IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 12, 2019, accepted June 24, 2019, date of publication July 8, 2019, date of current version July 25, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2927294

Some New Classes of Entanglement-Assisted Quantum MDS Codes Derived From Constacyclic Codes

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

[1]College of Computer and Information Sciences, Fujian Agriculture and Forestry University, Fuzhou 350002, China
[2]State Key Laboratory of Information Engineering in Surveying, Mapping, and Remote Sensing, Wuhan University, Wuhan 430079, China
[3]Department of Network Engineering, Chengdu University of Information Technology, Chengdu 610225, China
[4]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, 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 Although quantum maximal-distance-separable (MDS) codes that satisfy the quantum singleton bound have become an important research topic in the quantum coding theory, it is not an easy task to search for quantum MDS codes with the minimum distance that is larger than $(q/2)+1$. The pre-shared entanglement between the sender and the receiver can improve the minimum distance of quantum MDS codes such that the minimum distance of some constructed codes achieves $(q/2)+1$ or exceeds $(q/2)+1$. Meanwhile, how to determine the required number of maximally entangled states to make the minimum distance of quantum MDS codes larger than $(q/2)+1$ is an interesting problem in the quantum coding theory. In this paper, we utilize the decomposition of the defining set and q^2-cyclotomic cosets of constacyclic codes with the form $q=\alpha m+t$ or $q=\alpha m+\alpha-t$ and $n=(q^2+1/\alpha)$ to construct some new families of entanglement-assisted quantum MDS codes that satisfy the entanglement-assisted quantum singleton bound, where q is an odd prime power and m is a positive integer, while both α and t are positive integers such that $\alpha=t^2+1$. The parameters of these codes constructed in this paper are more general compared with the ones in the literature. Moreover, the minimum distance of some codes in this paper is larger than $(q/2)+1$ or $q+1$.

INDEX TERMS Entanglement-assisted quantum codes, constacyclic codes, maximal-distance-separable (MDS) codes.

I. INTRODUCTION

In the quantum information and quantum computing, an important subject is to constuct some good quantum error-correcting codes (quantum codes for short) [3], [5], [7], [8], [15], [18], [30], [31], [35]–[37], [42]. Let q be a prime power, a q-ary quantum code of length n can be denoted as $[[n,k,d]]_q$, where k represents the size of q^k that is a q^k-dimensional subspace of the q^n-dimensional Hilbert space and d is the minimum distance. The quantum code can detect up to $d-1$ quantum errors and correct up to $\lfloor \frac{d-1}{2} \rfloor$ quantum errors. Quantum MDS codes that satisfy the quantum Singleton bound, that is, $2d=n-k+2$, are constructed from the Hermitian construction by most scholars. Based on this Hermitian construction, quantum MDS codes have been constructed from constacyclic codes including negacyclic codes and cyclic codes. Some quantum MDS codes with minimum distance exceeding $\frac{q}{2}+1$ have been constructed from constacyclic codes. In [16], Kai et al. constructed two families of quantum MDS codes by using negacyclic codes. In [17], Kai et al. researched some families of constacyclic codes. In [38], Wang et al. studied two families of constacyclic codes extended from some results of [17]. In [4], Chen et al. studied some families of constacyclic codes that were different from the ones in [17] and used them to construct quantum MDS codes. For more results of quantum MDS codes,

The associate editor coordinating the review of this manuscript and approving it for publication was Soon Xin Ng.

the readers can consult [24], [33], [40], [41]. However, the construction of quantum MDS codes with relatively large minimum distance is not an easy task. Most of known q-ary quantum MDS codes have minimum distance less than or equal to $\frac{q}{2}+1$ except for some special codes' length.

In recent years, the discovery of the theory of entanglement-assisted quantum codes plays an important role in the area of quantum error-correction. Entanglement-assisted stabilizer formalism was proposed by Brun et al. in [2]. They showed that if the sender and the receiver shared a certain amount of pre-existing entanglement, some entanglement-assisted quantum codes can be constructed without dual-containing classical quaternary codes [2]. Many scholars have constructed some entanglement-assisted quantum codes with good parameters in [1], [13], [21], [39]. In [25], the concept about a decomposition of the defining set of cyclic code was proposed by Li et al., and this method was used to construct some entanglement-assisted quantum codes having good parameters. In [32], Qian et al. constructed some families of entanglement-assisted quantum codes by using arbitrary binary linear codes and showed 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. A construction of entanglement-assisted quantum MDS codes with the help of a small amount of pre-shared maximally entanglement was provided by Fan et al. in [10]. Guenda et al. introduced the hull of the classical codes and constructed some families of entanglement-assisted quantum MDS codes in [12]. Based on the results of [22], [25], we proposed a decomposition of the defining set of negacyclic codes and utilized this method to construct some families of entanglement-assisted quantum MDS codes with different lengths in [6]. In [26], [27], Lü et al. used the decomposition of the defining set of negacyclic codes and constacyclic codes to construct some families of entanglement-assisted quantum MDS codes respectively, and someone of those constructed quantum MDS codes have larger minimum distance with $d \geq q+1$. In [23], Liu et al. constructed some new entanglement-assisted quantum MDS codes from constacyclic codes of length $n=\frac{q^2-1}{r}$ for $r=3,5,6,7$ and $q \equiv -1 \bmod r$. In fact, pre-shared entanglement can improve the error-correcting ability of quantum codes. By using the method of pre-shared entanglement, those quantum MDS codes with minimum distance not exceeding $\frac{q}{2}+1$ can exceed $\frac{q}{2}+1$ or even $q+1$. Therefore, it is necessary for us to consider the construction of entanglement-assisted quantum MDS codes with larger distance.

Moreover, in quantum coding theory, how to determine the number of pre-shared maximally entangled states to make the minimum distance of quantum MDS codes larger than $\frac{q}{2}+1$ or even $q+1$ is an interesting problem. In [28], although Luo et al. studied some classes of entanglement-assisted MDS codes from generalized Reed-Solomon codes under the Euclidean case and the parameters of those codes were new and flexible relative to the ones from [6], [12], [27], [34], the authors just consider the Euclidean construction not Hermitian construction. Very recently, in [11], although Fang et al. presented several classes of entanglement-assisted quantum MDS codes by employing the Hermitian hull of generalized Reed-Solomon codes, they did not consider the case of entanglement-assisted quantum MDS codes with length $\frac{q^2+1}{\alpha}$. In this paper, the method that is the decomposition of the defining set of constacyclic codes with length $\frac{q^2+1}{\alpha}$ is used to determine the number of pre-shared maximally entangled states, and then to construct some new families of entanglement-assisted quantum MDS codes with length $\frac{q^2+1}{\alpha}$, which is different from the one used in [11], [28]. Additionally, by the method, the length of entanglement-assisted quantum codes is more general, so 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 [19], [26], [27]. Furthermore, we can also use the same method of the decomposition of the defining set of constacyclic codes to obtain other entanglement-assisted quantum MDS codes with the number of pre-shared maximally entangled states that exceeds 9 in the Hermitian construction. Some families of entanglement-assisted quantum MDS codes constructed in this paper are listed as follows.

(1) $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha}-2d+3, d; 1]]_q$, where q is an odd prime power with the form $q=\alpha m+t$, m is a positive integer, α and $t \geq 2$ are positive integers such that $\alpha = t^2+1$ and $2 \leq d \leq \frac{2tq+2}{\alpha}$ is even.

(2) $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha}-2d+7, d; 5]]_q$, where q is an odd prime power of the form $q=\alpha m+t$, m is a positive integer, α and $t \geq 2$ are positive integers such that $\alpha = t^2+1$ and $\frac{2tq+2+2\alpha}{\alpha} \leq d \leq \frac{2(t+1)q-2(t-1)}{\alpha}$ is even.

(3) $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha}-2d+11, d; 9]]_q$, where q is an odd prime power of the form $q=\alpha m+t$, m is a positive integer, α and $t \geq 3$ are positive integers such that $\alpha = t^2+1$ and $\frac{2(t+1)q-2(t-1)+2\alpha}{\alpha} \leq d \leq \frac{2(2t-1)q+2t+4}{\alpha}$ is even. If $t=2$, then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha}-2d+11, d; 9]]_q$, where $\frac{6q+8}{5} \leq d \leq \frac{8q-6}{5}$ is even.

(4) $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha}-2d+3, d; 1]]_q$, where q is an odd prime power with the form $q=\alpha m+\alpha-t$, m is a positive integer, α and $t \geq 2$ are positive integers such that $\alpha = t^2+1$ and $2 \leq d \leq \frac{2tq-2}{\alpha}$ is even.

(5) $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha}-2d+7, d; 5]]_q$, where q is an odd prime power of the form $q=\alpha m+\alpha-t$, m is a positive integer, α and $t \geq 2$ are positive integers such that $\alpha = t^2+1$ and $\frac{2tq-2+2\alpha}{\alpha} \leq d \leq \frac{2(t+1)q+2(t-1)}{\alpha}$ is even.

(6) $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha}-2d+11, d; 9]]_q$, where q is an odd prime power of the form $q=\alpha m+\alpha-t$, m is a positive integer, α and $t > 3$ are positive integers such that $\alpha = t^2+1$ and $\frac{2(t+1)q+2(t-1)+2\alpha}{\alpha} \leq d \leq \frac{2(2t-1)q-2t-4}{\alpha}$ is even.

If $t = 2$, then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha}-2d+11, d; 9]]_q$, where $\frac{6q+12}{5} \leq d \leq \frac{8q-4}{5}$ is even. If $t = 3$, then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha}-2d+11, d; 9]]_q$, where $\frac{8q+24}{10} \leq d \leq \frac{10q+10}{10}$ is even.

The main organization of this paper is as follows. In Sec. 2, we present some definitions and basic results of constacyclic codes and entanglement-assisted quantum codes. In Sec. 3, we construct some families of entanglement-assisted quantum MDS codes by using constacyclic codes with length $\frac{q^2+1}{\alpha}$, where some quantum MDS codes have larger minimum distance exceeding $\frac{q}{2}+1$ or $q+1$. In Sec. 4, we give the conclusion and discussion.

II. PREMILINARIES

In this section, we recall some basic results about constacyclic codes in [4], [14], [16], [17], [20], [24], [29], [33], [38], [40], [41] and some results of entanglement-assisted quantum codes in [2], [6], [23], [25], [26].

Let F_{q^2} be the finite field with q^2 elements, where q is a power of p and p is an odd prime number. Assume that n is a positive integer relatively prime to q, i.e., $gcd(n, q) = 1$. If $\mathcal{C}$ is a k-dimensional subspace of $F_{q^2}^n$, then $\mathcal{C}$ is said to be an $[n, k]$-linear code. The number of nonzero components of $c \in \mathcal{C}$ is said to be the weight $wt(c)$ of the codeword c. The minimum nonzero weight d of all codewords in $\mathcal{C}$ is said to be the minimum weight of $\mathcal{C}$. 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

$$\langle u, v\rangle_h = u_0v_0^q + u_1v_1^q + \cdots + u_{n-1}v_{n-1}^q.$$

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

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

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

Given 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. We know that a q^2-ary λ-constacyclic code $\mathcal{C}$ of length n is an ideal of $F_{q^2}[x]/\langle x^n - \lambda\rangle$ and $\mathcal{C}$ can be generated by a monic polynomial $g(x)$ which divides $x^n - \lambda$. From [4], [17], 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. Assume that $\lambda \in F_{q^2}^*$ is a primitive r-th root of unity, and then there 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 $1 \leq i \leq n-1$. Let $\mathcal{O}_{rn} = \{1 + jr | 0 \leq j \leq n-1\}$. 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 of a constacyclic code $\mathcal{C} = \langle g(x)\rangle$ of length n is the set

$$Z = \{i \in \mathcal{O}_{rn} \mid \eta^i \ is\ a\ root\ of\ g(x)\}.$$

Let $\mathcal{C}$ be an $[n, k]$ constacyclic code over F_{q^2} with defining set Z. Then the Hermitian dual $\mathcal{C}^{\perp_h}$ has a defining set $Z^{\perp_h} = \{z \in \mathcal{O}_{rn}| -qz \text{ mod } rn \notin Z\}$.

Proposition 1 (The BCH Bound for Constacyclic Codes [17], [20]): Let $\mathcal{C}$ be a q^2-ary 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.

Proposition 2 (Singleton bound [14], [29]): If an $[n, k, d]$ linear code $\mathcal{C}$ over F_q exists, then

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

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

Lemma 1 ([4], [17]): Let $\mathcal{C}$ be a q^2-ary 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 basic notions and results of entanglement-assisted quantum codes in [2], [6], [23], [25], [26].

An entanglement-assisted quantum code can be denoted as $[[n, k, d; c]]_q$, with the help of c pairs of maximally entangled states, which encodes k information qubits into n channel qubits, where the minimum distance is d. Let H be an $(n - k) \times n$ parity check matrix of $\mathcal{C}$ over F_{q^2}. Then $\mathcal{C}^{\perp_h}$ has an $n \times (n - k)$ generator matrix $H^\dagger$, where $H^\dagger$ is the conjugate transpose matrix of H over F_{q^2}.

Theorem 1 ([2], [6], [23], [25], [26]): If $\mathcal{C}$ 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.

Proposition 3 ([2], [6], [23], [25], [26]): 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 [23], [26], the authors gave the definition for the decomposition of the defining set of constacyclic codes that containing cyclic codes and negacyclic codes.

Definition 1 ([23], [26]): Let $\mathcal{C}$ be a 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 ([23], [26]): Let Z be a defining set of a 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 required number of entangled states is $c = |Z_1|$.

Similar to Lemma 3.1 in [24], we can get Lemma 3 as follows.

Lemma 3: Let $n = \frac{q^2+1}{\alpha}$, where q is an odd prime power with the form $q = \alpha m + t$ or $q = \alpha m + \alpha - t$, m is a positive integer, both α and $t \geq 2$ are integers such that $\alpha = t^2 + 1$. Then the q^2-cyclotomic cosets modulo $(q+1)n$ are $C_n = \{n\}$ and $C_{n-(q+1)j} = \{n-(q+1)j, n+(q+1)j\}$ for $1 \leq j \leq \frac{n-1}{2}$.

Theorem 2: Let $n = \frac{q^2+1}{\alpha}$, where q is an odd prime power with the form $q = \alpha m + t$, m is a positive integer, both α and $t \geq 2$ are integers such that $\alpha = t^2 + 1$. If $\mathcal{C}$ is a constacyclic code whose defining set is given by $Z = \cup_{i=1}^{\delta} C_{n-(q+1)i}$, where $1 \leq \delta \leq \frac{tq-\alpha+1}{\alpha}$, 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 $1 \leq i, j \leq \frac{tq-\alpha+1}{\alpha}$, such that

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

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

(1) If $k = 0$, then

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

is equivalent to $0 \equiv qj + i \bmod n$.

For $1 \leq i, j \leq \frac{tq-\alpha+1}{\alpha}$, we can consider the following cases.

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

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

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

(ii) When $\frac{q-t+\alpha}{\alpha} \leq j \leq \frac{2q-2t}{\alpha}$, let $j' = j - \frac{q-t}{\alpha}$, where $1 \leq j' \leq \frac{q-t}{\alpha}$. Then we have

$$0 \equiv q(j' + \frac{q-t}{\alpha}) + i \bmod n,$$

which is equivalent to

$$0 \equiv qj' + \frac{q^2-tq}{\alpha} + i \equiv qj' - \frac{tq+1}{\alpha} + i \bmod n.$$

Moreover,

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

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

(iii) When $\frac{(\varepsilon-1)q-(\varepsilon-1)t+\alpha}{\alpha} \leq j \leq \frac{\varepsilon q-\varepsilon t}{\alpha}$, where $3 \leq \varepsilon \leq t$ (if there exists $t \geq 3$), let $j' = j - \frac{(\varepsilon-1)q-(\varepsilon-1)t}{\alpha}$, where $1 \leq j' \leq \frac{q-t}{\alpha}$. Then we have

$$0 \equiv q(j' + \frac{(\varepsilon-1)q-(\varepsilon-1)t}{\alpha}) + i \bmod n,$$

which is equivalent to

$$\begin{aligned} 0 &\equiv qj' + \frac{(\varepsilon-1)q^2-(\varepsilon-1)qt}{\alpha} + i \\ &\equiv qj' - \frac{(\varepsilon-1)tq+(\varepsilon-1)}{\alpha} + i \bmod n. \end{aligned}$$

Moreover,

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

It is in contradiction with the congruence

$$0 \equiv qj' - \frac{(\varepsilon-1)tq+(\varepsilon-1)}{\alpha} + i \bmod n.$$

(2) If $k = 1$, then

$$n - (q+1)i \equiv -q(n - (q+1)j)q^2 \bmod (q+1)n$$

is equivalent to $qj \equiv i \bmod n$.

For $1 \leq i, j \leq \frac{tq-\alpha+1}{\alpha}$, we can consider the following cases.

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

$$q \leq qj \leq q\frac{q-t}{\alpha} \leq \frac{q^2-tq}{\alpha} < n.$$

It is in contradiction with $1 \leq i \leq \frac{tq-\alpha+1}{\alpha}$.

(ii) When $\frac{q-t+\alpha}{\alpha} \le j \le \frac{2q-2t}{\alpha}$, let $j' = j - \frac{q-t}{\alpha}$, where $1 \le j' \le \frac{q-t}{\alpha}$. Then we have

$$i \equiv q(j' + \frac{q-t}{\alpha}) \bmod n,$$

which is equivalent to

$$i \equiv qj' + \frac{q^2-tq}{\alpha} \equiv qj' - \frac{tq+1}{\alpha} \bmod n.$$

Moreover,

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

It is in contradiction with $1 \le i \le \frac{tq-\alpha+1}{\alpha}$.

(iii) When $\frac{(\varepsilon-1)q-(\varepsilon-1)t+\alpha}{\alpha} \le j \le \frac{\varepsilon q-\varepsilon t}{\alpha}$, where $3 \le \varepsilon \le t$ (if there exists $t \ge 3$), let $j' = j - \frac{(\varepsilon-1)q-(\varepsilon-1)t}{\alpha}$ and $1 \le j' \le \frac{q-t}{\alpha}$.

Then we have

$$i \equiv q(j' + \frac{(\varepsilon-1)q-(\varepsilon-1)t}{\alpha}) \bmod n,$$

which is equivalent to

$$\begin{aligned} i &\equiv qj' + \frac{(\varepsilon-1)q^2-(\varepsilon-1)qt}{\alpha} \\ &\equiv qj' - \frac{(\varepsilon-1)tq+(\varepsilon-1)}{\alpha} \bmod n. \end{aligned}$$

Moreover,

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

It is in contradiction with $1 \le i \le \frac{tq-\alpha+1}{\alpha}$.

From the above discussion, the result follows. □

Theorem 3: Let $n = \frac{q^2+1}{\alpha}$, where q is an odd prime power with the form $q = \alpha m + t$, m is a positive integer, both α and $t \ge 2$ are positive integers such that $\alpha = t^2 + 1$. If $\mathcal{C}$ is a q^2-ary constacyclic code of length n with defining set $Z = \cup_{i=0}^{\delta} C_{n-(q+1)i}$ for $0 \le \delta \le \frac{tq-\alpha+1}{\alpha}$, then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 3, d; 1]]_q$, where $2 \le d \le \frac{2tq+2}{\alpha}$ is even.

Proof: From Lemma 3, we assume that the defining set of constacyclic code $\mathcal{C}$ is $Z = \cup_{i=0}^{\delta} C_{n-(q+1)i}$ for $0 \le \delta \le \frac{tq-\alpha+1}{\alpha}$, and then $\mathcal{C}$ is a constacyclic code with parameters $[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2\delta - 1, 2\delta + 2]_{q^2}$ from Propositions 1 and 2. The defining set of $\mathcal{C}$ can be divided into two mutually disjoint subsets, i.e., $Z = Z_0 \cup Z_1$, where $Z_0 = C_n$ and $Z_1 = \cup_{i=1}^{\delta} C_{n-(q+1)i}$ for $1 \le \delta \le \frac{tq-\alpha+1}{\alpha}$. Assume that 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 can see that $H_1H_1^{\dagger} = 0$. Moreover, we have $H_0H_1^{\dagger} = 0$, and $H_1H_0^{\dagger} = 0$ from

$$C_n \cap -q(\cup_{i=1}^{\delta} C_{n-(q+1)i}) = -q(C_n \cap (\cup_{i=1}^{\delta} C_{n-(q+1)i})) = \emptyset,$$

and then

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

Since $Z_0 \cap -qZ_0 = \{n\}$, it follows that $rank(H_0H_0^{\dagger}) = 1$. From Lemma 2, we have $c = 1$. Therefore, there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 3, d; 1]]_q$ from Theorem 1 and Proposition 3, where $2 \le d \le \frac{2tq+2}{\alpha}$ is even. □

Example 1: If $t = 7$ and $m = 3$, then $q = 157$ and $n = 493$. Hence, there exist entanglement-assisted quantum MDS codes that from Theorem 3 are listed in Table 1.

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

q	n	$[[n, k, d; c]]_q$
157	493	$[[493, 492, 2; 1]]_{157}$
157	493	$[[493, 488, 4; 1]]_{157}$
157	493	$[[493, 484, 6; 1]]_{157}$
157	493	$[[493, 480, 8; 1]]_{157}$
157	493	$[[493, 476, 10; 1]]_{157}$
157	493	$[[493, 472, 12; 1]]_{157}$
157	493	$[[493, 468, 14; 1]]_{157}$
157	493	$[[493, 464, 16; 1]]_{157}$
157	493	$[[493, 460, 18; 1]]_{157}$
157	493	$[[493, 456, 20; 1]]_{157}$
157	493	$[[493, 452, 22; 1]]_{157}$
157	493	$[[493, 448, 24; 1]]_{157}$
157	493	$[[493, 444, 26; 1]]_{157}$
157	493	$[[493, 440, 28; 1]]_{157}$
157	493	$[[493, 436, 30; 1]]_{157}$
157	493	$[[493, 432, 32; 1]]_{157}$
157	493	$[[493, 428, 34; 1]]_{157}$
157	493	$[[493, 424, 36; 1]]_{157}$
157	493	$[[493, 420, 38; 1]]_{157}$
157	493	$[[493, 416, 40; 1]]_{157}$
157	493	$[[493, 412, 42; 1]]_{157}$
157	493	$[[493, 408, 44; 1]]_{157}$

Theorem 4: Let $n = \frac{q^2+1}{\alpha}$, where q is an odd prime power with the form $q = \alpha m + t$, m is a positive integer, both

α and $t \geq 2$ are positive integers such that $\alpha = t^2 + 1$. If $\mathcal{C}$ is a q^2-ary constacyclic code of length n with defining set $Z = \cup_{i=0}^{\delta} C_{n-(q+1)i}$ for $\frac{tq+1}{\alpha} \leq \delta \leq \frac{(t+1)q-t(t+1)}{\alpha}$, then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 7, d; 5]]_q$, where $\frac{2tq+2\alpha+2}{\alpha} \leq d \leq \frac{2(t+1)q-2(t-1)}{\alpha}$ is even.

Proof: From Lemma 3, we assume that the defining set of constacyclic code $\mathcal{C}$ is given by $Z = \cup_{i=0}^{\delta} C_{n-(q+1)i}$ for $\frac{tq+1}{\alpha} \leq \delta \leq \frac{(t+1)q-t(t+1)}{\alpha}$, and then $\mathcal{C}$ is a constacyclic code with parameters $[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2\delta - 1, 2\delta + 2]_{q^2}$ from Propositions 1 and 2. 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 $Z_0 = C_n$, $Z_1 = \cup_{i=1}^{\frac{tq-\alpha+1}{\alpha}} C_{n-(q+1)i}$ and $Z_2 = \cup_{i=\frac{tq+1}{\alpha}}^{\delta} C_{n-(q+1)i}$. Assume that 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 3, we have $rank(H_0H_0^{\dagger}) = 1$, $H_0H_1^{\dagger} = 0$, $H_1H_0^{\dagger} = 0$ and $H_1H_1^{\dagger} = 0$, furthermore, $H_0H_2^{\dagger} = 0$ and $H_2H_0^{\dagger} = 0$ from

$$C_n \cap -q(\cup_{i=\frac{tq+1}{\alpha}}^{\delta} C_{n-(q+1)i}) = -q(C_n \cap (\cup_{i=\frac{tq+1}{\alpha}}^{\delta} C_{n-(q+1)i}) = \emptyset,$$

and then

$$HH^{\dagger} = \begin{pmatrix} H_0H_0^{\dagger} & 0 & 0 \\ 0 & 0 & H_1H_2^{\dagger} \\ 0 & H_2H_1^{\dagger} & H_2H_2^{\dagger} \end{pmatrix}.$$

In order to determine the number of entangled states of entanglement-assisted quantum codes, we discuss two cases as follows.

(1) $H_2H_2^{\dagger} = 0$. In fact, we only need to consider that $Z_2 \cap -qZ_2 = \emptyset$ from Lemma 1. If $Z_2 \cap -qZ_2 \neq \emptyset$, where $Z_2 = \cup_{i=1}^{\delta} C_{n-(q+1)(i+\frac{tq-\alpha+1}{\alpha})}$ with $1 \leq \delta \leq \frac{q-t}{\alpha}$, then there exist two integers i and j, where $1 \leq i, j \leq \frac{q-t}{\alpha}$, such that

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

for $k \in \{0, 1\}$.

If $k = 0$, then we have

$$qj + i \equiv \frac{t(t-1)q + t(t+1)}{\alpha} \bmod n,$$

and then

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

which is in contradiction with

$$qj + i \equiv \frac{t(t-1)q + t(t+1)}{\alpha} \bmod n.$$

If $k = 1$, then we have

$$qj \equiv i + \frac{t(t+1)q - t(t-1)}{\alpha} \bmod n.$$

When $j = 1$, then

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

which is in contradiction with

$$q \equiv i + \frac{t(t+1)q - t(t-1)}{\alpha} \bmod n.$$

For $1 \leq i \leq \frac{q-t}{\alpha}$, and $2 \leq j \leq \frac{q-t}{\alpha}$ (if $q = \alpha + t$, then we have $j = 1$, which has been discussed), we have

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

which is in contradiction with

$$qj \equiv i + \frac{t(t+1)q - t(t-1)}{\alpha} \bmod n.$$

(2) $rank(H_1H_2^\dagger) = rank(H_2H_1^\dagger) = 2$. We can assume that $Z_1 = \cup_{i=1}^{\frac{tq-\alpha+1}{\alpha}} C_{n-(q+1)i}$ can be divided into three defining sets which are

$$Z_{11} = \cup_{i=1}^{\frac{q-\alpha-t}{\alpha}} C_{n-(q+1)i},$$
$$Z_{12} = C_{n-(q+1)\frac{q-t}{\alpha}}$$

and

$$Z_{13} = \cup_{i=\frac{q+\alpha-t}{\alpha}}^{\frac{tq-\alpha+1}{\alpha}} C_{n-(q+1)i}.$$

Here, we only consider the case of $q > \alpha + t$, if $q = \alpha + t$, then we can use the same method to discuss that $Z_1 = \cup_{i=1}^{\frac{tq-\alpha+1}{\alpha}} C_{n-(q+1)i} = C_{n-(q+1)\frac{q-t}{\alpha}} \cup (\cup_{i=\frac{q+\alpha-t}{\alpha}}^{\frac{tq-\alpha+1}{\alpha}} C_{n-(q+1)i})$.

Therefore, the defining sets Z_{11}, Z_{12}, Z_{13} and Z_2 can generate constacyclic codes $\mathcal{C}_{11}, \mathcal{C}_{12}, \mathcal{C}_{13}$ and $\mathcal{C}_2$ respectively.

Let the parity check matrices of $\mathcal{C}_1, \mathcal{C}_{11}, \mathcal{C}_{12}, \mathcal{C}_{13}$ and $\mathcal{C}_2$ over F_{q^2} be H_1, H_{11}, H_{12}, H_{13} and H_2, respectively. Therefore,

$$H_1H_2^\dagger = \begin{pmatrix} H_{11}H_2^\dagger \\ H_{12}H_2^\dagger \\ H_{13}H_2^\dagger \end{pmatrix}.$$

Since

$$\begin{aligned} -qC_{n-(q+1)\frac{q-t}{\alpha}} &\cap (\cup_{i=\frac{tq+1}{\alpha}}^{\delta} C_{n-(q+1)i}) \\ &= C_{n-(q+1)\frac{tq+1}{\alpha}} \cap (\cup_{i=\frac{tq+1}{\alpha}}^{\delta} C_{n-(q+1)i}) \\ &= C_{n-(q+1)\frac{tq+1}{\alpha}}, \end{aligned}$$

in order to obtain $rank(H_1H_2^\dagger) = rank(H_2H_1^\dagger) = 2$, we have to show that $H_{11}H_2^\dagger = 0$ and $H_{13}H_2^\dagger = 0$ as follows.

(i) $H_{11}H_2^\dagger = 0$. In fact, it only need to show that

$$-q(\cup_{i=1}^{\frac{q-\alpha-t}{\alpha}} C_{n-(q+1)i}) \cap (\cup_{i=0}^{\delta} C_{n-(q+1)(i+\frac{tq+1}{\alpha})}) = \emptyset$$

from Lemma 1, where $0 \le \delta \le \frac{q-\alpha-t}{\alpha}$. Assume that there exist two integers i, j, $1 \le i \le \frac{q-\alpha-t}{\alpha}$ and $0 \le j \le \frac{q-\alpha-t}{\alpha}$, such that

$$-q(C_{n-(q+1)i}) \cap (C_{n-(q+1)(j+\frac{tq+1}{\alpha})}) \ne \emptyset.$$

Then we have

$$-q(n-(q+1)i)q^{2k} \equiv n-(q+1)(j+\frac{tq+1}{\alpha}) \bmod (q+1)n.$$

If $k = 0$, then

$$-q(n-(q+1)i) \equiv n-(q+1)(j+\frac{tq+1}{\alpha}) \bmod (q+1)n,$$

which is equivalent to

$$j + \frac{tq+1}{\alpha} + qi \equiv 0 \bmod n,$$

where $1 \le i \le \frac{q-\alpha-t}{\alpha}$ and $0 \le j \le \frac{q-\alpha-t}{\alpha}$. Since

$$\begin{aligned} 0 &< \frac{(\alpha+t)q+1}{\alpha} \\ &= q + \frac{tq+1}{\alpha} \\ &\le j + \frac{tq+1}{\alpha} + qi \\ &\le (q+1)\frac{q-\alpha-t}{\alpha} + \frac{tq+1}{\alpha} \\ &= \frac{q^2-(\alpha-1)q-t(t+1)}{\alpha} < n, \end{aligned}$$

it is in contradiction with $j + \frac{tq+1}{\alpha} + qi \equiv 0 \bmod n$.

If $k = 1$, then

$$-q^3(n-(q+1)i) \equiv n-(q+1)(j+\frac{tq+1}{\alpha}) \bmod (q+1)n,$$

which is equivalent to

$$j + \frac{tq+1}{\alpha} \equiv qi \bmod n,$$

where $1 \le i \le \frac{q-\alpha-t}{\alpha}$ and $0 \le j \le \frac{q-\alpha-t}{\alpha}$. Since

$$\begin{aligned} 0 &< \frac{tq+1}{\alpha} \\ &\le j + \frac{tq+1}{\alpha} \\ &\le \frac{(t+1)q-t(t+1)}{\alpha} < q, \end{aligned}$$

it is in contradiction with $q \le qi \le \frac{q^2-(\alpha+t)q}{\alpha}$.

(ii) $H_{13}H_2^\dagger = 0$. In fact, it only need to show that

$$(\cup_{i=1}^{\frac{(t-1)q-t(t-1)}{\alpha}} C_{n-(q+1)(i+\frac{q-t}{\alpha})}) \cap -q(\cup_{i=0}^{\delta} C_{n-(q+1)(i+\frac{tq+1}{\alpha})}) = \emptyset.$$

from Lemma 1, where $0 \le \delta \le \frac{q-\alpha-t}{\alpha}$. Assume that

$$(\cup_{i=1}^{\frac{(t-1)q-t(t-1)}{\alpha}} C_{n-(q+1)(i+\frac{q-t}{\alpha})}) \cap -q(\cup_{i=0}^{\delta} C_{n-(q+1)(i+\frac{tq+1}{\alpha})}) \ne \emptyset,$$

then there exist two integers i, j, where $0 \le j \le \frac{q-\alpha-t}{\alpha}$ and $1 \le i \le \frac{(t-1)q-t(t-1)}{\alpha}$ such that

$$n-(q+1)(i+\frac{q-t}{\alpha}) \equiv -q(n-(q+1)(j+\frac{tq+1}{\alpha}))q^{2k} \bmod (q+1)n$$

for $k \in \{0, 1\}$.

If $k = 0$, then

$$n-(q+1)(i+\frac{q-t}{\alpha}) \equiv -q(n-(q+1)(j+\frac{tq+1}{\alpha})) \bmod (q+1)n,$$

which is equivalent to

$$q(j+\frac{tq+1}{\alpha}) + (i+\frac{q-t}{\alpha}) \equiv 0 \bmod n,$$

i.e.,

$$qj + i + \frac{2q-2t}{\alpha} \equiv 0 \bmod n,$$

where $0 \leq j \leq \frac{q-\alpha-t}{\alpha}$ and $1 \leq i \leq \frac{(t-1)q-t(t-1)}{\alpha}$. Since

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

it is in contradiction with

$$qj + i + \frac{2q-2t}{\alpha} \equiv 0 \bmod n.$$

If $k = 1$, then

$$\begin{aligned} &n-(q+1)(i+\frac{q-t}{\alpha}) \\ &\qquad \equiv -q(n+(q+1)(j+\frac{tq+1}{\alpha})) \bmod (q+1)n, \end{aligned}$$

which is equivalent to

$$q(j+\frac{tq+1}{\alpha}) \equiv i + \frac{q-t}{\alpha} \bmod n,$$

i.e.,

$$qj \equiv i \bmod n,$$

where $0 \leq j \leq \frac{q-\alpha-t}{\alpha}$ and $1 \leq i \leq \frac{(t-1)q-t(t-1)}{\alpha}$. If $j = 0$, then $i = 0$, which is in contradiction with $1 \leq i \leq \frac{(t-1)q-t(t-1)}{\alpha}$. For $q \leq qj \leq \frac{q^2-\alpha q-tq}{\alpha} < n$, it is in contradiction with $1 \leq i \leq \frac{(t-1)q-t(t-1)}{\alpha}$.

Therefore, we have $rank(H_1H_2^\dagger) = 2$ and $rank(HH^\dagger) = 5$. Moreover, we have $c = 5$ from Lemma 2. From Theorem 1 and Proposition 3, there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 7, d; 5]]_q$, where $\frac{2tq+2\alpha+2}{\alpha} \leq d \leq \frac{2(t+1)q-2(t-1)}{\alpha}$ is even. □

Example 2: If $t = 7$ and $m = 3$, then $q = 157$ and $n = 493$. Additionally, Let $t = 7$ and $m = 5$, then $q = 257$ and $n = 1321$. Therefore, there exist entanglement-assisted quantum MDS code that from Theorem 4 are listed in Table 2.

Theorem 5: Let $n = \frac{q^2+1}{\alpha}$, where q is an odd prime power with the form $q = \alpha m + t$, m is a positive integer, both α and $t \geq 2$ are positive integers such that $\alpha = t^2 + 1$. Then we have the following results.

(1) If $\mathcal{C}$ is a q^2-ary constacyclic code of length n with defining set $Z = \cup_{i=0}^{\delta} C_{n-(q+1)i}$ for $\frac{3q-1}{5} \leq \delta \leq \frac{4q-8}{5}$ (i.e., $t = 2$), then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 11, d; 9]]_q$, where $\frac{6q+8}{5} \leq d \leq \frac{8q-6}{5}$ is even.

(2) If $\mathcal{C}$ is a q^2-ary constacyclic code of length n with defining set $Z = \cup_{i=0}^{\delta} C_{n-(q+1)i}$ for $\frac{(t+1)q-t+1}{\alpha} \leq \delta \leq \frac{(2t-1)q-\alpha+t+2}{\alpha}$ (here, $t \geq 3$), then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 11, d; 9]]_q$, where $\frac{(2t+2)q+2\alpha-2t+2}{\alpha} \leq d \leq \frac{(4t-2)q+2t+4}{\alpha}$ is even.

TABLE 2. Sample parameters of entanglement-assisted quantum MDS codes constructed from Theorem 4.

q	n	$[[n,k,d;c]]_q$
157	493	$[[493, 408, 46; 5]]_{157}$
157	493	$[[493, 404, 48; 5]]_{157}$
157	493	$[[493, 400, 50; 5]]_{157}$
257	1321	$[[1321, 1180, 74; 5]]_{257}$
257	1321	$[[1321, 1176, 76; 5]]_{257}$
257	1321	$[[1321, 1172, 78; 5]]_{257}$
257	1321	$[[1321, 1168, 80; 5]]_{257}$
257	1321	$[[1321, 1164, 82; 5]]_{257}$

Proof: Here, we only show the part (2) of this theorem, since the part (1) could be obtained by using the same method. From Lemma 3, the defining set of constacyclic code $\mathcal{C}$ is given by $Z = \cup_{i=0}^{\delta} C_{n-(q+1)i}$ for $\frac{(t+1)q-t+1}{\alpha} \leq \delta \leq \frac{(2t-1)q-\alpha+t+2}{\alpha}$. We can see that $\mathcal{C}$ is a constacyclic code with parameters $[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2\delta - 1, 2\delta + 2]_{q^2}$ from Propositions 1 and 2. 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 $Z_0 = C_n$, $Z_1 = \cup_{i=1}^{\frac{tq-\alpha+1}{\alpha}} C_{n-(q+1)i}$, $Z_2 = \cup_{i=\frac{tq+1}{\alpha}}^{\frac{(t+1)q-\alpha-t+1}{\alpha}} C_{n-(q+1)i}$ and $Z_3 = \cup_{i=\frac{(t+1)q-t+1}{\alpha}}^{\delta} C_{n-(q+1)i}$. Assume that 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

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

It is easy to see that $rank(H_0H_0^\dagger) = 1$, $rank(H_2H_1^\dagger) = rank(H_1H_2^\dagger) = 2$, $H_0H_1^\dagger = 0$, $H_0H_2^\dagger = 0$, $H_0H_3^\dagger = 0$ and $H_0H_4^\dagger = 0$, then

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

From the proof of Theorem 4, we have

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

In order to obtain

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

we discuss three cases as follows.

(1) $rank(H_1H_3^{\dagger}) = rank(H_3H_1^{\dagger}) = 2$. In fact, if $\delta = \frac{(t+1)q-t+1}{\alpha}$, we have

$$-qC_{n-(q+1)(\frac{(t+1)q-t+1}{\alpha})}\cap(\cup_{i=1}^{\frac{tq-t^2}{\alpha}}C_{n-(q+1)i}) = C_{n-(q+1)(\frac{(t-1)q+t+1}{\alpha})},$$

then $rank(H_1H_3^{\dagger}) = rank(H_3H_1^{\dagger}) = 2$. For $\frac{(t+1)q+\alpha-t+1}{\alpha} \le \delta \le \frac{(2t-1)q-\alpha+t+2}{\alpha}$, we have

$$\begin{aligned}&-q(\cup_{i=\frac{(t+1)q-t+1}{\alpha}}^{\delta}C_{n-(q+1)i})\cap(\cup_{i=1}^{\frac{tq-t^2}{\alpha}}C_{n-(q+1)i})\\ &= -q(\cup_{i=\frac{(t+1)q+\alpha-t+1}{\alpha}}^{\delta}C_{n-(q+1)i}\cup C_{n-(q+1)(\frac{(t+1)q-t+1}{\alpha})})\\ &\quad\cap(\cup_{i=1}^{\frac{tq-t^2}{\alpha}}C_{n-(q+1)i})\\ &= (-q(\cup_{i=\frac{(t+1)q+\alpha-t+1}{\alpha}}^{\delta}C_{n-(q+1)i})\cap(\cup_{i=1}^{\frac{tq-t^2}{\alpha}}C_{n-(q+1)i}))\\ &\quad\cup(C_{n-(q+1)(\frac{(t-1)q+t+1}{\alpha})}\cap(\cup_{i=1}^{\frac{tq-t^2}{\alpha}}C_{n-(q+1)i}))\\ &= (-q(\cup_{i=\frac{(t+1)q+\alpha-t+1}{\alpha}}^{\delta}C_{n-(q+1)i})\cap(\cup_{i=1}^{\frac{tq-t^2}{\alpha}}C_{n-(q+1)i}))\\ &\quad\cup C_{n-(q+1)(\frac{(t-1)q+t+1}{\alpha})}.\end{aligned}$$

In order to get that $rank(H_1H_3^{\dagger}) = rank(H_3H_1^{\dagger}) = 2$, we need to show that

$$-q(\cup_{i=\frac{(t+1)q+\alpha-t+1}{\alpha}}^{\delta}C_{n-(q+1)i})\cap(\cup_{i=1}^{\frac{tq-t^2}{\alpha}}C_{n-(q+1)i}) = \emptyset,$$

with $\frac{(t+1)q+\alpha-t+1}{\alpha} \le \delta \le \frac{(2t-1)q-\alpha+t+2}{\alpha}$, which is equivalent to

$$-q(\cup_{i=1}^{\delta}C_{n-(q+1)(i+\frac{(t+1)q-(t-1)}{\alpha})})\cap(\cup_{i=1}^{\frac{tq-t^2}{\alpha}}C_{n-(q+1)i}) = \emptyset$$

for $1 \le \delta \le \frac{(t-2)q-t(t-2)}{\alpha}$.

If

$$-q(\cup_{i=1}^{\delta}C_{n-(q+1)(i+\frac{(t+1)q-(t-1)}{\alpha})})\cap(\cup_{i=1}^{\frac{tq-t^2}{\alpha}}C_{n-(q+1)i}) \ne \emptyset,$$

then we assume that there exist two integers i, j, where $1 \le i \le \frac{(t-2)q-t(t-2)}{\alpha}$ and $1 \le j \le \frac{tq-t^2}{\alpha}$, such that

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

for $k \in \{0, 1\}$.

If $k = 0$, then it is equivalent to

$$qi+j-\frac{(t+1)+(t-1)q}{\alpha} \equiv 0 \bmod n.$$

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

$$\begin{aligned}0 &< \frac{(\alpha-t+1)q+\alpha-t-1}{\alpha}\\ &= q+1-\frac{(t+1)+(t-1)q}{\alpha}\\ &\le qi-\frac{(t+1)+(t-1)q}{\alpha}+j\\ &\le \frac{q^2-(t-1)q-t-\alpha}{\alpha} < n,\end{aligned}$$

which is in contradiction with $qi+j-\frac{(t+1)+(t-1)q}{\alpha} \equiv 0 \bmod n$.

(ii) When $\frac{q+\alpha-t}{\alpha} \le i \le \frac{2q-2t}{\alpha}$, and let $i' = i-\frac{q-t}{\alpha}$, we have $1 \le i' \le \frac{q-t}{\alpha}$. Then

$$q(i'+\frac{q-t}{\alpha})-\frac{(t+1)+(t-1)q}{\alpha}+j \equiv 0 \bmod n,$$

which is equivalent to $qi'-\frac{t+2+(2t-1)q}{\alpha}+j \equiv 0 \bmod n$, then we have

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

which is in contradiction with $qi'-\frac{t+2+(2t-1)q}{\alpha}+j \equiv 0 \bmod n$.

(iii) When $\frac{(\varepsilon-1)q+\alpha-(\varepsilon-1)t}{\alpha} \le i \le \frac{\varepsilon q-\varepsilon t}{\alpha}$, where $3 \le \varepsilon \le t-2$ (Here, if there exists $t \ge 5$), and let $i' = i-\frac{(\varepsilon-1)q-(\varepsilon-1)t}{\alpha}$, then $1 \le i' \le \frac{q-t}{\alpha}$. We have

$$q(i'+\frac{(\varepsilon-1)q-(\varepsilon-1)t}{\alpha})-\frac{(t+1)+(t-1)q}{\alpha}+j \equiv 0 \bmod n,$$

which is equivalent to $qi'-\frac{t+\varepsilon+(t-1+(\varepsilon-1)t)q}{\alpha}+j \equiv 0 \bmod n$, and then we have

$$\begin{aligned}0 &< \frac{(2t+2)q+\alpha-2t+2}{\alpha}\\ &\le \frac{(\alpha-t+1-(\varepsilon-1)t)q+\alpha-t-\varepsilon}{\alpha}\\ &= q+1-\frac{t+\varepsilon+(t-1+(\varepsilon-1)t)q}{\alpha}\\ &\le qi'-\frac{t+\varepsilon+(t-1+(\varepsilon-1)t)q}{\alpha}+j\end{aligned}$$

$$\leq \frac{q^2-tq}{\alpha} - \frac{t+\varepsilon+(t-1+(\varepsilon-1)t)q}{\alpha} + \frac{tq-t^2}{\alpha}$$
$$\leq \frac{q^2-(t-1+(\varepsilon-1)t)q-t^2-t-\varepsilon}{\alpha}$$
$$\leq \frac{q^2-(3t-1)q-t^2-t-3}{\alpha} < n,$$

which is in contradiction with $qi' - \frac{t+\varepsilon+(t-1+(\varepsilon-1)t)q}{\alpha} + j \equiv 0 \bmod n$.

If $k=1$, then we have

$$-q(n+(q+1)(i+\frac{(t+1)q-(t-1)}{\alpha})) \equiv n-(q+1)j \bmod (q+1)n,$$

which is equivalent to $qi - \frac{(t+1)+(t-1)q}{\alpha} - j \equiv 0 \bmod n$.

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

$$0 < \frac{(\alpha-2t+1)q+(t^2-t-1)}{\alpha}$$
$$= q - \frac{(t+1)+(t-1)q}{\alpha} - \frac{tq-t^2}{\alpha}$$
$$\leq qi - \frac{(t+1)+(t-1)q}{\alpha} - j$$
$$\leq \frac{q^2-(2t-1)q-(\alpha+t+1)}{\alpha} < n,$$

which is in contradiction with $qi - \frac{(t+1)+(t-1)q}{\alpha} - j \equiv 0 \bmod n$.

(ii) When $\frac{q+\alpha-t}{\alpha} \leq i \leq \frac{2q-2t}{\alpha}$, and let $i' = i - \frac{q-t}{\alpha}$, we have $1 \leq i' \leq \frac{q-t}{\alpha}$. We have

$$q(i' + \frac{q-t}{\alpha}) - \frac{(t+1)+(t-1)q}{\alpha} - j \equiv 0 \bmod n,$$

which is equivalent to $qi' - \frac{t+2+(2t-1)q}{\alpha} - j \equiv 0 \bmod n$, then we have

$$0 < \frac{(\alpha-3t+1)q+(t^2-t-2)}{\alpha}$$
$$= q - \frac{tq-t^2}{\alpha} - \frac{t+2+(2t-1)q}{\alpha}$$
$$\leq qi' - \frac{t+2+(2t-1)q}{\alpha} - j$$
$$\leq \frac{q^2-(3t-1)q-t-2-\alpha}{\alpha} < n,$$

which is in contradiction with $qi' - \frac{t+2+(2t-1)q}{\alpha} - j \equiv 0 \bmod n$.

(iii) When $\frac{(\varepsilon-1)q+\alpha-(\varepsilon-1)t}{\alpha} \leq i \leq \frac{\varepsilon q-\varepsilon t}{\alpha}$, where $3 \leq \varepsilon \leq t-2$ (Here, if there exists $t \geq 5$), and let $i' = i - \frac{(\varepsilon-1)q-(\varepsilon-1)t}{\alpha}$, we have $1 \leq i' \leq \frac{q-t}{\alpha}$. Additionally,

$$q(i' + \frac{(\varepsilon-1)q-(\varepsilon-1)t}{\alpha}) - \frac{(t+1)+(t-1)q}{\alpha} - j \equiv 0 \bmod n,$$

which is equivalent to $qi' - \frac{\varepsilon+t+(\varepsilon t-1)q}{\alpha} - j \equiv 0 \bmod n$.

For $1 \leq i' \leq \frac{q-t}{\alpha}$ and $1 \leq j \leq \frac{tq-t^2}{\alpha}$, we have

$$0 < \frac{(t+2)q+t^2-2t+2}{\alpha}$$
$$\leq \frac{(\alpha-\varepsilon t-t+1)q+t^2-\varepsilon-t}{\alpha}$$
$$= q - \frac{tq-t^2}{\alpha} - \frac{\varepsilon+t+(\varepsilon t-1)q}{\alpha}$$
$$\leq qi' - \frac{\varepsilon+t+(\varepsilon t-1)q}{\alpha} - j$$
$$\leq \frac{q^2-(\varepsilon t+t-1)q-\varepsilon-t-\alpha}{\alpha}$$
$$\leq \frac{q^2-(4t-1)q-3-t-\alpha}{\alpha} < n,$$

which is in contradiction with $qi' - \frac{\varepsilon+t+(\varepsilon t-1)q}{\alpha} - j \equiv 0 \bmod n$.

(2) $H_3H_2^\dagger = H_3H_2^\dagger = 0$. In fact, we need to show that

$$-q(\cup_{i=\frac{(t+1)q-t+1}{\alpha}}^{\delta} C_{n-(q+1)i}) \cap (\cup_{i=\frac{tq+1}{\alpha}}^{\frac{(t+1)q-t(t+1)}{\alpha}} C_{n-(q+1)i} = \emptyset,$$

which is equivalent to

$$-q(\cup_{i=0}^{\delta} C_{n-(q+1)(i+\frac{(t+1)q-t+1}{\alpha})}) \cap (\cup_{i=0}^{\frac{q-t-\alpha}{\alpha}} C_{n-(q+1)(i+\frac{tq+1}{\alpha})}) = \emptyset.$$

If

$$-q(\cup_{i=0}^{\delta} C_{n-(q+1)(i+\frac{(t+1)q-t+1}{\alpha})}) \cap (\cup_{i=0}^{\frac{q-t-\alpha}{\alpha}} C_{n-(q+1)(i+\frac{tq+1}{\alpha})}) = \emptyset,$$

then we assume that there exist two integers $0 \leq i \leq \frac{(t-2)q-t(t-2)}{\alpha}$ and $0 \leq j \leq \frac{q-\alpha-t}{\alpha}$ such that

$$-q(n-(q+1)(i+\frac{(t+1)q-(t-1)}{\alpha}))q^{2k} \equiv n-(q+1)(j+\frac{tq+1}{\alpha}) \bmod (q+1)n$$

for $k \in \{0, 1\}$.

If $k=0$, it is equivalent to $qi+j+\frac{q-t}{\alpha} \equiv 0 \bmod n$ for $0 \leq i \leq \frac{(t-2)q-(t-2)t}{\alpha}$ and $0 \leq j \leq \frac{q-\alpha-t}{\alpha}$.

(i) When $0 \leq i \leq \frac{q-t}{\alpha}$, we have

$$0 < \frac{q-t}{\alpha}$$
$$\leq qi + \frac{q-t}{\alpha} + j$$
$$\leq \frac{q^2-(t-2)q-\alpha-2t}{\alpha} < n,$$

which is in contradiction with $qi+j+\frac{q-t}{\alpha} \equiv 0 \bmod n$.

(ii) When $\frac{q+\alpha-t}{\alpha} \leq i \leq \frac{2q-2t}{\alpha}$, and let $i' = i - \frac{q-t}{\alpha}$, we have $1 \leq i' \leq \frac{q-t}{\alpha}$. We have

$$q(i' + \frac{q-t}{\alpha}) + j + \frac{q-t}{\alpha} \equiv 0 \bmod n,$$

which is equivalent to $qi' - \frac{(t-1)q+t+1}{\alpha} + j \equiv 0 \bmod n$, and then we have

$$0 < \frac{(\alpha-t+1)q-t-1}{\alpha}$$
$$= q - \frac{(t-1)q+t+1}{\alpha}$$
$$\leq qi' - \frac{(t-1)q+t+1}{\alpha} + j$$
$$\leq \frac{q^2-(2t-2)q-2t-1-\alpha}{\alpha} < n,$$

which is in contradiction with $qi' - \frac{(t-1)q+t+1}{\alpha} + j \equiv 0 \bmod n$.

(iii) When $\frac{(\varepsilon-1)q+\alpha-(\varepsilon-1)t}{\alpha} \leq i \leq \frac{\varepsilon q-\varepsilon t}{\alpha}$, where $3 \leq \varepsilon \leq t-2$ (Here, if there exists $t \geq 5$), and let $i' = i-\frac{(\varepsilon-1)q-(\varepsilon-1)t}{\alpha}$, we have $1 \leq i' \leq \frac{q-t}{\alpha}$. Additionally,

$$q(i' + \frac{(\varepsilon-1)q-(\varepsilon-1)t}{\alpha}) + j + \frac{q-t}{\alpha} \equiv 0 \bmod n,$$

which is equivalent to $qi' - \frac{((\varepsilon-1)t-1)q+(\varepsilon-1)+t}{\alpha} + j \equiv 0 \bmod n$, and then we have

$$\begin{aligned} 0 &< \frac{(3t+2)q-2t+3}{\alpha} \\ &\leq \frac{(\alpha-(\varepsilon-1)t+1)q-(\varepsilon-1)-t}{\alpha} \\ &= q - \frac{((\varepsilon-1)t-1)q+(\varepsilon-1)+t}{\alpha} \\ &\leq qi' - \frac{((\varepsilon-1)t-1)q+(\varepsilon-1)+t}{\alpha} + j \\ &\leq \frac{q^2-(\varepsilon t-2)q-(\varepsilon-1)-\alpha-2t}{\alpha} \\ &\leq \frac{q^2-(3\,t-2)q-2-\alpha-2t}{\alpha} < n, \end{aligned}$$

which is in contradiction with $qi' - \frac{((\varepsilon-1)t-1)q+(\varepsilon-1)+t}{\alpha} + j \equiv 0 \bmod n$.

If $k = 1$, we have

$$\begin{aligned} &-q(n+(q+1)(i+\frac{(t+1)q-(t-1)}{\alpha})) \\ &\qquad \equiv n-(q+1)(j+\frac{tq+1}{\alpha}) \bmod (q+1)n \end{aligned}$$

for $0 \leq i \leq \frac{(t-2)q-(t-2)t}{\alpha}$ and $0 \leq j \leq \frac{q-\alpha-t}{\alpha}$, which is equivalent to $qi \equiv j + \frac{(2t-1)q+t+2}{\alpha} \bmod n$.

(i) When $0 \leq i \leq \frac{q-t}{\alpha}$, for $i = 0$, we have $j = n - \frac{(2t-1)q+t+2}{\alpha} = \frac{q^2-(2t-1)q-t-1}{\alpha}$, which is in contradiction with $0 \leq j \leq \frac{q-\alpha-t}{\alpha}$. For $1 \leq i \leq \frac{q-t}{\alpha}$, we have

$$\begin{aligned} 0 &< \frac{(\alpha-2t)q+(\alpha-2)}{\alpha} \\ &= q - \frac{(2t-1)q+t+2}{\alpha} - \frac{q-\alpha-t}{\alpha} \\ &\leq qi - \frac{(2t-1)q+t+2}{\alpha} - j \\ &\leq \frac{q^2-(3t-1)q-t-2}{\alpha} < n, \end{aligned}$$

which is in contradiction with $qi \equiv j + \frac{(2t-1)q+t+2}{\alpha} \bmod n$.

(ii) When $\frac{q+\alpha-t}{\alpha} \leq i \leq \frac{2q-2t}{\alpha}$, and let $i' = i - \frac{q-t}{\alpha}$, we have $1 \leq i' \leq \frac{q-t}{\alpha}$. Additionally,

$$q(i' + \frac{q-t}{\alpha}) - \frac{(2t-1)q+t+2}{\alpha} - j \equiv 0 \bmod n,$$

which is equivalent to $qi' - \frac{(3t-1)q+t+3}{\alpha} - j \equiv 0 \bmod n$, and then we have

$$\begin{aligned} 0 &< \frac{(\alpha-3t)q+\alpha-3}{\alpha} \\ &= q - \frac{(3t-1)q+t+3}{\alpha} - \frac{q-\alpha-t}{\alpha} \\ &\leq qi' - \frac{(3t-1)q+t+3}{\alpha} - j \\ &\leq \frac{q^2-(4t-1)q-t-3}{\alpha} < n, \end{aligned}$$

which is in contradiction with $qi' - \frac{(3t-1)q+t+3}{\alpha} - j \equiv 0 \bmod n$.

(iii) When $\frac{(\varepsilon-1)q+\alpha-(\varepsilon-1)t}{\alpha} \leq i \leq \frac{\varepsilon q-\varepsilon t}{\alpha}$, where $3 \leq \varepsilon \leq t-2$ (Here, if there exists $t \geq 5$), and let $i' = i-\frac{(\varepsilon-1)q-(\varepsilon-1)t}{\alpha}$, we have $1 \leq i' \leq \frac{q-t}{\alpha}$. Additionally,

$$\begin{aligned} q(i' + \tfrac{(\varepsilon-1)q-(\varepsilon-1)t}{\alpha}) - \tfrac{(2t-1)q+t+2}{\alpha} - j \\ \equiv \qquad\qquad 0 \bmod n, \end{aligned}$$

which is equivalent to $qi' - \frac{\varepsilon+1+t+((\varepsilon+1)t-1)q}{\alpha} - j \equiv 0 \bmod n$, and then we have

$$\begin{aligned} 0 &< \frac{\alpha-t+3+(t+1)q}{\alpha} \\ &\leq \frac{\alpha-\varepsilon+1+(\alpha-(\varepsilon+1)t)q}{\alpha} \\ &= q - \frac{\varepsilon-1+t+((\varepsilon+1)t-1)q}{\alpha} - \frac{q-\alpha-t}{\alpha} \\ &\leq qi' - \frac{\varepsilon-1+t+((\varepsilon+1)t-1)q}{\alpha} - j \\ &\leq \frac{q^2-tq}{\alpha} - \frac{\varepsilon-1+t+((\varepsilon+1)t-1)q}{\alpha} \\ &\leq \frac{q^2-\varepsilon-t+1-((\varepsilon+2)t-1)q}{\alpha} \\ &\leq \frac{q^2-2-t-(5t-1)q}{\alpha} < n, \end{aligned}$$

which is in contradiction with $qi' - \frac{\varepsilon+1+t+((\varepsilon+1)t-1)q}{\alpha} - j \equiv 0 \bmod n$.

(3) We have $H_3H_3^{\dagger} = 0$. In fact, we need to show that

$$-q(\cup_{i=\frac{(t+1)q-t+1}{\alpha}}^{\delta} C_{n-(q+1)i}) \cap (\cup_{i=\frac{(t+1)q-t+1}{\alpha}}^{\delta} C_{n-(q+1)i}) = \emptyset,$$

which is equivalent to

$$\begin{aligned} &-q(\cup_{i=0}^{\delta} C_{n-(q+1)(i+\frac{(t+1)q-t+1}{\alpha})}) \\ &\qquad \cap(\cup_{i=0}^{\delta} C_{n-(q+1)(i+\frac{(t+1)q-t+1}{\alpha})}) = \emptyset. \end{aligned}$$

If

$$\begin{aligned} &-q(\cup_{i=0}^{\delta} C_{n-(q+1)(i+\frac{(t+1)q-t+1}{\alpha})}) \\ &\qquad \cap(\cup_{i=0}^{\delta} C_{n-(q+1)(i+\frac{(t+1)q-t+1}{\alpha})}) \neq \emptyset, \end{aligned}$$

we assume that there exist two integers i, j, where $0 \leq i, j \leq \frac{(t-2)q-(t-2)t}{\alpha}$ such that

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

for $k \in \{0, 1\}$.

If $k = 0$, then it is equivalent to $qi + \frac{2q-2t}{\alpha} + j \equiv 0 \bmod n$.

(i) When $0 \leq i \leq \frac{q-t}{\alpha}$, we have

$$0 < \frac{2q-2t}{\alpha}$$

$$\le qi + \frac{2q-2t}{\alpha} + j \le \frac{q^2-t^2}{\alpha} < n,$$

which is in contradiction with $qi + j + \frac{2q-2t}{\alpha} \equiv 0 \bmod n$.

(ii) When $\frac{q+\alpha-t}{\alpha} \le i \le \frac{2q-2t}{\alpha}$, and let $i' = i - \frac{q-t}{\alpha}$, then $1 \le i' \le \frac{q-t}{\alpha}$. We have

$$q(i' + \frac{q-t}{\alpha}) + j + \frac{2q-2t}{\alpha} \equiv 0 \bmod n,$$

which is equivalent to $qi' - \frac{(t-2)q+2t+1}{\alpha} + j \equiv 0 \bmod n$, and then we have

$$\begin{aligned} 0 &< \frac{(\alpha-t+2)q-2t-1}{\alpha} \\ &= q - \frac{(t-2)q+2t+1}{\alpha} \\ &\le qi' - \frac{(t-2)q+2t+1}{\alpha} + j \\ &\le \frac{q^2-tq-t^2-1}{\alpha} < n, \end{aligned}$$

which is in contradiction with $qi' - \frac{(t-2)q+2t+1}{\alpha} + j \equiv 0 \bmod n$.

(iii) When $\frac{(\varepsilon-1)q+\alpha-(\varepsilon-1)t}{\alpha} \le i \le \frac{\varepsilon q-\varepsilon t}{\alpha}$, where $3 \le \varepsilon \le t-2$ (Here, if there exists $t \ge 5$), and let $i' = i - \frac{(\varepsilon-1)q-(\varepsilon-1)t}{\alpha}$, we have $1 \le i' \le \frac{q-t}{\alpha}$. Additionally,

$$q(i' + \frac{(\varepsilon-1)q-(\varepsilon-1)t}{\alpha}) + j + \frac{2q-2t}{\alpha} \equiv 0 \bmod n,$$

which is equivalent to $qi' - \frac{((\varepsilon-1)t-2)q+(\varepsilon-1)+2t}{\alpha} + j \equiv 0 \bmod n$, and then we have

$$\begin{aligned} 0 &< \frac{(3t+3)q-3t+3}{\alpha} \\ &\le \frac{(\alpha-(\varepsilon-1)t+2)q-(\varepsilon-1)-2t}{\alpha} \\ &= q - \frac{((\varepsilon-1)t-2)q+(\varepsilon-1)+2t}{\alpha} \\ &\le qi' - \frac{((\varepsilon-1)t-2)q+(\varepsilon-1)+2t}{\alpha} + j \\ &\le \frac{q^2-(\varepsilon-1)tq-(\varepsilon-1)-t^2}{\alpha} \\ &\le \frac{q^2-2tq-2-t^2}{\alpha} < n, \end{aligned}$$

which is in contradiction with $qi' - \frac{((\varepsilon-1)t-2)q+(\varepsilon-1)+2t}{\alpha} + j \equiv 0 \bmod n$.

If $k = 1$, then we have

$$\begin{aligned} &-q(n + (q+1)(i + \frac{(t+1)q-(t-1)}{\alpha})) \\ &\equiv n - (q+1)(j + \frac{(t+1)q-(t-1)}{\alpha}) \bmod (q+1)n \end{aligned}$$

for $0 \le i, j \le \frac{(t-2)q-(t-2)t}{\alpha}$, which is equivalent to $qi \equiv j + \frac{2tq+2}{\alpha} \bmod n$.

(i) If $0 \le i \le \frac{q-t}{\alpha}$, for $i = 0$, we have $j = n - \frac{2tq+2}{\alpha} = \frac{q^2-2tq-1}{\alpha}$, which is in contradiction with $0 \le j \le \frac{(t-2)q-(t-2)t}{\alpha}$. For $1 \le i \le \frac{q-t}{\alpha}$, we have

$$\begin{aligned} 0 &< \frac{2tq+2}{\alpha} \\ &\le \frac{2tq+2}{\alpha} + j \\ &\le \frac{2tq+2}{\alpha} + \frac{(t-2)q-(t-2)t}{\alpha} \\ &\le \frac{(3t-2)q-t^2+2t+2}{\alpha} < q, \end{aligned}$$

which is in contradiction with $qi \equiv j + \frac{2tq+2}{\alpha} \bmod n$.

(ii) If $\frac{q+\alpha-t}{\alpha} \le i \le \frac{2q-2t}{\alpha}$, and let $i' = i - \frac{q-t}{\alpha}$, then $1 \le i' \le \frac{q-t}{\alpha}$. We have

$$q(i' + \frac{q-t}{\alpha}) - j - \frac{2tq+2}{\alpha} \equiv 0 \bmod n,$$

which is equivalent to $qi' - \frac{3tq+3}{\alpha} - j \equiv 0 \bmod n$, and then we have

$$\begin{aligned} 0 &< \frac{(\alpha-4t+2)q+t^2-2t-3}{\alpha} \\ &= q - \frac{3tq+3}{\alpha} - \frac{(t-2)q-(t-2)t}{\alpha} \\ &\le qi' - \frac{3tq+3}{\alpha} - j \\ &\le \frac{q^2-4tq-3}{\alpha} < n, \end{aligned}$$

which is in contradiction with $qi' - \frac{3tq+3}{\alpha} - j \equiv 0 \bmod n$.

(iii) If $\frac{(\varepsilon-1)q+\alpha-(\varepsilon-1)t}{\alpha} \le i \le \frac{\varepsilon q-\varepsilon t}{\alpha}$, where $3 \le \varepsilon \le t-2$ (Here, if there exists $t \ge 5$), and let $i' = i - \frac{(\varepsilon-1)q-(\varepsilon-1)t}{\alpha}$, then $1 \le i' \le \frac{q-t}{\alpha}$. We have

$$q(i' + \frac{(\varepsilon-1)q-(\varepsilon-1)t}{\alpha}) - \frac{2tq+2}{\alpha} - j \equiv 0 \bmod n,$$

which is equivalent to $qi' - \frac{(\varepsilon+1)tq+\varepsilon+1}{\alpha} - j \equiv 0 \bmod n$, and then we have

$$\begin{aligned} 0 &< \frac{3q+t^2-3t+1}{\alpha} \\ &\le \frac{(\alpha-\varepsilon t-2t+2)q+t^2-2t-\varepsilon-1}{\alpha} \\ &= q - \frac{(\varepsilon+1)tq+\varepsilon+1}{\alpha} - \frac{(t-2)q-(t-2)t}{\alpha} \\ &\le qi' - \frac{(\varepsilon+1)tq+\varepsilon+1}{\alpha} - j \\ &\le q\frac{q-t}{\alpha} - \frac{(\varepsilon+1)tq+\varepsilon+1}{\alpha} \\ &\le \frac{q^2-(\varepsilon+2)tq-\varepsilon-1}{\alpha} \\ &\le \frac{q^2-5tq-4}{\alpha} < n, \end{aligned}$$

which is in contradiction with $qi' - \frac{(\varepsilon+1)tq+\varepsilon+1}{\alpha} - j \equiv 0 \bmod n$.

Therefore, we have

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

and $rank(HH^{\dagger}) = 9$. From Theorem 1 and Proposition 3, there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 11, d; 9]]_q$, where $\frac{2(t+1)q+2\alpha-2t+2}{\alpha} \leq d \leq \frac{(4t-2)q+2t+4}{\alpha}$ is even. □

Example 3: If $t = 7$ and $m = 3$, then $q = 157$ and $n = 493$. Therefore, there exist entanglement-assisted quantum MDS code from Theorem 5 that are listed in Table 3.

TABLE 3. Sample parameters of entanglement-assisted quantum MDS codes constructed from Theorem 5.

q	n	$[[n, k, d; c]]_q$
157	493	$[[493, 400, 52; 9]]_{157}$
157	493	$[[493, 396, 54; 9]]_{157}$
157	493	$[[493, 392, 56; 9]]_{157}$
157	493	$[[493, 388, 58; 9]]_{157}$
157	493	$[[493, 384, 60; 9]]_{157}$
157	493	$[[493, 380, 62; 9]]_{157}$
157	493	$[[493, 376, 64; 9]]_{157}$
157	493	$[[493, 372, 66; 9]]_{157}$
157	493	$[[493, 368, 68; 9]]_{157}$
157	493	$[[493, 364, 70; 9]]_{157}$
157	493	$[[493, 360, 72; 9]]_{157}$
157	493	$[[493, 356, 74; 9]]_{157}$
157	493	$[[493, 352, 76; 9]]_{157}$
157	493	$[[493, 348, 78; 9]]_{157}$
157	493	$[[493, 344, 80; 9]]_{157}$
157	493	$[[493, 340, 82; 9]]_{157}$

When $n = \frac{q^2+1}{\alpha}$, where q is an odd prime power with the form $q = \alpha m + \alpha - t$, m is a positive integer, both α and $t \geq 2$ are positive integers such that $\alpha = t^2 + 1$, we have the following result of Theorem 6 by using the same method of Theorem 2. Moreover, based on Theorem 6, we can use the method of Theorems 3, 4 and 5 to get Theorem 7.

Theorem 6: Let $n = \frac{q^2+1}{\alpha}$, where q is an odd prime power with the form $q = \alpha m + \alpha - t$, m is a positive integer, both α and $t \geq 2$ are positive integers such that $\alpha = t^2 + 1$. If $\mathcal{C}$ is a constacyclic code whose defining set is given by $Z = \cup_{i=1}^{\delta} C_{n-(q+1)i}$, where $1 \leq \delta \leq \frac{tq-\alpha-1}{\alpha}$, then $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$.

Theorem 7: Let $n = \frac{q^2+1}{\alpha}$, where q is an odd prime power with the form $q = \alpha m + \alpha - t$, m is a positive integer, both α and $t \geq 2$ are positive integers such that $\alpha = t^2 + 1$. Then we have the following results.

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

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

(3) If $\mathcal{C}$ is a q^2-ary constacyclic code of length n with defining set $Z = \cup_{i=0}^{\delta} C_{n-(q+1)i}$ for $\frac{(t+1)q+t-1}{\alpha} \leq \delta \leq \frac{(2t-1)q-\alpha-t-2}{\alpha}$ (here, $t > 3$), then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 11, d; 9]]_q$, where $\frac{2(t+1)q+2(t-1)+2\alpha}{\alpha} \leq d \leq \frac{2(2t-1)q-2t-4}{\alpha}$. If $\mathcal{C}$ is a q^2-ary constacyclic code of length n with defining set $Z = \cup_{i=0}^{\delta} C_{n-(q+1)i}$ for $\frac{3q+1}{5} \leq \delta \leq \frac{4q-7}{5}$ (here, $t = 2$), then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 11, d; 9]]_q$, where $\frac{6q+12}{5} \leq d \leq \frac{8q-4}{5}$. If $\mathcal{C}$ is a q^2-ary constacyclic code of length n with defining set $Z = \cup_{i=0}^{\delta} C_{n-(q+1)i}$ for $\frac{4q+2}{10} \leq \delta \leq \frac{5q-5}{10}$ (here, $t = 3$), then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 11, d; 9]]_q$, where $\frac{8q+24}{10} \leq d \leq \frac{10q+10}{10}$.

Example 4: If $t = 7$ and $m = 3$, then $q = 193$ and $n = 745$. Then there exist some entanglement-assisted quantum MDS code that from Theorem 7 are listed in Table 4.

TABLE 4. Sample parameters of entanglement-assisted quantum MDS codes constructed from Theorem 7.

q	n	$[[n, k, d; c]]_q$
193	745	$[[745, 744, 2; 1]]_{193}$
193	745	$[[745, 740, 4; 1]]_{193}$
193	745	$[[745, 736, 6; 1]]_{193}$
...	...	...
193	745	$[[745, 648, 50; 1]]_{193}$
193	745	$[[745, 644, 52; 1]]_{193}$
193	745	$[[745, 640, 54; 1]]_{193}$
193	745	$[[745, 640, 56; 5]]_{193}$
193	745	$[[745, 636, 58; 5]]_{193}$
193	745	$[[745, 632, 60; 5]]_{193}$
193	745	$[[745, 628, 62; 5]]_{193}$
193	745	$[[745, 628, 64; 9]]_{193}$
193	745	$[[745, 624, 66; 9]]_{193}$
193	745	$[[745, 620, 68; 9]]_{193}$
...	...	...
193	745	$[[745, 564, 96; 9]]_{193}$
193	745	$[[745, 560, 98; 9]]_{193}$
193	745	$[[745, 556, 100; 9]]_{193}$

IV. CONCLUSION AND DISCUSSION

In this paper, we use constacyclic codes with length $\frac{q^2+1}{\alpha}$ to construct some classes of entanglement-assisted quantum MDS codes. When $\alpha = 5, 10$, we can see that the minimum distance of some entanglement-assisted quantum MDS codes constructed in this paper is larger than $\frac{q}{2} + 1$ or even $q + 1$. Furthermore, as the α increases, it becomes more and more difficult to search for the codes with the minimum distance that is larger than $\frac{q}{2} + 1$.

In Table 5, we give some families of entanglement-assisted quantum MDS codes available in [19], [26], [27] as well as the new families of entanglement-assisted quantum MDS codes constructed in this paper. We give the parameters

TABLE 5. Entanglement-assisted quantum MDS codes.

$[[n,k,d;c]]_q$	Range of parameters	d	Ref.
$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - \frac{6}{5}(q-7) - 4\lambda - 1, \frac{3}{5}(q-7)+2\lambda+4; 5]]_q$	q is an odd prime power with the form $q \equiv 7 \pmod{10}$ and $1 \le \lambda \le \frac{q+3}{10}$	$d = \frac{3}{5}(q-7)+2\lambda+4$ and $\frac{3q+9}{5} \le d \le \frac{4q+2}{5}$	[19]
$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - \frac{4}{5}(2q+1) - 4\lambda + 7, \frac{2}{5}(2q+1)+2\lambda+2; 9]]_q$	q is an odd prime power with the form $q \equiv 7 \pmod{10}$ and $1 \le \lambda \le \frac{q-7}{10}$	$d = \frac{2}{5}(2q+1)+2\lambda+2$ and $\frac{4q+22}{5} \le d \le \frac{5q+5}{5}$	[19]
$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - \frac{6}{5}(q-3) - 4\lambda + 3, \frac{3}{5}(q-3)+2\lambda+2; 5]]_q$	q is an odd prime power with the form $q \equiv 3 \pmod{10}$ and $1 \le \lambda \le \frac{q-3}{10}$	$d = \frac{3}{5}(q-3)+2\lambda+2$ and $\frac{3q+11}{5} \le d \le \frac{4q-2}{5}$	[19]
$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - \frac{8}{5}(q-3) - 4\lambda + 7, \frac{4}{5}(q-3)+2\lambda+2; 9]]_q$	q is an odd prime power with the form $q \equiv 3 \pmod{10}$ and $1 \le \lambda \le \frac{q-3}{10}$	$d = \frac{4}{5}(q-3)+2\lambda+2$ and $\frac{4q+8}{5} \le d \le \frac{5q-5}{5}$	[19]
$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - 2d + 3, d; 1]]_q$	q is an odd prime power with the form $q = 10m+3$, m is a positive integer	$2 \le d \le 6m+2$ and d is even.	[26]
$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - 2d + 3, d; 1]]_q$	q is an odd prime power with the form $q = 10m+7$, m is a positive integer	$2 \le d \le 6m+4$ and d is even	[26]
$[[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 3, d; 1]]_q$	q is an odd prime power with the form $q = 10m+3$, $m = 2\chi$ is an even, and χ is a positive integer	$2 \le d \le 8m+2$ and d is an even	[27]
$[[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 7, d; 5]]_q$	q is an odd prime power with the form $q = 10m+3$, $m = 2\chi$ is an even, and χ is a positive integer	$8m+4 \le d \le 12m+4$ and d is an even	[27]
$[[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 3, d; 1]]_q$	q is an odd prime power with the form $q = 10m+7$, $m = 2\chi$ is an even, and χ is a positive integer	$2 \le d \le 8m+6$ and d is an even	[27]
$[[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 7, d; 5]]_q$	q is an odd prime power with the form $q = 10m+7$, $m = 2\chi$ is an even, and χ is a positive integer	$8m+8 \le d \le 12m+8$ and d is an even	[27]

TABLE 5. *(Continued.)* **Entanglement-assisted quantum MDS codes.**

$[[n, k, d; c]]_q$	Range of parameters	d	Ref.
$[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 3, d; 1]]_q$	q is an odd prime power with the form $q = \alpha m + t$, m is a positive integer, α and $t \geq 2$ are positive integers such that $\alpha = t^2 + 1$	$2 \leq d \leq \frac{2tq+2}{\alpha}$ and d is even	Theorem 3
$[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 7, d; 5]]_q$	q is an odd prime power with the form $q = \alpha m + t$, m is a positive integer, α and $t \geq 2$ are positive integers such that $\alpha = t^2 + 1$	$\frac{2tq+2+2\alpha}{\alpha} \leq d \leq \frac{2(t+1)q-2(t-1)}{\alpha}$ and d is even	Theorem 4
$[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 11, d; 9]]_q$	q is an odd prime power, with the form $q = \alpha m + t$, m is a positive integer, α and $t \geq 2$ are positive integers such that $\alpha = t^2 + 1$	$\frac{2(t+1)q-2(t-1)+2\alpha}{\alpha} \leq d \leq \frac{2(2t-1)q+2t+4}{\alpha}$ with $t \geq 3$ and d is even, $\frac{6q+8}{5} \leq d \leq \frac{8q-6}{5}$ with $t = 2$ and d is even	Theorem 5
$[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 3, d; 1]]_q$	q is an odd prime power, with the form $q = \alpha m + \alpha - t$, m is a positive integer, α and $t \geq 2$ are positive integers such that $\alpha = t^2 + 1$	$2 \leq d \leq \frac{2tq-2}{\alpha}$ and d is even	Theorem 7
$[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 7, d; 5]]_q$	q is an odd prime power, with the form $q = \alpha m + \alpha - t$, m is a positive integer, α and $t \geq 2$ are positive integers such that $\alpha = t^2 + 1$	$\frac{2tq-2+2\alpha}{\alpha} \leq d \leq \frac{2(t+1)q+2(t-1)}{\alpha}$ and d is even	Theorem 7
$[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 11, d; 9]]_q$	q is an odd prime power, with the form $q = \alpha m + \alpha - t$, m is a positive integer, α and $t \geq 2$ are positive integers such that $\alpha = t^2 + 1$	$\frac{2(t+1)q+2(t-1)+2\alpha}{\alpha} \leq d \leq \frac{2(2t-1)q-2t-4}{\alpha}$ with $t > 3$ and d is even, $\frac{6q+12}{5} \leq d \leq \frac{8q-4}{5}$ with $t = 2$ and d is even, $\frac{8q+24}{10} \leq d \leq \frac{10q+10}{10}$ with $t = 3$ and d is even	Theorem 7

$[[n, k, d; c]]_q$ 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 fourth column.

In [19], when $s = \frac{q^2+1}{2}$, there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - \frac{4}{5}(2q+1) - 4\lambda + 7, \frac{2}{5}(2q+1) + 2\lambda + 2; 9]]_q$, where q is an odd prime power with the form $q \equiv 7 (\mathrm{mod}\ 10)$ and $1 \leq \lambda \leq \frac{q+3}{10}$. Here, the range of λ should be $1 \leq \lambda \leq \frac{q-7}{10}$. In fact, if $\lambda = \frac{q+3}{10}$, $-qC_{s-(q+1)(\frac{2q+1}{5}+\lambda)} = -qC_{s-(q+1)(\frac{q+1}{2})} = C_{s-(q+1)\frac{q-1}{2}}$, then the required number of entangled states is 13.

Compared with the entanglement-assisted quantum MDS codes constructed from [19], [26] and [27], the ones constructed in this paper are more general. From Table 5, the range of d of some codes constructed in [19], [26] are included in the results of this paper. Additionally, in [27], when q is an odd prime power in the form of $20\chi + 3$ with a positive integer χ, and then there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 3, d; 1]]_q$ and $[[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 7, d; 5]]_q$, whose minimum distance is even and the range of the ones are $2 \leq d \leq 16\chi+2$ and $16\chi + 4 \leq d \leq 24\chi + 4$ respectively. The minimum distance can be transformed to $2 \leq d \leq \frac{4q-2}{5}$ and $\frac{4q+8}{5} \leq d \leq \frac{6q+2}{5}$ respectively and the minimum distance is even. From Theorem 7, we have entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 3, d; 1]]_q$ where $2 \leq d \leq \frac{4q-2}{5}$ is even, and $[[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 7, d; 5]]_q$ where $\frac{4q+8}{5} \leq d \leq \frac{6q+2}{5}$ is even. Moreover, when q is an odd prime power in the form of $20\chi + 7$ with a positive integer χ, there exist entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 3, d; 1]]_q$ where $2 \leq d \leq 16\chi + 6$ is even, and $[[\frac{q^2+1}{\alpha}, \frac{q^2+1}{\alpha} - 2d + 7, d; 5]]_q$ where $16\chi+8 \leq d \leq 24\chi+8$ is even. The minimum distance can be transformed to $2 \leq d \leq \frac{4q+2}{5}$ and $\frac{4q+12}{5} \leq d \leq \frac{6q-2}{5}$ respectively and the minimum distance d is even. From Theorems 3 and 4, we have entanglement-assisted quantum MDS codes with parameters $[[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 3, d; 1]]_q$ where $2 \leq d \leq \frac{4q+2}{5}$ is even, and $[[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 7, d; 5]]_q$ where $\frac{4q+12}{5} \leq d \leq \frac{6q-2}{5}$ is even. Therefore, entanglement-assisted quantum MDS codes of length $\frac{q^2+1}{5}$ listed in Table 5 of [27] are included in this paper.

Although the number of pre-shared entangled states is fixed relative to the codes of [11], [28], entanglement-assisted quantum MDS codes with different lengths in this paper are got in the Hermitian case that not covered in [11], [28]. In order to get more entanglement-assisted quantum MDS with flexible entangled states, we will use combinatorial method or computer search algorithm to obtain them in the future work. Moreover, how to determine the minimum required number of pre-shared entangled states to make some entanglement-assisted quantum MDS codes constructed from other constacyclic codes with better parameters is still an interesting topic.

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] 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.

[10] 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.

[11] 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

[12] 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.

[13] 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.

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

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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

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

[21] 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.

[22] R.-H. 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. (Natural Sci. Ed.)*, vol. 12, no. 1, pp. 87–89, 2011.

[23] Y. Liu, R. Li, L. Lv, and Y. Ma, "Application of constacyclic codes to entanglement-assisted quantum maximum distance separable codes," *Quantum Inf. Process.*, vol. 17, no. 8, p. 210, 2018.

[24] L. Lu, 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

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

[26] L. Lu, 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.

[27] L. Lu, 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.

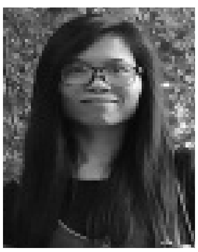
[28] G. Luo, X. Cao, and X. Chen, "MDS codes with hulls of arbitrary dimensions and their quantum error correction," *IEEE Trans. Inf. Theory*, vol. 65, no. 5, pp. 2944–2952, May 2019.

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

[30] 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.

[31] J. Qian and L. Zhang, "New optimal subsystem codes," *Discrete Math.*, vol. 313, pp. 2451–2455, Nov. 2013.
[32] 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.
[33] J. Qian and L. Zhang, "Improved constructions for quantum maximum distance separable codes," *Quantum Inf. Process.*, vol. 16, no. 1, p. 20, 2017.
[34] 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.
[35] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A, Gen. Phys.*, vol. 52, pp. R2493–R2496, Oct. 1995.
[36] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman, "Asymptotically good quantum codes," *Phys. Rev. A, Gen. Phys.*, vol. 63, no. 3, 2001, Art. no. 032311.
[37] 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.
[38] L. Wang and S. Zhu, "New quantum MDS codes derived from constacyclic codes," *Quantum Inf. Process.*, vol. 14, no. 3, pp. 881–889, 2015.
[39] 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.
[40] G. Zhang and B. Chen, "New quantum MDS codes," *Int. J. Quantum Inf.*, vol. 12, no. 4, 2014, Art. no. 1450019.
[41] 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.
[42] 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. 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.

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 the University of Washington, Seattle, USA, for 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 an 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.