i \leq \frac{(t+1)q-3\gamma-t+1}{2\gamma}$.

(iii) When $\frac{(\vartheta-1)q-(\vartheta-1)t+2\gamma}{2\gamma} \leq j \leq \frac{\vartheta q-\vartheta t}{2\gamma}$, where $3 \leq \vartheta \leq 2t-3$ (if there exists the case of $t \geq 4$), let $j' = j - \frac{(\vartheta-1)q-(\vartheta-1)t}{2\gamma}$ for $1 \le j' \le \frac{q-t}{2\gamma}$. Then we have $\frac{(t-1)q+\gamma+t+1}{2\gamma} + i \equiv q(j' + \frac{(\vartheta-1)q-(\vartheta-1)t}{2\gamma}) \bmod n$, which is equivalent to $i \equiv \frac{(\vartheta-1)q^2-(\vartheta t-1)q-\gamma-t-1}{2\gamma} + qj' \bmod n$.

If ϑ is an odd, then we have $i \equiv \frac{-(\vartheta t-1)q-\vartheta-\gamma-t}{2\gamma} + qj' \bmod n$. Moreover,

$$\begin{aligned}0 &< \frac{(3t+3)q-3t-\gamma+3}{2\gamma}\\ &\le \frac{(2\gamma-\vartheta t+1)q-\vartheta-\gamma-t}{2\gamma}\\ &\le q-\frac{(\vartheta t-1)q+\vartheta+\gamma+t}{2\gamma}\\ &\le qj'-\frac{(\vartheta t-1)q+\vartheta+\gamma+t}{2\gamma}\\ &\le q\frac{q-t}{2\gamma}-\frac{(\vartheta t-1)q+\vartheta+\gamma+t}{2\gamma}\\ &\le \frac{q^2-(4t-1)q-3-\gamma-t}{2\gamma} < n,\end{aligned}$$

which is in contradiction with $0 \le i \le \frac{(t+1)q-3\gamma-t+1}{2\gamma}$.

If ϑ is an even, then we have $i \equiv \frac{q^2-\vartheta+1-(\vartheta t-1)q-\gamma-t}{2\gamma} + qj' \bmod n$. Moreover,

$$\begin{aligned}0 &< \frac{q^2+(4t+3)q-3t+5-\gamma}{2\gamma}\\ &\le \frac{q^2+(2\gamma-\vartheta t+1)q-\vartheta+1-\gamma-t}{2\gamma}\\ &\le q+\frac{q^2-\vartheta+1-(\vartheta t-1)q-\gamma-t}{2\gamma}\\ &\le qj'+\frac{q^2-\vartheta+1-(\vartheta t-1)q-\gamma-t}{2\gamma}\\ &\le q\frac{q-t}{2\gamma}+\frac{q^2-\vartheta+1-(\vartheta t-1)q-\gamma-t}{2\gamma}\\ &= \frac{2q^2-\vartheta+1-(\vartheta t+t-1)q-\gamma-t}{2\gamma}\\ &\le \frac{2q^2-3-(5t-1)q-\gamma-t}{2\gamma} < n,\end{aligned}$$

which is in contradiction with $0 \le i \le \frac{(t+1)q-3\gamma-t+1}{2\gamma}$.

(iv) When $\frac{(2t-3)q-t(2t-3)+2\gamma}{2\gamma} \le j \le \frac{(2t-2)q+2t+2-2\gamma}{2\gamma}$, let $-\frac{(2t-3)q-t(2t-3)}{2\gamma} + j = j'$ for $1 \le j' \le \frac{q-t}{2\gamma}$. Then we have $\frac{(t-1)q+\gamma+t+1}{2\gamma} + i \equiv q(j' + \frac{(2t-3)q-t(2t-3)}{2\gamma}) \bmod n$, which is equivalent to $i \equiv \frac{q^2-(2t^2-2t-1)q-\gamma-3t+3}{2\gamma} + qj' \bmod n$. Moreover, we have

$$\begin{aligned}0 &< \frac{q^2+(2t+3)q-\gamma-3t+3}{2\gamma}\\ &\le \frac{q^2-(2t^2-2t-1)q-\gamma-3t+3}{2\gamma}+qj'\\ &\le q\frac{q-t}{2\gamma}+\frac{q^2-(2t^2-2t-1)q-\gamma-3t+3}{2\gamma}\\ &= \frac{2q^2-(2t^2-t-1)q-\gamma-3t+3}{2\gamma} < n,\end{aligned}$$

which is in contradiction with $0 \le i \le \frac{(t+1)q-3\gamma-t+1}{2\gamma}$. Therefore, we have

$$HH^\dagger = \begin{pmatrix} 0 & H_0H_1^\dagger & 0\\ H_1H_0^\dagger & 0 & 0\\ 0 & 0 & 0\end{pmatrix}.$$

From $-qC_{\beta+(q+1)\frac{(t+1)q-\gamma-t+1}{2\gamma}} = C_{\beta+(q+1)(\frac{(t-1)(q+1)+2-\gamma}{2\gamma})}$, we have $rank(H_0H_1^\dagger) = 2$ and $rank(HH^\dagger) = 4$. Additionally, we have $c = 4$ from Lemma 2. Then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma} - 2d + 6, d; 4]]_q$ from Theorem 1 and Proposition 3, where $\frac{(t+1)q-t+1+2\gamma}{\gamma} \le d \le \frac{(3t-1)q+t+3}{\gamma}$ is odd. □

Example 2: If $t = 4$ and $e = 5$, then $q = 1024$ and $n = 61681$. Therefore, there exist entanglement-assisted quantum MDS codes from Theorem 5 that are listed in Table 2.

TABLE 2. Sample parameters of entanglement-assisted quantum MDS codes constructed from Theorem 5.

q	n	$[[n,k,d;c]]_q$
1024	61681	$[[61681, 61081, 303; 4]]_{1024}$
1024	61681	$[[61681, 61077, 305; 4]]_{1024}$
1024	61681	$[[61681, 61073, 307; 4]]_{1024}$
1024	61681	$[[61681, 61069, 309; 4]]_{1024}$
1024	61681	$[[61681, 61065, 311; 4]]_{1024}$
1024	61681	$[[61681, 61061, 313; 4]]_{1024}$
1024	61681	$[[61681, 61057, 315; 4]]_{1024}$
1024	61681	$[[61681, 61053, 317; 4]]_{1024}$
...	... ...	...
1024	61681	$[[61681, 60381, 653; 4]]_{1024}$
1024	61681	$[[61681, 60377, 655; 4]]_{1024}$
1024	61681	$[[61681, 60373, 657; 4]]_{1024}$
1024	61681	$[[61681, 60369, 659; 4]]_{1024}$
1024	61681	$[[61681, 60365, 661; 4]]_{1024}$
1024	61681	$[[61681, 60361, 663; 4]]_{1024}$

Theorem 6: Let $n = \frac{q^2+1}{\gamma}$ and $s = \frac{(q+\gamma+1)n}{2}$, where $\gamma = t^2+1$, t is a power of 2 and $q = t^e > 4$ with $e \equiv 1 \bmod 4$. If $\mathcal{C}$ is a q^2-ary λ-constacyclic code of length n with defining set $Z = \cup_{i=0}^{\delta} C_{s-(q+1)i}$ for $\frac{2tq+2}{2\gamma} \le \delta \le \frac{2(t+1)q-2\gamma-2t+2}{2\gamma}$, then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma} - 2d + 7, d; 5]]_q$, where $\frac{2tq+2+2\gamma}{\gamma} \le d \le \frac{2(t+1)q-2t+2}{\gamma}$ is even.

Proof: From Lemma 3, we can assume that the defining set of constacyclic code $\mathcal{C}$ is given by $Z = \cup_{i=0}^{\delta} C_{s-(q+1)i}$ for $\frac{2tq+2}{2\gamma} \le \delta \le \frac{2(t+1)q-2\gamma-2t+2}{2\gamma}$, and then $\mathcal{C}$ is a constacyclic code with parameters $[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma} - 2\delta - 1, 2\delta + 2]_{q^2}$ from Propositions 1 and 2. If $\delta = \frac{2tq+2}{2\gamma}$, then $Z = \cup_{i=0}^{\frac{2tq+2}{2\gamma}} C_{s-(q+1)i}$.

Since $-qC_{s-(q+1)\frac{2tq+2}{2\gamma}} = C_{s-(q+1)\frac{2q-2t}{2\gamma}}$, it follows that

$$\begin{aligned} Z \cap -qZ &= (\cup_{i=0}^{\frac{2tq+2}{2\gamma}} C_{s-(q+1)i}) \cap -q(\cup_{i=0}^{\frac{2tq+2}{2\gamma}} C_{s-(q+1)i}) \\ &= (\cup_{i=0}^{\frac{2tq-2t^2}{2\gamma}} C_{s-(q+1)i} \cap (-q \cup_{i=0}^{\frac{2tq-2t^2}{2\gamma}} C_{s-(q+1)i})) \\ &\quad \cup (\cup_{i=0}^{\frac{2tq-2t^2}{2\gamma}} C_{s-(q+1)i} \cap (-qC_{s-(q+1)\frac{2tq+2}{2\gamma}})) \\ &\quad \cup (C_{s-(q+1)\frac{2tq+2}{2\gamma}} \cap -q(\cup_{i=0}^{\frac{2tq-2t^2}{2\gamma}} C_{s-(q+1)i})) \\ &\quad \cup (-qC_{s-(q+1)\frac{2tq+2}{2\gamma}} \cap C_{s-(q+1)\frac{2tq+2}{2\gamma}}) \\ &= C_{s-(q+1)\frac{2tq+2}{2\gamma}} \cup C_{s-(q+1)(\frac{2q-2t}{2\gamma})} \cup C_s. \end{aligned}$$

From Lemma 2, $c = 5$. Therefore, there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma} - 2d + 7, d; 5]]_q$ from Theorem 1 and Proposition 3, where $d = \frac{2tq+2+2\gamma}{\gamma}$. If $\frac{2tq+2+2\gamma}{2\gamma} \le \delta \le \frac{2(t+1)q-2\gamma-2t+2}{2\gamma}$, then the defining set of $\mathcal{C}$ can be divided into four mutually disjoint subsets, i.e., $Z = Z_0 \cup Z_1 \cup Z_2 \cup Z_3$, where $Z_0 = C_s$, $Z_1 = \cup_{i=1}^{\frac{2tq-2t^2}{2\gamma}} C_{s-(q+1)i}$, $Z_2 = C_{s-(q+1)\frac{2tq+2}{2\gamma}}$ and $Z_3 = \cup_{i=\frac{2tq+2+2\gamma}{2\gamma}}^{\delta} C_{s-(q+1)i}$. The defining sets Z_0, Z_1, Z_2 and Z_3 can generate constacyclic codes $\mathcal{C}_0$, $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_3$ respectively. Let the parity check matrices of $\mathcal{C}, \mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{C}_3$ over F_{q^2} be H, H_0, H_1, H_2 and H_3, respectively. Therefore,

$$H = \begin{pmatrix} H_0 \\ H_1 \\ H_2 \\ H_3 \end{pmatrix},$$

and

$$HH^\dagger = \begin{pmatrix} H_0H_0^\dagger & H_0H_1^\dagger & H_0H_2^\dagger & H_0H_3^\dagger \\ H_1H_0^\dagger & H_1H_1^\dagger & H_1H_2^\dagger & H_1H_3^\dagger \\ H_2H_0^\dagger & H_2H_1^\dagger & H_2H_2^\dagger & H_2H_3^\dagger \\ H_3H_0^\dagger & H_3H_1^\dagger & H_3H_2^\dagger & H_3H_3^\dagger \end{pmatrix}.$$

Since $-qC_s = C_s$, it follows that $rank(H_0H_0^\dagger) = 1$ and

$$HH^\dagger = \begin{pmatrix} H_0H_0^\dagger & 0 & 0 & 0 \\ 0 & H_1H_1^\dagger & H_1H_2^\dagger & H_1H_3^\dagger \\ 0 & H_2H_1^\dagger & H_2H_2^\dagger & H_2H_3^\dagger \\ 0 & H_3H_1^\dagger & H_3H_2^\dagger & H_3H_3^\dagger \end{pmatrix}.$$

From Theorem 2 and $-qC_{s-(q+1)\frac{2tq+2}{2\gamma}} = C_{s-(q+1)\frac{2q-2t}{2\gamma}}$, it follwos that $rank(H_2H_1^\dagger) = rank(H_1H_2^\dagger) = 2$ and

$$HH^\dagger = \begin{pmatrix} H_0H_0^\dagger & 0 & 0 & 0 \\ 0 & 0 & H_1H_2^\dagger & H_1H_3^\dagger \\ 0 & H_2H_1^\dagger & 0 & 0 \\ 0 & H_3H_1^\dagger & 0 & H_3H_3^\dagger \end{pmatrix}.$$

Now, in order to determine the number of entangled states, we have to discuss two cases as follows.

(1) We have $H_3H_3^\dagger = 0$. In fact, from Lemma 1, we only need to consider that $Z_3 \cap -qZ_3 = \emptyset$. If $Z_3 \cap -qZ_3 \neq \emptyset$, where $Z_3 = \cup_{i=0}^{\delta} C_{s-(q+1)(\frac{2tq+2+2\gamma}{2\gamma}+i)}$ with $0 \le \delta \le \frac{2q-4\gamma-2t}{2\gamma}$, then there exist two integers i and j, where $0 \le i, j \le \frac{2q-4\gamma-2t}{2\gamma}$, such that $s-(q+1)(\frac{2tq+2+2\gamma}{2\gamma}+i) \equiv -q(s-(q+1)(\frac{2tq+2+2\gamma}{2\gamma}+j))q^{2k} \bmod (q+1)n$ for $k \in \{0, 1\}$.

If $k = 0$, then we have $0 \equiv \frac{(2t+2\gamma+2)q+2\gamma-2t+2}{2\gamma} + qj + i \bmod n$. Moreover,

$$\begin{aligned} 0 &< \frac{(2t+2\gamma+2)q+2\gamma-2t+2}{2\gamma} \\ &\le \frac{(2t+2\gamma+2)q+2\gamma-2t+2}{2\gamma} + qj + i \\ &\le \frac{(2t+2\gamma+2)q+2\gamma-2t+2}{2\gamma} \\ &\quad + q\frac{2q-4\gamma-2t}{2\gamma} + \frac{2q-4\gamma-2t}{2\gamma} \\ &= \frac{2q^2-(2\gamma-4)q-2\gamma-4t+2}{2\gamma} < n, \end{aligned}$$

which is in contradiction with $0 \equiv \frac{(2t+2\gamma+2)q+2\gamma-2t+2}{2\gamma} + qj + i \bmod n$.

If $k = 1$, then we have $i \equiv qj + \frac{(2\gamma-2t+2)q-2\gamma-2t-2}{2\gamma} \bmod n$. Moreover, we have

$$\begin{aligned} 0 &< \frac{(2\gamma-2t+2)q-2\gamma-2t-2}{2\gamma} \\ &\le qj + \frac{(2\gamma-2t+2)q-2\gamma-2t-2}{2\gamma} \\ &\le q\frac{2q-4\gamma-2t}{2\gamma} \\ &\quad + \frac{(2\gamma-2t+2)q-2\gamma-2t-2}{2\gamma} \\ &= \frac{2q^2-(2\gamma+4t-2)q-2\gamma-2t-2}{2\gamma} < n, \end{aligned}$$

which is in contradiction with $0 \le i \le \frac{2q-4\gamma-2t}{2\gamma}$.

(2) We have $H_1H_3^\dagger = H_3H_1^\dagger = 0$. In fact, we only need to show that $Z_1 \cap -qZ_3 = \cup_{i=1}^{\frac{2tq-2t^2}{2\gamma}} C_{s-(q+1)i} \cap -q(\cup_{i=0}^{\delta} C_{s-(q+1)(\frac{2tq+2+2\gamma}{2\gamma}+i)}) = \emptyset$ with $0 \le \delta \le \frac{2q-4\gamma-2t}{2\gamma}$. Assume that $\cup_{i=1}^{\frac{2tq-2t^2}{2\gamma}} C_{s-(q+1)i} \cap -q(\cup_{i=0}^{\delta} C_{s-(q+1)(\frac{2tq+2+2\gamma}{2\gamma}+i)}) \neq \emptyset$, then there exist two integers i, j, $1 \le i \le \frac{2tq-2t^2}{2\gamma}$ and $0 \le j \le \frac{2q-4\gamma-2t}{2\gamma}$, such that

$$\begin{aligned} &s-(q+1)i \\ &\quad \equiv -q(s-(q+1)(\frac{2tq+2+2\gamma}{2\gamma}+j))q^{2k} \bmod (q+1)n. \end{aligned}$$

If $k=0$, we have $0 \equiv i+\frac{2\gamma q+2q-2t}{2\gamma}+qj \bmod n$, where $1 \leq i \leq \frac{2tq-2t^2}{2\gamma}$ and $0 \leq j \leq \frac{2q-4\gamma-2t}{2\gamma}$. Moreover,

$$\begin{aligned} 0 &< \frac{2\gamma q+2q+2\gamma-2t}{2\gamma} \\ &= 1+\frac{2\gamma q+2q-2t}{2\gamma} \\ &\leq i+\frac{2\gamma q+2q-2t}{2\gamma}+qj \\ &\leq \frac{2tq-2t^2}{2\gamma} \\ &\quad +\frac{2\gamma q+2q-2t}{2\gamma}+q\frac{2q-4\gamma-2t}{2\gamma} \\ &= \frac{2q^2-(2\gamma-2)q-2t^2-2t}{2\gamma}<n, \end{aligned}$$

which is in contradiction with $0 \equiv i+\frac{2\gamma q+2q-2t}{2\gamma}+qj \bmod n$.

If $k=1$, we have $i \equiv \frac{2q+2\gamma q-2t}{2\gamma}+qj \bmod n$, where $1 \leq i \leq \frac{2tq-2t^2}{2\gamma}$ and $0 \leq j \leq \frac{2q-4\gamma-2t}{2\gamma}$. Moreover, we have

$$\begin{aligned} 0 &< \frac{2q+2\gamma q-2t}{2\gamma} \\ &\leq \frac{2q+2\gamma q-2t}{2\gamma}+qj \\ &\leq \frac{2q+2\gamma q-2t}{2\gamma}+q\frac{2q-4\gamma-2t}{2\gamma} \\ &= \frac{2q^2-2\gamma q-2tq+2q-2t}{2\gamma}<n, \end{aligned}$$

which is in contradiction with $1 \leq i \leq \frac{2tq-2t^2}{2\gamma}$.

Therefore, we have

$$HH^{\dagger}=\begin{pmatrix} H_0H_0^{\dagger} & 0 & 0 & 0 \\ 0 & 0 & H_1H_2^{\dagger} & 0 \\ 0 & H_2H_1^{\dagger} & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

and $rank(HH^{\dagger})=5$ from Lemma 2. Then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma}-2d+7, d; 5]]_q$ from Theorem 1 and Proposition 3, where $\frac{2tq+2+2\gamma}{\gamma} \leq d \leq \frac{2(t+1)q-2t+2}{\gamma}$ is even. □

Example 3: If $t=4$ and $e=5$, then $q=1024$ and $n=61681$. Therefore, there exist entanglement-assisted quantum MDS codes from Theorem 6 that are listed in Table 3.

Follows the method of Theorems 2 and 4, we can obtain the Theorems 7 and 8. We can also get Theorem 9 by using the same method of Theorem 3, 5 and 6.

Theorem 7: Let $n=\frac{q^2+1}{\gamma}$ and $s=\frac{(q+\gamma+1)n}{2}$, where $\gamma=t^2+1$, t is a power of 2 and $q=t^e$ with $e \equiv 3 \bmod 4$. If $\mathcal{C}$ is a q^2-ary λ-constacyclic code whose defining set is given by $Z=\cup_{i=1}^{\delta}C_{s-(q+1)i}$, where $1 \leq \delta \leq \frac{tq-\gamma-1}{\gamma}$, then $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$.

Theorem 8: Let $n=\frac{q^2+1}{\gamma}$, where $\gamma=t^2+1$, t is a power of 2 and $q=t^e$ with $e \equiv 3 \bmod 4$. Assume that $s=\frac{(q+\gamma+1)n}{2}$ and $\beta=\frac{q^2+q}{2}+1$, where $\beta=s-\frac{(q+1)(n-1)}{2}$. If $\mathcal{C}$ is a q^2-ary λ-constacyclic whose defining set is given by $Z=\cup_{i=0}^{\delta}C_{\beta+(q+1)i}$, where $0 \leq \delta \leq \frac{(t+1)q-3\gamma+t-1}{2\gamma}$, then $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$.

Remark 1: In Lemma 11 of [20], the author studied Hermitian dual-containing case of constacyclic codes with $q \equiv 13 \bmod 17$ when $0 \leq \lambda \leq \frac{3q+8}{10}$, in which $q=2^e$, while we can obtain Hermitian dual case of constacyclic codes with length $n=\frac{q^2+1}{17}$ when $0 \leq \delta \leq \frac{5q-48}{34}$ from Theorem 8, which implies that if δ exceeds the range of $0 \leq \delta \leq \frac{5q-48}{34}$, the Hermitian dual-containing case does not hold. We can obtain $0 \leq \lambda \leq \frac{5q-48}{34}$ by recalculating the rang of λ in Lemma 11 of [20].

Theorem 9: Let $n=\frac{q^2+1}{\gamma}$, where $\gamma=t^2+1$, t is a power of 2 and $q=t^e$ with $e \equiv 3 \bmod 4$. Assume that $s=\frac{(q+\gamma+1)n}{2}$ and $\beta=\frac{q^2+q}{2}+1$, where $\beta=s-\frac{(q+1)(n-1)}{2}$. Then we have the following results.

TABLE 3. Sample parameters of entanglement-assisted quantum MDS codes constructed from Theorem 6.

q	n	$[[n,k,d;c]]_q$
1024	61681	$[[61681,60720,484;5]]_{1024}$
1024	61681	$[[61681,60716,486;5]]_{1024}$
1024	61681	$[[61681,60712,488;5]]_{1024}$
1024	61681	$[[61681,60708,490;5]]_{1024}$
1024	61681	$[[61681,60704,492;5]]_{1024}$
1024	61681	$[[61681,60700,494;5]]_{1024}$
1024	61681	$[[61681,60696,496;5]]_{1024}$
...	...	...
1024	61681	$[[61681,60508,590;5]]_{1024}$
1024	61681	$[[61681,60504,592;5]]_{1024}$
1024	61681	$[[61681,60500,594;5]]_{1024}$
1024	61681	$[[61681,60496,596;5]]_{1024}$
1024	61681	$[[61681,60492,598;5]]_{1024}$
1024	61681	$[[61681,60488,600;5]]_{1024}$
1024	61681	$[[61681,60484,602;5]]_{1024}$

TABLE 4. Sample parameters of entanglement-assisted quantum MDS codes constructed from Theorem 9.

q	n	$[[n,k,d;c]]_q$
128	3277	$[[3277,3276,2;1]]_{128}$
128	3277	$[[3277,3272,4;1]]_{128}$
128	3277	$[[3277,3268,6;1]]_{128}$
...	...	...
128	3277	$[[3277,3084,98;1]]_{128}$
128	3277	$[[3277,3080,100;1]]_{128}$
128	3277	$[[3277,3076,102;1]]_{128}$
128	3277	$[[3277,3125,79;4]]_{128}$
128	3277	$[[3277,3121,81;4]]_{128}$
128	3277	$[[3277,3117,83;4]]_{128}$
...	...	...
128	3277	$[[3277,3031,125;4]]_{128}$
128	3277	$[[3277,3029,127;4]]_{128}$
128	3277	$[[3277,3025,129;4]]_{128}$
128	3277	$[[3277,3076,104;5]]_{128}$
128	3277	$[[3277,3072,106;5]]_{128}$
128	3277	$[[3277,3068,108;5]]_{128}$
...	...	...
128	3277	$[[3277,2984,150;5]]_{128}$
128	3277	$[[3277,2980,152;5]]_{128}$
128	3277	$[[3277,2976,154;5]]_{128}$

TABLE 5. Codes comparison.

$[[n,k,d;c]]_q$	Range of parameters	d	Ref.
$[[\frac{q^2+1}{5}, \frac{q^2-6q+33}{5}-4t, \frac{3q-1}{5}+2t; 4]]_q$	$q=2^e>4$ with $e\equiv 1 \bmod 4$, and $1\le t\le \frac{q+3}{5}$	$\frac{3q+9}{5}\le d\le q+1$ and d is odd	[10]
$[[\frac{q^2+1}{5}, \frac{q^2-6q+29}{5}-4t, \frac{3q+1}{5}+2t; 4]]_q$	$q=2^e$ with $e\equiv 3 \bmod 4$, and $1\le t\le \frac{q+2}{5}$	$\frac{3q+11}{5}\le d\le q+1$ and d is odd	[10]
$[[n, n-\frac{6}{5}(q-2)-4\lambda+4, \frac{3}{5}(q-2)+2\lambda+1; 4]]_q$	$n=\frac{q^2+1}{5}$, $q=2^e$ with $q\equiv 2 \bmod 10$, $1\le\lambda\le\frac{q+3}{5}$	$\frac{3q+9}{5}\le d=\frac{3}{5}(q-2)+2\lambda+1\le q+1$ and d is odd	[20]
$[[n, n-\frac{2}{5}(3q-14)-4\lambda, \frac{3q-14}{5}+2\lambda+3; 4]]_q$	$n=\frac{q^2+1}{5}$, $q=2^e$ with $q\equiv 8 \bmod 10$, $1\le\lambda\le\frac{q+2}{5}$	$\frac{3q+11}{5}\le d=\frac{3q-14}{5}+2\lambda+3\le q+1$ and d is odd	[20]
$[[n, n-\frac{10q-96}{17}-4\lambda, \frac{5q+3}{17}+2\lambda; 4]]_q$	$n=\frac{q^2+1}{17}$, $q=2^e$ with $q\equiv 13 \bmod 17$, $1\le\lambda\le\frac{3q-5}{17}$	$\frac{5q+37}{17}\le d=\frac{5q+3}{17}+2\lambda\le\frac{11q-7}{17}$ and d is odd	[20]
$[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma}-2d+3, d; 1]]_q$	$q=t^e>4$ with $e\equiv 1 \bmod 4$, and $\gamma=t^2+1$ with t is a power of 2	$2\le d\le\frac{2tq+2}{\gamma}$ and d is even	Theorem 3
$[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma}-2d+6, d; 4]]_q$	$q=t^e>4$ with $e\equiv 1 \bmod 4$, and $\gamma=t^2+1$ with t is a power of 2	$\frac{(t+1)q-t+1+2\gamma}{\gamma}\le d\le\frac{(3t-1)q+t+3}{\gamma}$ and d is odd	Theorem 5
$[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma}-2d+7, d; 5]]_q$	$q=t^e>4$ with $e\equiv 1 \bmod 4$, and $\gamma=t^2+1$ with t is a power of 2	$\frac{2tq+2\gamma+2}{\gamma}\le d\le\frac{2(t+1)q-2t+2}{\gamma}$ and d is even	Theorem 6
$[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma}-2d+3, d; 1]]_q$	$q=t^e$ with $e\equiv 3 \bmod 4$, and $\gamma=t^2+1$ with t is a power of 2	$2\le d\le\frac{2tq-2}{\gamma}$ and d is even	Theorem 9
$[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma}-2d+6, d; 4]]_q$	$q=t^e$ with $e\equiv 3 \bmod 4$, and $\gamma=t^2+1$ with t is a power of 2	$\frac{(t+1)q+2\gamma+t-1}{\gamma}\le d\le\frac{(3t-1)q-t-3}{\gamma}$ and d is odd; $\frac{3q+11}{5}\le d\le\frac{5q+5}{5}$ with $t=2$, and d is odd	Theorem 9
$[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma}-2d+7, d; 5]]_q$	$q=t^e$ with $e\equiv 3 \bmod 4$, and $\gamma=t^2+1$ with t is a power of 2	$\frac{2tq+2\gamma-2}{\gamma}\le d\le\frac{2(t+1)q+2t-2}{\gamma}$ and d is even	Theorem 9

(1) If $\mathcal{C}$ is a q^2-ary λ-constacyclic of length n with defining set $Z=\cup_{i=0}^{\delta}C_{s-(q+1)i}$ for $0\le\delta\le\frac{tq-\gamma-1}{\gamma}$, then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma}-2d+3, d; 1]]_q$, where $2\le d\le\frac{2tq-2}{\gamma}$ is even.

(2) If $\mathcal{C}$ is a q^2-ary λ-constacyclic of length n with defining set $Z=\cup_{i=0}^{\zeta}C_{\beta+(q+1)i}$ for $\frac{(t+1)q-\gamma+t-1}{2\gamma}\le\zeta\le\frac{(3t-1)q-3\gamma-t-3}{2\gamma}$ with $t\ge 4$, then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma}-2d+6, d; 4]]_q$, where $\frac{(t+1)q+2\gamma+t-1}{\gamma}\le d\le\frac{(3t-1)q-t-3}{\gamma}$ is odd. When $t=2$, we have $\frac{3q+11}{5}\le d\le\frac{5q+5}{5}$ is odd.

(3) If $\mathcal{C}$ is a q^2-ary λ-constacyclic of length n with defining set $Z=\cup_{i=0}^{\delta}C_{s-(q+1)i}$ for $\frac{2tq-2}{2\gamma}\le\delta\le\frac{2(t+1)q-2\gamma+2t-2}{2\gamma}$, then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\gamma}, \frac{q^2+1}{\gamma}-2d+7, d; 5]]_q$, where $\frac{2tq+2\gamma-2}{\gamma}\le d\le\frac{2(t+1)q+2t-2}{\gamma}$ is even.

Remark 2: From Remark 1, Theorem 9 in [20] can be rewritten as follows.

Let $q\equiv 13 \bmod 17$. If $\mathcal{C}$ is an q^2-ary λ-constacyclic constacyclic code of length n with defining set $Z=\cup_{j=0}^{\frac{5q-48}{34}+\lambda}C_{s-rj}$, then there exist entanglement-assisted quantum MDS codes with parameters $[[n, n-\frac{10q-96}{17}-4\lambda, \frac{5q+3}{17}+2\lambda; 4]]_q$, where $n=\frac{q^2+1}{17}$ and $1\le\lambda\le\frac{3q-5}{17}$.

Example 4: If $e=7$ and $t=2$, then $q=128$ and $n=3277$. Therefore, there exist entanglement-assisted quantum MDS codes from Theorem 9 that are listed in Table 4. Some codes from Theorem 9 have the same parameters as the ones in [10], [20].

IV. CONCLUSION AND DISCUSSION

In this work, we utilize constacyclic codes with length $\frac{q^2+1}{\gamma}$ to construct some families of entanglement-assisted quantum MDS codes, where $\gamma=t^2+1$, t is a power of 2 and q is a prime power of the form $q=t^e>4$ with $e\equiv 1 \bmod 4$ or $e\equiv 3 \bmod 4$. Some classes of entanglement-assisted quantum MDS codes available in [10], [20] as well as the new families of entanglement-assisted quantum MDS codes constructed in this paper that are listed in Table 5, with the parameters $[[n,k,d;c]]_q$ of entanglement-assisted quantum MDS codes in the first column, the range of parameters in the second column, the minimum distance d of the corresponding entanglement-assisted quantum MDS codes in the third column, and the corresponding references in the third column. We can see that entanglement-assisted codes constructed in this paper are more general in the sense that their parameters are not covered by the codes available in the literature. Additionally, it is more and more difficult to get the minimum distance d of entanglement-assisted quantum MDS codes that is greater than $\frac{q}{2}+1$ with the increase of γ.

In Table 5, entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{5}, \frac{q^2-6q+33}{5}-4t, \frac{3q-1}{5}+2t; 4]]_q$ are constructed from Theorem 4.4 in [10], where $\frac{3q+9}{5} \leq d \leq q+1$ is odd. Moreover, entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{5}, \frac{q^2-6q+29}{5}-4t, \frac{3q+1}{5}+2t; 4]]_q$ are also constructed from Theorem 4.5 in [10], where $\frac{3q+11}{5} \leq d \leq q+1$ is odd. These two families of entanglement-assisted quantum MDS from [10] are included in Theorem 5 and the part (2) of Theorem 9, which imply that entanglement-assisted quantum MDS codes constructed from this paper are more general. Additionally, those codes constructed from Theorems 6 and 7 from [20] are also included in Theorem 5 and the part (2) of Theorem 9. From Remark 2, we can see that entanglement-assisted quantum codes constructed from Theorem 9 in [20] are included in the part (2) of Theorem 9. Although the authors studied some families of entanglement-assisted quantum MDS with flexible entangled states in [12], [30], we discuss the different cases of entanglement-assisted quantum MDS codes with general length $\frac{q^2+1}{\gamma}$. In order to get more entanglement-assisted MDS codes with the number of entangled states that is more than 5, we can use the same method of this paper to achieve this goal. In the future work, we look forward to using some other constacyclic codes with different lengths to construct some new entanglement-assisted quantum MDS codes with flexible entangled states.

REFERENCES

[1] G. Bowen, "Entanglement required in achieving entanglement-assisted channel capacities," *Phys. Rev. A, Gen. Phys.*, vol. 66, Nov. 2002, Art. no. 052313.

[2] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, Oct. 2006.

[3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.

[4] B. Chen, S. Ling, and G. Zhang, "Application of constacyclic codes to quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 3, pp. 1474–1484, Mar. 2015.

[5] H. Chen, "Some good quantum error-correcting codes from algebraic-geometric codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 2059–2061, Jul. 2001.

[6] J. Chen, Y. Huang, C. Feng, and R. Chen, "Entanglement-assisted quantum MDS codes constructed from negacyclic codes," *Quantum Inf. Process.*, vol. 16, p. 303, Dec. 2017.

[7] J. Chen, Y. Huang, C. Feng, and R. Chen, "Some families of optimal quantum codes derived from constacyclic codes," *Linear Multilinear Algebra*, vol. 67, no. 4, pp. 725–742, 2018.

[8] J. Chen, Y. Chen, Y. Huang, and C. Feng, "New optimal asymmetric quantum codes and quantum convolutional codes derived from constacyclic codes," *Quantum Inf. Process.*, vol. 18, no. 2, p. 40, 2019.

[9] J. Chen, Y. Chen, and Y. Huang, "Some new classes of entanglement-assisted quantum MDS codes derived from constacyclic codes," *IEEE Access*, vol. 7, pp. 91679–91695, 2019. doi: 10.1109/ACCESS.2019.2927294.

[10] X. Chen, S, Zhu, and X. Kai, "Entanglement-assisted quantum MDS codes constructed from constacyclic codes," *Quantum Inf. Process.*, vol. 17, no. 10, p. 273, 2018.

[11] J. Fan, H. Chen, and J. Xu, "Constructions of q-ary entanglement-assisted quantum MDS codes with minimum distance greater than q + 1," *Quantum Inf. Comput.*, vol. 16, nos. 5–6, pp. 423–434, 2016.

[12] W. Fang, F.-W. Fu, L. Li, and S. Zhu, "Euclidean and Hermitian hulls of MDS codes and their applications to EAQECCs," 2018, *arXiv:1812.09019*. [Online]. Available: https://arxiv.org/abs/1812.09019

[13] K. Guenda, S. Jitman, and T. A. Gulliver, "Constructions of good entanglement-assisted quantum error correcting codes," *Des., Codes Cryptogr.*, vol. 86, no. 1, pp. 121–136, 2018.

[14] L. Guo and R. Li, "Linear Plotkin bound for entanglement-assisted quantum codes," *Phys. Rev. A, Gen. Phys.*, vol. 87, no. 3, 2013, Art. no. 032309.

[15] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[16] Y. Huang, J. Chen, C. Feng, and R. Chen, "Some families of asymmetric quantum MDS codes constructed from constacyclic codes," *Int. J. Theor. Phys.*, vol. 57, no. 2, pp. 453–464, 2018.

[17] X. Kai and S. Zhu, "New quantum MDS codes from negacyclic codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 1193–1197, Feb. 2013.

[18] X. Kai, S. Zhu, and P. Li, "Constacyclic codes and some new quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2080–2086, Apr. 2014.

[19] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4892–4914, Nov. 2006.

[20] M. E. Koroglu, "New entanglement-assisted MDS quantum codes from constacyclic codes," *Quantum Inf. Process.*, vol. 18, no. 1, p. 44, Feb. 2019.

[21] G. G. La Guardia, "On optimal constacyclic codes," *Linear Algebra Appl.*, vol. 496, pp. 594–610, May 2016.

[22] C.-Y. Lai and A. Ashikhmin, "Linear programming bounds for entanglement-assisted quantum error-correcting codes by split weight enumerators," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 622–639, Jan. 2018.

[23] C.-Y. Lai and T. A. Brun, "Entanglement increases the error-correcting ability of quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 88, no. 1, 2013, Art. no. 012320.

[24] R. Li, F. Zuo, and Y. Liu, "A study of skew asymmetric q^2-cyclotomic coset and its application," (in Chinese), *J. Air Force Eng. Univ., Nat. Sci. Ed.*, vol. 12, no. 1, pp. 87–89, 2011.

[25] Y. Liu, R. Li, L. Lü, and Y. Ma, "Application of constacyclic codes to entanglement-assisted quantum maximum distance separable codes," *Quantum Inf. Process.*, vol. 17, no. 8, pp. 1–19, 2018.

[26] L. Lü, W. Ma, R. Li, Y. Ma, and L. Guo, "New quantum MDS codes constructed from constacyclic codes," 2018, *arXiv:1803.07927*. [Online]. Available: https://arxiv.org/abs/1803.07927

[27] L.-D. Lü and R. Li, "Entanglement-assisted quantum codes constructed from primitive quaternary BCH codes," *Int. J. Quantum Inf.*, vol. 12, no. 3, 2014, Art. no. 1450015.

[28] L. Lü, W. Ma, R. Li, Y. Ma, Y. Liu, and H. Cao, "Entanglement-assisted quantum MDS codes from constacyclic codes with large minimum distance," *Finite Fields Appl.*, vol. 53, pp. 309–325, Sep. 2018.

[29] L. Lü, R. Li, L. Guo, Y. Ma, and Y. Liu, "Entanglement-assisted quantum MDS codes from negacyclic codes," *Quantum Inf. Process.*, vol. 17, no. 3, p. 69, 2018.

[30] G. Luo, X. Cao, and X. Chen, "MDS codes with hulls of arbitrary dimensions and their quantum error correction," *IEEE Trans. Inf. Theory*, vol. 65, no. 5, pp. 2944–2952, May 2019.

[31] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.

[32] J. Qian and L. Zhang, "Nonbinary quantum codes derived from group character codes," *Int. J. Quantum Inf.*, vol. 10, no. 4, 2012, Art. no. 1250042.

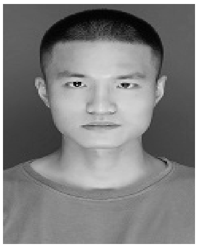
[33] J. Qian and L. Zhang, "New optimal subsystem codes," *Discrete Math.*, vol. 313, pp. 2451–2455, Nov. 2013.

[34] J. Qian and L. Zhang, "Entanglement-assisted quantum codes from arbitrary binary linear codes," *Des., Codes Cryptogr.*, vol. 77, no. 1, pp. 193–202, 2015.

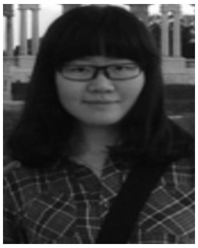
[35] J. Qian and L. Zhang, "Improved constructions for quantum maximum distance separable codes," *Quantum Inf. Process.*, vol. 16, no. 1, p. 20, 2017.
[36] J. Qian and L. Zhang, "On MDS linear complementary dual codes and entanglement-assisted quantum codes," *Des., Codes Cryptogr.*, vol. 86, no. 7, pp. 1565–1572, 2018.
[37] P. W. Shor, "Scheme for reducing decoherence in quantum memory," *Phys. Rev. A*, vol. 52, no. 4, pp. 2493–2496, 1995.
[38] A. M. Steane, "Simple quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 6, pp. 4741–4751, 1996.
[39] A. M. Steane, "Enlargement of Calderbank–Shor–Steane quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2492–2495, Nov. 1999.
[40] A. Shikhmin, S. Litsyn, and M. A. Tsfasman, "Asymptotically good quantum codes," *Phys. Rev. A, Gen. Phys.*, vol. 63, no. 3, 2001, Art. no. 032311.
[41] N. Tang, Z. Li, L. Xing, and M. Zhang, "The Gilbert–Varshamov bound for stabilizer codes over $\mathbb{Z}_m$," *IEEE Access*, vol. 6, pp. 45699–45706, 2018.
[42] L. Wang and S. Zhu, "New quantum MDS codes derived from constacyclic codes," *Quantum Inf. Process.*, vol. 14, no. 3, pp. 881–889, 2015.
[43] M. M. Wilde and T. A. Brun, "Optimal entanglement formulas for entanglement-assisted quantum coding," *Phys. Rev. A, Gen. Phys.*, vol. 77, no. 6, 2008, Art. no. 064302.
[44] G. Zhang and B. Chen, "New quantum MDS codes," *Int. J. Quantum Inf.*, vol. 12, no. 4, p. 1450019, 2014.
[45] T. Zhang and G. Ge, "Some new classes of quantum MDS codes from constacyclic codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 5224–5228, Sep. 2015.
[46] M. Zhang, Z. Li, L. Xing, and N. Tang, "Construction of some new quantum BCH codes," *IEEE Access*, vol. 6, pp. 36122–36131, 2018.

JIANZHANG CHEN received the Ph.D. degree in information and communication engineering from the University of Electronic Science and Technology of China (UESTC), in 2015. He is currently a Lecturer with the Department of Computer Science and Technology, Fujian Agriculture and Forestry University. Since 2017, he has been a Postdoctoral Fellow with UESTC. His research interests include information theory and coding theory, complex networks, and evolutionary game theory.

YOUQIN CHEN received the B.S. and M.S. degrees from Fujian Normal University, in 2008 and 2011, respectively. She is currently pursuing the Ph.D. degree with Wuhan University. She was a Software Development Engineer with Chinatelecom Fufu Information Technology Company Ltd., from 2011 to 2017. Her research interests include data mining and privacy protection, information theory, and coding theory.



DONG YU received the B.S. degree in computer science and technology from Fujian Agriculture and Forestry University, in 2018. His research interests include machine learning and data mining, information theory, and coding theory.



CHUNHUI FENG received the M.S. and Ph.D. degrees from Wuhan University, in 2010 and 2015, respectively. She is currently a Lecturer with the Department of Electronic Engineering, Fujian Agriculture and Forestry University. Her research interests include multimedia information security and coding theory.

YUANYUAN HUANG received the B.S., M.S., and Ph.D. degrees from the University of Electronic Science and Technology of China (UESTC), in 2004, 2007, and 2013, respectively. He was with University of Washington, Seattle, WA, USA, for his research work, from 2009 to 2011. He is currently a Lecturer with the Chengdu University of Information Technology. His research interests include information theory and coding theory, image/video processing, and data science.

RIQING CHEN received the B.Eng. degree in communication engineering from Tongji University, China, in 2001, the M.Sc. degree in communications and signal processing from Imperial College London, U.K., in 2004, and the Ph.D. degree in engineering science from the University of Oxford, U.K., in 2010. Since 2014, he has been a Professor and a M.S. Supervisor with the College of Computer and Information Sciences, Fujian Agriculture and Forestry University, Fuzhou, China. His current research interests include big data and visualization, cloud computing, consumer electronics, flash memory, wireless sensor networking, and image processing.