International Journal of Theoretical Physics (2022) 61:247
https://doi.org/10.1007/s10773-022-05230-7

On the Constructions of Entanglement-Assisted Quantum MDS Codes

Sujuan Huang[1] · Shixin Zhu[1]

Received: 3 August 2022 / Accepted: 27 September 2022 / Published online: 8 October 2022

Abstract

Entanglement-assisted quantum error-correcting codes, which is a generalization of quantum error-correcting codes, could be derived from any classical codes by utilizing pre-shared entangled states between the sender and the receiver. In this paper, we construct some entanglement-assisted quantum maximum-distance-separable (EAQMDS) codes from constacyclic codes and cyclic codes by exploiting less pre-shared entangled states, respectively. Most of these codes are new in the sense that their parameters are not covered by the codes available in the literature. In particular, we extend the results in Tian et al. (Int. J. Theor. Phys. **60**, 1843–1857, 2021) to more general case.

Keywords Entanglement-assisted quantum error-correcting codes · Constacyclic codes · Cyclic codes · Cyclotomic cosets

Mathematics subject classification (2010) 94B15 · 94B65

1 Introduction

Quantum error-correcting(QEC) codes were introduced to preserve coherent states against noise and other unwanted interactions in quantum computation and quantum communication. Given a prime power q, an $[[n,k,d]]_q$ QEC code is a q^k-dimensional vector subspace of the Hilbert space $(\mathbb{C}^q)^{\otimes n} \cong \mathbb{C}^{q^n}$ with minimum distance d, which can detect up to $d-1$ quantum errors and correct up to $\lfloor \frac{d-1}{2} \rfloor$ quantum errors. As we know, QEC codes can be constructed from classical linear codes with certain self-orthogonality properties. However, self-orthogonal conditions of some famous codes, such as LDPC codes and Turbo codes are hard to determine. In 2006, a more general framework named entanglement-assisted stabilizer formalism was introduced [2, 19], the related codes are called entanglement-assisted quantum error-correcting(EAQEC) codes, which can increase the communication capacity and can be contructed from any classical

✉ Sujuan Huang
huangsujuan1019@163.com

Shixin Zhu
zhushixin@hfut.edu.cn

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

linear codes without self-orthogonality properties by utilizing pre-shared entanglement between the sender and the receiver. After that, many EAQEC codes with good parameters have been constructed. (Please see, for example, [8, 10, 11, 16, 24–27, 33, 44] and the relevant references therein).

Assume that q is a prime power. A q-ary EAQEC code encodes k information qudits into n channel qudits by utilizing c pairs of maximally entangled states, denoted by $[[n,k,d;c]]_q$, can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors, where d is the minimum distance of the EAQEC code. Actually, if $c=0$, it is indeed the standard $[[n,k,d]]_q$ QEC code. In this paper, QEC codes are also regarded as EAQEC codes. Similar to QEC codes, the parameters of EAQEC codes are mutually restricted, and there is an entanglement-assisted (EA) quantum Singleton bound for EAQEC codes.

Theorem 1 [1, 2, 14, 24] *Assume that* Q *is an* $[[n,k,d;c]]_q$ *EAQEC code. If* $d \leqslant \frac{n+2}{2}$, *then*

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

where $0 \leqslant c \leqslant n-1$.

If $c=0$, it is the quantum Singleton bound and a QEC code achieving this bound is called a quantum MDS code. When $d \leqslant \frac{n+2}{2}$, an $[[n,k,d;c]]_q$ EAQEC code achieving such bound is called an EAQMDS code. Recently, for $d > \frac{n+2}{2}$, Grassl [13] gave some examples of EAQEC codes with parameters beating such bound. A difficulty in the construction of EAQEC codes is to determine the number of maximally entangled states. There are two main techniques to find such number for present. One is through computing the hull dimension of linear codes [15], and the other is through decomposing the defining sets of constacyclic codes [6, 31]. When the number of maximally entangled states c is fixed, EAQMDS codes are optimal in the sense that they have the largest minimum distance. So far, many families of EAQMDS codes have been constructed from LCD codes [39], k-Galois dual codes [30], generalized Reed-Solomon codes and Goppa codes [3, 9, 12, 28, 36, 37], etc.

Due to the rich algebraic structure and efficient encoding and decoding circuits, constacyclic codes including cyclic codes and negacyclic codes are preferred objects on the construction of EAQMDS codes and many EAQMDS codes have been constructed from them. Among the obtained results, the lengths of these EAQMDS codes divide q^2-1 (Please see, for example, [6, 29, 31, 32, 34, 35, 41]) or q^2+1 (Please see, for example, q^2+1 in [6, 35, 40, 41]; $\frac{q^2+1}{2}$ in [6, 45]; $\frac{q^2+1}{5}$ in [7, 21, 34, 45]; $\frac{q^2+1}{10}$ in [21, 35, 45]; $\frac{q^2+1}{13}$ in [21, 43]; $\frac{q^2+1}{17}$ in [21], etc). Recently, Chen et al. [4, 5] constructed some families of EAQMDS codes of length $\frac{q^2+1}{a}$, where $a=t^2+1$ and $t \geqslant 2$ is a positive integer, which can be seen as the generalization of EAQMDS codes of lengths $\frac{q^2+1}{5}$, $\frac{q^2+1}{10}$ and $\frac{q^2+1}{17}$. Concrete parameters of already known EAQMDS codes of lengths $\frac{q^2+1}{5}$ and $\frac{q^2+1}{13}$ are listed in Table 1, which will be used in the sequel.

In this paper, through the analysis of the intersection of the defining set $\mathscr{Z}$ of constacyclic codes (including cyclic codes) and $-q\mathscr{Z}$, we obtain some families of EAQMDS codes of length $\frac{q^2+1}{\rho}$, where $\rho=a^2+(a+1)^2$ and $a \geqslant 2$ is a positive integer. It can be easily derived that there are very little even prime power q to satisfy $\frac{q^2+1}{\rho}$ to be an integer, except for $\rho=5$, which had already been extensively studied in [5, 7, 21] (Please see Table 1). Hence, here we only consider q being an odd prime power, and $a \geqslant 2$. The concrete parameters of the EAQMDS codes constructed in this paper are listed in Table 2.

Table 1 Known entanglement-assisted quantum MDS codes of lengths $\frac{q^2+1}{5}$ and $\frac{q^2+1}{13}$

q	Parameters $[[n,k,d;c]]_q$	d	References
$10m+2$	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+6,d;4]]_q$	$6m+3\leqslant d\leqslant 10m+3$ is odd	[5, 7, 21]
	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+3,d;1]]_q$	$2\leqslant d\leqslant 8m+2$ is even	[5]
	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+7,d;5]]_q$	$8m+4\leqslant d\leqslant 12m+2$ is even	
$10m+8$	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+6,d;4]]_q$	$6m+7\leqslant d\leqslant 10m+9$ is odd	[5, 7, 21]
	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+3,d;1]]_q$	$2\leqslant d\leqslant 8m+6$ is even	[5]
	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+7,d;5]]_q$	$8m+8\leqslant d\leqslant 12m+10$ is even	
$20m+3$	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+6,d;4]]_q$	$12m+4\leqslant d\leqslant 20m+4$ is even	[7]
$20m+7$	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+6,d;4]]_q$	$12m+6\leqslant d\leqslant 20m+8$ is even	[7]
$10m+3$	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+6,d;4]]_q$	$4m+3\leqslant d\leqslant 6m+1$ is odd	[34]
m odd		$6m+4\leqslant d\leqslant 10m+4$ is even	
m even	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+3,d;1]]_q$	$2\leqslant d\leqslant 8m+2$ is even	
	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+6,d;4]]_q$	$4m+3\leqslant d\leqslant 6m+1$ is odd	
	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+7,d;5]]_q$	$8m+4\leqslant d\leqslant 12m+4$ is even	
$10m+7$	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+6,d;4]]_q$	$8m+7\leqslant d\leqslant 14m+11$ is odd	[34]
m odd		$6m+6\leqslant d\leqslant 10m+8$ is even	
m even	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+3,d;1]]_q$	$2\leqslant d\leqslant 8m+6$ is even	
	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+6,d;4]]_q$	$8m+7\leqslant d\leqslant 14m+11$ is odd	
	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+7,d;5]]_q$	$8m+8\leqslant d\leqslant 12m+8$ is even	
$10m+3$	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+3,d;1]]_q$	$2\leqslant d\leqslant 8m+2$ is even	[4, 45]
	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+7,d;5]]_q$	$8m+4\leqslant d\leqslant 12m+4$ is even	
	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+11,d;9]]_q$	$12m+6\leqslant d\leqslant 16m+4$ is even	[4]
$10m+7$	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+3,d;1]]_q$	$2\leqslant d\leqslant 8m+6$ is even	[4, 45]
	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+7,d;5]]_q$	$8m+8\leqslant d\leqslant 12m+8$ is even	
	$[[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+11,d;9]]_q$	$12m+10\leqslant d\leqslant 16m+10$ is even	[4]
$13m+5$	$[[\frac{q^2+1}{13},\frac{q^2+1}{13}-2d+6,d;4]]_q$	$\frac{3}{5}(q-2)+3\leqslant d\leqslant q+1$	[21]
q even			
$26m+5$	$[[\frac{q^2+1}{13},\frac{q^2+1}{13}-2d+6,d;4]]_q$	$10m+4\leqslant d\leqslant 18m+4$ is even	[43]
	$[[\frac{q^2+1}{13},\frac{q^2+1}{13}-2d+10,d;8]]_q$	$18m+6\leqslant d\leqslant 22m+4$ is even	
	$[[\frac{q^2+1}{13},\frac{q^2+1}{13}-2d+3,d;1]]_q$	$2\leqslant d\leqslant 12m+2$ is even	
	$[[\frac{q^2+1}{13},\frac{q^2+1}{13}-2d+7,d;5]]_q$	$12m+4\leqslant d\leqslant 20m+4$ is even	
	$[[\frac{q^2+1}{13},\frac{q^2+1}{13}-2d+11,d;9]]_q$	$20m+6\leqslant d\leqslant 24m+4$ is even	
$26m+21$	$[[\frac{q^2+1}{13},\frac{q^2+1}{13}-2d+6,d;4]]_q$	$10m+10\leqslant d\leqslant 18m+14$ is even	[43]
	$[[\frac{q^2+1}{13},\frac{q^2+1}{13}-2d+10,d;8]]_q$	$18m+16\leqslant d\leqslant 22m+18$ is even	
	$[[\frac{q^2+1}{13},\frac{q^2+1}{13}-2d+3,d;1]]_q$	$2\leqslant d\leqslant 12m+10$ is even	
	$[[\frac{q^2+1}{13},\frac{q^2+1}{13}-2d+7,d;5]]_q$	$12m+12\leqslant d\leqslant 20m+16$ is even	
	$[[\frac{q^2+1}{13},\frac{q^2+1}{13}-2d+11,d;9]]_q$	$20m+18\leqslant d\leqslant 24m+20$ is even	

Table 2 Obtained entanglement-assisted quantum MDS codes of length $\frac{q^2+1}{\rho}$

q	Parameters $[[n,k,d;c]]_q$	d
$2\rho m+2a+1$	$[[\frac{q^2+1}{\rho},\frac{q^2+1}{\rho}-2d+2,d]]_q$	$2\leqslant d\leqslant\frac{(2a+1)q+1}{\rho}$ is even
	$[[\frac{q^2+1}{\rho},\frac{q^2+1}{\rho}-2d+6,d;4]]_q$	$\frac{(2a+1)q+1}{\rho}+2\leqslant d\leqslant\frac{(4a+1)q+2a+3}{\rho}$ is even
	$[[\frac{q^2+1}{\rho},\frac{q^2+1}{\rho}-2d+10,d;8]]_q$	$\frac{(4a+1)q+2a+3}{\rho}+2\leqslant d\leqslant\frac{(4a+3)q-2a+1}{\rho}$ is even
	$[[\frac{q^2+1}{\rho},\frac{q^2+1}{\rho}-2d+3,d;1]]_q$	$2\leqslant d\leqslant\frac{(2a+2)q-2a}{\rho}$ is even
	$[[\frac{q^2+1}{\rho},\frac{q^2+1}{\rho}-2d+7,d;5]]_q$	$\frac{(2a+2)q-2a}{\rho}+2\leqslant d\leqslant\frac{(4a+2)q+2}{\rho}$ is even
	$[[\frac{q^2+1}{\rho},\frac{q^2+1}{\rho}-2d+11,d;9]]_q$	$\frac{(4a+2)q+2}{\rho}+2\leqslant d\leqslant\frac{(4a+4)q-4a}{\rho}$ is even
$2\rho m-2a-1$	$[[\frac{q^2+1}{\rho},\frac{q^2+1}{\rho}-2d+2,d]]_q$	$2\leqslant d\leqslant\frac{(2a+1)q-1}{\rho}$ is even
	$[[\frac{q^2+1}{\rho},\frac{q^2+1}{\rho}-2d+6,d;4]]_q$	$\frac{(2a+1)q-1}{\rho}+2\leqslant d\leqslant\frac{(4a+1)q-2a-3}{\rho}$ is even
	$[[\frac{q^2+1}{\rho},\frac{q^2+1}{\rho}-2d+10,d;8]]_q$	$\frac{(4a+1)q-2a-3}{\rho}+2\leqslant d\leqslant\frac{(4a+3)q+2a-1}{\rho}$ is even
	$[[\frac{q^2+1}{\rho},\frac{q^2+1}{\rho}-2d+3,d;1]]_q$	$2\leqslant d\leqslant\frac{(2a+2)q+2a}{\rho}$ is even
	$[[\frac{q^2+1}{\rho},\frac{q^2+1}{\rho}-2d+7,d;5]]_q$	$\frac{(2a+2)q+2a}{\rho}+2\leqslant d\leqslant\frac{(4a+2)q-2}{\rho}$ is even
	$[[\frac{q^2+1}{\rho},\frac{q^2+1}{\rho}-2d+11,d;9]]_q$	$\frac{(4a+2)q-2}{\rho}+2\leqslant d\leqslant\frac{(4a+4)q+4a}{\rho}$ is even

The paper is organized as follows. In Section 2, some notations and basic results of constacyclic codes and EAQEC codes are presented. In Sections 3 and 4, some families of EAQMDS codes with small pre-shared entangled states are derived from constacyclic codes and cyclic codes, respectively. The conclusion is given in Section 5.

2 Preliminaries

Let $\mathbb{F}_{q^2}$ be the Galois field with q^2 elements, where q is a prime power. A q^2-ary linear code $\mathscr{C}$ of length n with dimension k and minimum distance d, denoted by $[n,k,d]_{q^2}$, is a linear subspace of $\mathbb{F}_{q^2}^n$ and its parameters satisfy the well-known Singleton bound: $d\leqslant n-k+1$. If $d=n-k+1$, then $\mathscr{C}$ is called a maximun distance separable (MDS) code. For two vectors $\mathbf{x}=(x_0,x_1,\ldots,x_{n-1})$, and $\mathbf{y}=(y_0,y_1,\ldots,y_{n-1})\in\mathbb{F}_{q^2}^n$, define their Hermitian inner product as

$$\langle\mathbf{x},\mathbf{y}\rangle:=x_0y_0^q+x_1y_1^q+\cdots+x_{n-1}y_{n-1}^q.$$

The vectors $\mathbf{x}$ and $\mathbf{y}$ are called orthogonal with respect to the Hermitian inner product if $\langle\mathbf{x},\mathbf{y}\rangle=0$. For a q^2-ary linear code $\mathscr{C}$, its Hermitian dual code $\mathscr{C}^{\perp_H}$ is defined as

$$\mathscr{C}^{\perp_H}:=\{\mathbf{x}\in\mathbb{F}_{q^2}^n:\langle\mathbf{x},\mathbf{y}\rangle=0\text{ for all }\mathbf{y}\in\mathscr{C}\}.$$

Then, $\mathscr{C}^{\perp_H}$ is a q^2-ary linear code with dimension $n-\dim(\mathscr{C})$.

Let τ: $\tau(c_0, c_1, \dots, c_{n-1}) = (\lambda c_{n-1}, c_0, \dots, c_{n-2})$ be the constacyclic shift on $\mathbb{F}_{q^2}^n$. A q^2-ary linear code $\mathscr{C}$ of length n is called a λ-constacyclic code if $\tau(\mathscr{C}) = \mathscr{C}$. In case $\lambda = 1$, those constacyclic codes are called cyclic codes. Defining a map

$$\sigma : \mathbb{F}_{q^2}^n \longrightarrow \mathscr{R} = \frac{\mathbb{F}_{q^2}[x]}{\langle x^n - \lambda \rangle}$$

$$(c_0, c_1, \dots, c_{n-1}) \longmapsto c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$$

Then a q^2-ary linear code $\mathscr{C}$ of length n is a λ-constacyclic code if and only if $\sigma(\mathscr{C}) = \{\sigma(\mathbf{c}) | \mathbf{c} \in \mathscr{C}\}$ is an ideal of the quotient ring $\mathscr{R}$. Note that each ideal of $\mathscr{R}$ is principal. Let $\mathscr{C} = \langle f(x) \rangle$ be a λ-constacyclic code of length n, where $f(x)$ is a monic polynomial of minimal degree in $\mathscr{C}$. Then $f(x)$ is called the generator polynomial of $\mathscr{C}$ and $f(x) | (x^n - \lambda)$.

Assume that $\gcd(n, q) = 1$, $\mathrm{ord}(\lambda) = r$, and $\mathrm{ord}_{rn}(q^2) = m$, i.e., the multiplicative order of q^2 modulo rn is m. Then there exists a primitive rn-th root of unity ξ in $\mathbb{F}_{q^{2m}}$ such that $\xi^n = \lambda$, which implies that $x^n - \lambda = \prod_{i=0}^{n-1}(x - \xi^{1+ri})$. Let $m_i(x)$ be the minimal polynomial of ξ^{1+ri} over $\mathbb{F}_{q^2}$ and $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ be the ring of integers modulo n. For each q^2 -ary λ-constacyclic code $\mathscr{C}$ with generator polynomial $f(x)$ of length n, there is a subset $\Omega \subseteq \mathbb{Z}_n$ such that $f(x) = \prod_{i \in \Omega} m_i(x)$. Let $\mathbb{Z}_{rn}$ be the ring of integers modulo rn. For each $i \in \mathbb{Z}_{rn}$, the q^2-cyclotomic coset of i modulo rn is defined by

$$C_i := \{iq^{2\ell} \mod rn : 0 \leqslant \ell \leqslant \ell_i - 1\},$$

where ℓ_i is the smallest positive integer such that $iq^{2\ell_i} \equiv i \mod rn$. Assume that $\mathscr{C}$ is a q^2-ary λ-constacyclic code of length n with generator polynomial $f(x)$, then the set $\mathscr{Z} = \{i \in \mathbb{Z}_{rn} | f(\xi^i) = 0\}$, is called the defining set of $\mathscr{C}$, where ξ is a primitive rn-th root of unity in some extension field of $\mathbb{F}_{q^2}$. It is clear that $\mathscr{Z}$ is a union of some q^2-cyclotomic cosets and $\dim(\mathscr{C}) = n - |\mathscr{Z}|$, where $|\mathscr{Z}|$ denotes the cardinality of the set $\mathscr{Z}$. The minimum distance of $\mathscr{C}$ can be estimated by the following well-known bound.

Theorem 2 (**BCH bound**) [22] *Let δ be an integer in the range $2 \leqslant \delta \leqslant n$. Assume that $\mathscr{C}$ is a λ-constacyclic code of length n with defining set $\mathscr{Z}$. If $\mathscr{Z}$ consists of $\delta - 1$ consecutive elements, then $d(\mathscr{C}) \geqslant \delta$.*

The following lemma gives a criterion for verifying that $\mathscr{C}$ contains its Hermitian dual code $\mathscr{C}^{\perp_H}$.

Lemma 1 [20] *Let $\mathscr{C}$ be a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set $\mathscr{Z}$. Then $\mathscr{C}$ contains its Hermitian dual code $\mathscr{C}^{\perp_H}$ if and only if $\mathscr{Z} \bigcap \mathscr{Z}^{-q} = \emptyset$, where $\mathscr{Z}^{-q} = \{-qz \mod rn | z \in \mathscr{Z}\}$.*

As we know, the key in the construction of EAQEC codes is to determine the number of maximally entangled states. Scholars have proposed several methods to solve this problem and the related construction methods for EAQEC codes also have been given. Among these methods, a frequently used one is the decomposition of the defining set of the source codes, please see [6, 34], etc. Similar to such method, we have the following result.

Theorem 3 *Let $\mathscr{C}$ be a q^2-ary λ-constacyclic code of length n with defining set $\mathscr{Z}$. Suppose that $\Delta = \mathscr{Z} \bigcap \mathscr{Z}^{-q}$, where $\mathscr{Z}^{-q} = \{-qz \bmod rn : z \in \mathscr{Z}\}$. If $\mathscr{C}$ has parameters $[n, k = n - |\mathscr{Z}|, d]_{q^2}$, then there is an EAQEC code with parameters $[[n, n - 2|\mathscr{Z}| + |\Delta|, d; |\Delta|]]_q$.*

3 Entanglement-Assisted Quantum MDS codes Derived from Constacyclic Codes

Let $\eta \in \mathbb{F}_{q^2}^*$ and $ord(\eta) = q + 1$. In this section, we will construct some EAQMDS codes of length $n = \frac{q^2+1}{\rho}$ from η-constacyclic codes, where $\rho = a^2 + (a+1)^2$, and $a \geqslant 2$ is a positive integer. It is easy to obtain that q is a prime power with the form $q = \rho m + 2a + 1$ or $q = \rho m - 2a - 1$, where m is a positive integer. As we said before, we only consider q being odd with the form $q = 2\rho m \pm (2a + 1)$. Since $\rho = a^2 + (a+1)^2$ is always odd. Similar to the proof of Lemma 3.12 in [20], We can get the following lemma which will play an important role in our construction.

Lemma 2 [20] *Let $n = \frac{q^2+1}{\rho}$, $s = \frac{q^2+1}{2}$, and ρ be odd. Then all cyclotomic cosets modulo $(q+1)n$ containing $1 + (q+1)i$ are as follows*:

(1) $C_s = \{s\}$ *and* $C_{s \pm \frac{q+1}{2}n} = \{s \pm \frac{q+1}{2}n\}$.
(2) $C_{s-(q+1)i} = \{s - (q+1)i, s + (q+1)i\}$ *for* $1 \leqslant i \leqslant n/2 - 1$.

Now we give the construction of EAQMDS codes under the case $q = 2\rho m + 2a + 1$.

Lemma 3 *Let q be an odd prime power with the form $q = 2\rho m + 2a + 1$, where $\rho = a^2 + (a+1)^2$, and $a \geqslant 2, m$ is a positive integer. Let $n = \frac{q^2+1}{\rho}$, $s = \frac{q^2+1}{2}$. If $\mathscr{C}$ is an η -constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set $\mathscr{Z} = \bigcup_{j=0}^{\delta} C_{s-(q+1)j}$, where $0 \leqslant \delta \leqslant \frac{(2a+1)q+1}{2\rho} - 1$, then $\mathscr{C}^{\perp_H} \subseteq \mathscr{C}$.*

Proof According to Lemma 1, we only need to consider that $\mathscr{Z} \bigcap \mathscr{Z}^{-q} = \emptyset$. Suppose that $\mathscr{Z} \bigcap \mathscr{Z}^{-q} \neq \emptyset$, then there exist two integers i and j, where $0 \leqslant i, j \leqslant \frac{(2a+1)q+1}{2\rho} - 1$ such that

$$s - (q+1)i \equiv -q[s - (q+1)j]q^{2k} \mod (q+1)n,$$

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

(I) If $k = 0$, then

$$s - (q+1)i \equiv -q[s - (q+1)j] \mod (q+1)n,$$

which is equivalent to

$$2\rho(qj + i) \equiv q^2 + 1 \mod 2(q^2 + 1).$$

Due to $0 \leqslant i,j \leqslant \frac{(2a+1)q+1}{2\rho} - 1$, we have $0 \leqslant 2\rho i, 2\rho j \leqslant (2a+1)q + 1 - 2\rho$. We now divide into the following subcases.

(i) If $0 \leqslant 2\rho j \leqslant 2q - 2a - 1$, then

$$0 \leqslant 2\rho(qj + i) \leqslant 2(q^2 + 1) - 2\rho - 1 < 2(q^2 + 1).$$

Writing $2\rho i$ in the form $2\rho i = uq + v$, where $0 \leqslant u \leqslant 2a - 1$, $0 \leqslant v \leqslant q - 1$, and $u = 2a,\ 0 \leqslant v \leqslant q - 2\rho + 1$. Then $q^2 + 1 = 2\rho(qj + i) = (2\rho j + u)q + v$. By the division algorithm, it must be $q = 2\rho j + u$, which contradicts to the form of q.

(ii) If $wq - 2a \leqslant 2\rho j \leqslant (w+2)q - 2a - 1$, where $w = 2, 4, \ldots, 2a - 2$. Then

$$w(q^2 + 1) - 2aq - w \leqslant 2\rho(qj + i) \leqslant (w+2)(q^2 + 1) - 2\rho - w - 1.$$

Hence,

$$-(q^2 + 1) < 2\rho(qj + i) - w(q^2 + 1) < 2(q^2 + 1),$$

which means that $(w+1)(q^2 + 1) = 2\rho(qj + i) = (2\rho j + u)q + v$. Therefore, $(w+1)q = 2\rho j + u$, which also contradicts to the form of q.

(iii) If $2aq - 2a \leqslant 2\rho j \leqslant (2a+1)q - 2\rho + 1$, then

$$2a(q^2 + 1) - 2aq - 2a \leqslant 2\rho(qj + i) \leqslant (2a+1)(q^2 + 1) + 2(a - \rho + 1)q - 2a - 2\rho.$$

Hence,

$$-(q^2 + 1) < 2\rho(qj + i) \mod 2(q^2 + 1) < q^2 + 1,$$

which is a contradiction.

(II) If $k = 1$, then

$$s - (q+1)i \equiv -[s - (q+1)j]q^3 \mod (q+1)n.$$

Since $-[s - (q+1)j]q^3 = -sq^3 + (q+1)q^3 j \equiv -sq - (q+1)qj \mod (q+1)n$, one can get $s - (q+1)i \equiv -sq - (q+1)qj \mod (q+1)n$, which is equivalent to

$$q^2 + 1 + 2\rho qj \equiv 2\rho i \mod 2(q^2 + 1).$$

Due to $0 \leqslant i,j \leqslant \frac{(2a+1)q+1}{2\rho} - 1$, we have $0 \leqslant 2\rho i, 2\rho j \leqslant (2a+1)q + 1 - 2\rho$. We now divide into the following subcases.

(i) If $0 \leqslant 2\rho j \leqslant q - 2a - 1$, then

$$q^2 + 1 \leqslant 2\rho qj + q^2 + 1 \leqslant 2q^2 + 1 - (2a+1)q < 2(q^2 + 1),$$

while $0 \leqslant 2\rho i \leqslant (2a+1)q - 2\rho + 1 < q^2 + 1$. This is a contradiction.

(ii) If $wq - 2a \leqslant 2\rho j \leqslant (w+2)q - 2a - 1$, where $w = 1, 3, \ldots, 2a - 3$. Then

$$(w+1)(q^2 + 1) - 2aq - w \leqslant 2\rho qj + q^2 + 1 \leqslant (w+3)(q^2 + 1) - (2a+1)q - w - 2.$$

If $(w+1)(q^2+1)-2aq-w \leqslant 2\rho qj+q^2+1 \leqslant (w+1)(q^2+1)-1$, then $q^2+1 < 2(q^2+1)-2aq-w \leqslant 2\rho qj+q^2+1-(w-1)(q^2+1) \leqslant 2q^2+1$, which is impossible due to (i). If $(w+1)(q^2+1) \leqslant 2\rho qj+q^2+1 \leqslant (w+3)(q^2+1)-(2a+1)q-w-2$, then $0 \leqslant 2\rho qj+q^2+1-(w+1)(q^2+1) \leqslant 2(q^2+1)-(2a+1)q-w-2 < 2(q^2+1)$. Writing $2\rho i$ in the form $2\rho i = uq+v$, where $0 \leqslant u \leqslant 2a-1$, $0 \leqslant v \leqslant q-1$, and $u=2a$, $0 \leqslant v \leqslant q-2\rho+1$. Then $w(q^2+1) = 2\rho(qj-i) = (2\rho j-u)q-v$. By the division algorithm, it must be $wq = 2\rho j-u$, which contradicts to the form of q.

(iii) If $(2a-1)q-2a \leqslant 2\rho j \leqslant (2a+1)q-2\rho+1$, then

$$2aq^2-2aq+1 \leqslant 2\rho qj+q^2+1 \leqslant (2a+2)q^2-(2\rho-1)q+1.$$

If $2aq^2-2aq+1 \leqslant 2\rho qj+q^2+1 \leqslant 2a(q^2+1)-1$, then $q^2+1 < 2(q^2+1)-2aq-2a+1 \leqslant 2\rho qj+q^2+1-(2a-2)(q^2+1) \leqslant 2q^2+1$, which is also impossible due to (i). If $2a(q^2+1) \leqslant 2\rho qj+q^2+1 \leqslant (2a+2)q^2-(2\rho-1)q+1$, then $0 \leqslant 2\rho qj+q^2+1-2a(q^2+1) \leqslant 2q^2-(2\rho-1)q+1 < 2(q^2+1)$. Hence, $(2a-1)(q^2+1) = 2\rho(qj-i) = (2\rho j-u)q-v$, which means that $(2a-1)q = 2\rho j-u$, and it contradicts to the form of q.

Therefore, we conclude that $\mathscr{X} \bigcap \mathscr{X}^{-q} = \emptyset$ as desired.

Lemma 4 *Let q be an odd prime power with the form $q = 2\rho m+2a+1$, where $\rho = a^2+(a+1)^2$, and $a \geqslant 2$, m is a positive integer. Let $n = \frac{q^2+1}{\rho}$, $s = \frac{q^2+1}{2}$. Then*

(1) $-qC_s = C_{s-\frac{q+1}{2}n}$;

(2) $-qC_{s-\frac{(2a+1)q+1}{2\rho}(q+1)} = C_{s-\frac{q-2a-1}{2\rho}(q+1)}$;

(3) $-qC_{s-\frac{(4a+1)q+2a+3}{2\rho}(q+1)} = C_{s-\frac{(2a+3)q-4a-1}{2\rho}(q+1)}$.

Proof

(1) As $\rho = a^2+(a+1)^2$, and a is a positive integer, it is easy to see that ρ is odd.

$$\begin{aligned} -qs =& -(q+1)s+s \\ =& -\frac{\rho-1}{\rho}(q+1)s-\frac{q+1}{\rho}s+s \\ =& -\frac{\rho-1}{2}(q+1)n+s-\frac{q+1}{\rho}s \\ \equiv& s-\frac{q+1}{2}n \mod (q+1)n, \end{aligned}$$

which implies that $-qC_s = C_{s-\frac{q+1}{2}n}$.

(2) $-qC_{s-\frac{(2a+1)q+1}{2\rho}(q+1)} = C_{s-\frac{q-2a-1}{2\rho}(q+1)}$ holds for the following reason

$$
\begin{aligned}
&-q\left[s\pm\frac{(2a+1)q+1}{2\rho}(q+1)\right]\\
=&-qs\mp\frac{(2a+1)q^2+q}{2\rho}(q+1)\\
\equiv& s-\frac{q+1}{2}n\mp\frac{(2a+1)(q^2+1)+q-2a-1}{2\rho}(q+1) \mod (q+1)n\\
\equiv& s\mp\frac{q-2a-1}{2\rho}(q+1) \mod (q+1)n.
\end{aligned}
$$

(3) $-qC_{s-\frac{(4a+1)q+2a+3}{2\rho}(q+1)}=C_{s-\frac{(2a+3)q-4a-1}{2\rho}(q+1)}$ also holds for the following reason

$$
\begin{aligned}
&-q\left[s\pm\frac{(4a+1)q+2a+3}{2\rho}(q+1)\right]\\
=&-qs\mp\frac{(4a+1)q^2+(2a+3)q}{2\rho}(q+1)\\
\equiv& s-\frac{q+1}{2}n\mp\frac{(4a+1)(q^2+1)+(2a+3)q-4a-1}{2\rho}(q+1) \mod (q+1)n\\
\equiv& s\mp\frac{(2a+3)q-4a-1}{2\rho}(q+1) \mod (q+1)n.
\end{aligned}
$$

Lemma 5 *Let q be an odd prime power with the form $q=2\rho m+2a+1$, where $\rho=a^2+(a+1)^2$, and $a\geqslant 2, m$ is a positive integer. Let $n=\frac{q^2+1}{\rho}$, $s=\frac{q^2+1}{2}$. If $\mathscr{C}$ is an η -constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set $\mathscr{Z}=\bigcup_{j=0}^{\delta}C_{s-(q+1)j}$, then*

$$
|\mathscr{Z}^{-q}\bigcap\mathscr{Z}|=\begin{cases}0, & 0\leqslant\delta\leqslant\frac{(2a+1)q+1}{2\rho}-1;\\ 4, & \frac{(2a+1)q+1}{2\rho}\leqslant\delta\leqslant\frac{(4a+1)q+2a+3}{2\rho}-1;\\ 8, & \frac{(4a+1)q+2a+3}{2\rho}\leqslant\delta\leqslant\frac{(4a+3)q-(2a-1)}{2\rho}-1.\end{cases}
$$

Proof (1) Let $\mathscr{Z}=\bigcup_{j=0}^{\delta}C_{s-(q+1)j}$, where $0\leqslant\delta\leqslant\frac{(2a+1)q+1}{2\rho}-1$. Then $|\mathscr{Z}^{-q}\bigcap\mathscr{Z}|=0$ follows from Lemma 3.

(2) Let $\mathscr{Z}=\mathscr{Z}_1\bigcup\mathscr{Z}_2\bigcup C_{s-\frac{(2a+1)q+1}{2\rho}(q+1)}$, where $\mathscr{Z}_1=\bigcup_{j=0}^{\frac{(2a+1)q+1}{2\rho}-1}C_{s-(q+1)j}$, $\mathscr{Z}_2=\bigcup_{j=\frac{(2a+1)q+1}{2\rho}+1}^{\delta}C_{s-(q+1)j}$, and $\frac{(2a+1)q+1}{2\rho}+1\leqslant\delta\leqslant\frac{(4a+1)q+2a+3}{2\rho}-1$. Then

$$
\begin{aligned}
\mathscr{Z}^{-q}\bigcap\mathscr{Z}=&\left(\mathscr{Z}_1^{-q}\bigcup\mathscr{Z}_2^{-q}\bigcup -qC_{s-\frac{(2a+1)q+1}{2\rho}(q+1)}\right)\bigcap\left(\mathscr{Z}_1\bigcup\mathscr{Z}_2\bigcup C_{s-\frac{(2a+1)q+1}{2\rho}(q+1)}\right)\\
=&\left(\mathscr{Z}_1^{-q}\bigcap\mathscr{Z}_1\right)\bigcup\left(\mathscr{Z}_1^{-q}\bigcap\mathscr{Z}_2\right)\bigcup\left(\mathscr{Z}_1^{-q}\bigcap C_{s-\frac{(2a+1)q+1}{2\rho}(q+1)}\right)\bigcup\\
&\left(\mathscr{Z}_2^{-q}\bigcap\mathscr{Z}_1\right)\bigcup\left(\mathscr{Z}_2^{-q}\bigcap\mathscr{Z}_2\right)\bigcup\left(\mathscr{Z}_2^{-q}\bigcap C_{s-\frac{(2a+1)q+1}{2\rho}(q+1)}\right)\bigcup\\
&\left(-qC_{s-\frac{(2a+1)q+1}{2\rho}(q+1)}\bigcap\mathscr{Z}_1\right)\bigcup\left(-qC_{s-\frac{(2a+1)q+1}{2\rho}(q+1)}\bigcap\mathscr{Z}_2\right)\bigcup\\
&\left(-qC_{s-\frac{(2a+1)q+1}{2\rho}(q+1)}\bigcap C_{s-\frac{(2a+1)q+1}{2\rho}(q+1)}\right).
\end{aligned}
$$

According to Lemma 3, $\mathscr{Z}_1^{-q}\bigcap\mathscr{Z}_1=\emptyset$. It follows from Lemma 4, one can get

$$
\begin{aligned}
&-qC_{s-\frac{(2a+1)q+1}{2\rho}(q+1)} \bigcap C_{s-\frac{(2a+1)q+1}{2\rho}(q+1)} = \emptyset,\\
&-qC_{s-\frac{(2a+1)q+1}{2\rho}(q+1)} \bigcap \mathscr{Z}_1 = C_{s-\frac{q-2a-1}{2\rho}(q+1)},\\
&C_{s-\frac{(2a+1)q+1}{2\rho}(q+1)} \bigcap \mathscr{Z}_1^{-q} = C_{s-\frac{(2a+1)q+1}{2\rho}(q+1)},\\
&-qC_{s-\frac{(2a+1)q+1}{2\rho}(q+1)} \bigcap \mathscr{Z}_2 = \emptyset,\\
&C_{s-\frac{(2a+1)q+1}{2\rho}(q+1)} \bigcap \mathscr{Z}_2^{-q} = \emptyset.
\end{aligned}
$$

Now we only have to proof that $\mathscr{Z}_1^{-q} \bigcap \mathscr{Z}_2 = \mathscr{Z}_2^{-q} \bigcap \mathscr{Z}_1 = \emptyset$ and $\mathscr{Z}_2^{-q} \bigcap \mathscr{Z}_2 = \emptyset$.

Suppose $\mathscr{Z}_1 \bigcap \mathscr{Z}_2^{-q} \neq \emptyset$, then there exist two integers i and j, where $0 \leqslant i \leqslant \frac{(2a+1)q+1}{2\rho} - 1$ and $\frac{(2a+1)q+1}{2\rho} + 1 \leqslant j \leqslant \frac{(4a+1)q+2a+3}{2\rho} - 1$ such that

$$s - (q+1)i \equiv -q[s-(q+1)j]q^{2k} \mod (q+1)n,$$

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

(I) If $k = 0$, then

$$s - (q+1)i \equiv -q[s-(q+1)j] \mod (q+1)n,$$

which is equivalent to

$$2\rho(qj + i) \equiv q^2 + 1 \mod 2(q^2+1).$$

Since $0 \leqslant i \leqslant \frac{(2a+1)q+1}{2\rho} - 1$ and $\frac{(2a+1)q+1}{2\rho} + 1 \leqslant j \leqslant \frac{(4a+1)q+2a+3}{2\rho} - 1$, we have $0 \leqslant 2\rho i \leqslant (2a+1)q + 1 - 2\rho$, and $(2a+1)q + 1 + 2\rho \leqslant 2\rho j \leqslant (4a+1)q + 2a + 3 - 2\rho$. We now divide into the following subcases.

(i) If $(2a+1)q + 2\rho + 1 \leqslant 2\rho j \leqslant (2a+3)q - 2a - 1$, then

$$(2a+1)(q^2+1) + (2\rho+1)q - (2a+1) \leqslant 2\rho(qj+i) \leqslant (2a+3)(q^2+1) - 2(a+\rho+1).$$

Hence,

$$-(q^2+1) < 2\rho(qj+i) - (2a+2)(q^2+1) < q^2 + 1,$$

which is a contradiction.

(ii) If $(2a+3)q - 2a \leqslant 2\rho j \leqslant (2a+4)q - 2a - 1$, then

$$(2a+2)(q^2+1) + q^2 - 2(aq+a+1) \leqslant 2\rho(qj+i) \leqslant (2a+4)(q^2+1) - 2a - 2\rho - 3.$$

Hence,

$$0 < 2\rho(qj+i) - (2a+2)(q^2+1) < 2(q^2+1).$$

Writing $2\rho i$ in the form $2\rho i = uq + v$, where $0 \leqslant u \leqslant 2a - 1$, $0 \leqslant v \leqslant q - 1$, and $u = 2a$, $0 \leqslant v \leqslant q - 2\rho + 1$. Then $(2a+3)(q^2+1) = 2\rho(qj+i) = (2\rho j + u)q + v$. By the division algorithm, it must be $(2a+3)q = 2\rho j + u$, which contradicts to the form of q.

(iii) If $wq - 2a \leqslant 2\rho j \leqslant (w+2)q - 2a - 1$, where $w = 2a+4, \ldots, 4a-2$. Then

$$w(q^2+1)-2aq-w \leqslant 2\rho(qj+i) \leqslant (w+2)(q^2+1)-2\rho-w-1.$$

Hence,

$$-(q^2+1) < 2\rho(qj+i)-w(q^2+1) < 2(q^2+1),$$

which means that $(w+1)(q^2+1)=2\rho(qj+i)=(2\rho j+u)q+v$. Therefore, $(w+1)q=2\rho j+u$, which also contradicts to the form of q.

(iv) If $4aq-2a \leqslant 2\rho j \leqslant (4a+1)q+2a+3-2\rho$, then

$$4a(q^2+1)-2aq-4a \leqslant 2\rho(qj+i) \leqslant (4a+1)(q^2+1)+2(2a-\rho+2)q-2(2a+\rho).$$

Hence,

$$-(q^2+1) < 2\rho(qj+i) \mod 2(q^2+1) < q^2+1,$$

which is a contradiction.

(II) If $k=1$, then

$$s-(q+1)i \equiv -[s-(q+1)j]q^3 \mod (q+1)n,$$

which is equivalent to

$$q^2+1+2\rho qj \equiv 2\rho i \mod 2(q^2+1).$$

Similar to the discussion of Lemma 3 (2) and Lemma 5 (1), this case is impossible.

Finally, suppose $\mathscr{Z}_2^{-q}\bigcap\mathscr{Z}_2 \neq \emptyset$, then there exist two integers i and j, where $\frac{(2a+1)q+1}{2\rho}+1 \leqslant i,j \leqslant \frac{(4a+1)q+2a+3}{2\rho}-1$ such that

$$s-(q+1)i \equiv -q[s-(q+1)j]q^{2k} \mod (q+1)n,$$

for $k \in \{0,1\}$. Going on the line of the proofs similar to the above cases, one can get such case is impossible either.

Therefore,

$$\begin{aligned}\mathscr{Z}^{-q}\bigcap\mathscr{Z} &= C_{s-\frac{q-2a-1}{2\rho}(q+1)}\bigcup C_{s-\frac{(2a+1)q+1}{2\rho}(q+1)}\\ &=\left\{s \pm \frac{q-2a-1}{2\rho}(q+1), s \pm \frac{(2a+1)q+1}{2\rho}(q+1)\right\},\end{aligned}$$

which means that $|\mathscr{Z}^{-q}\bigcap\mathscr{Z}|=4$.

(3) This case can be proved by using the same method, we omit it here for simplification.

Theorem 4 *Let q be an odd prime power with the form $q=2\rho m+2a+1$, where $\rho=a^2+(a+1)^2$, and $a \geqslant 2, m$ is a positive integer. Let $n=\frac{q^2+1}{\rho}$. Then there exist q-ary EAQMDS codes with the following parameters*:

(1) $[[n, n-2d+2, d]]$, *where* $2 \leqslant d \leqslant \frac{(2a+1)q+1}{\rho}$ *is even*;
(2) $[[n, n-2d+6, d;4]]$, *where* $\frac{(2a+1)q+1}{\rho}+2 \leqslant d \leqslant \frac{(4a+1)q+2a+3}{\rho}$ *is even*;
(3) $[[n, n-2d+10, d;8]]$, *where* $\frac{(4a+1)q+2a+3}{\rho}+2 \leqslant d \leqslant \frac{(4a+3)q-2a+1}{\rho}$ *is even.*

Proof Let $\mathscr{C}$ be an η-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set $\mathscr{Z} = \bigcup_{j=0}^{\delta} C_{s-(q+1)j}$, where $0 \leqslant \delta \leqslant \frac{(4a+3)q-2a+1}{2\rho} - 1$. From Lemma 1, we can see that $\mathscr{Z}$ consists of $2\delta + 1$ consecutive integers $\{s-(q+1)\delta, \ldots, s-(q+1), s, s+(q+1), \ldots, s+(q+1)\delta\}$, which implies that $\mathscr{C}$ has minimum distance at least $2\delta + 2$ from Theorem 2. Hence, $\mathscr{C}$ is a q^2-ary η-constacyclic code with parameters $[n, n-(2\delta+1), \geqslant 2\delta+2]$. According to Lemma 5,

$$c = |\mathscr{Z}^{-q} \bigcap \mathscr{Z}| = \begin{cases} 0, & 0 \leqslant \delta \leqslant \frac{(2a+1)q+1}{2\rho} - 1; \\ 4, & \frac{(2a+1)q+1}{2\rho} \leqslant \delta \leqslant \frac{(4a+1)q+2a+3}{2\rho} - 1; \\ 8, & \frac{(4a+1)q+2a+3}{2\rho} \leqslant \delta \leqslant \frac{(4a+3)q-(2a-1)}{2\rho} - 1. \end{cases}$$

Combining Theorem 3 with the EA-quantum Singleton bound, there are q-ary EAQMDS codes with parameters as desired. The result follows.

Now we consider the case $q = 2\rho m - 2a - 1$, where $\rho = a^2 + (a+1)^2$, and $a \geqslant 2, m$ is a positive integer.

Lemma 6 *Let q be an odd prime power with the form $q = 2\rho m - 2a - 1$, where $\rho = a^2 + (a+1)^2$, and $a \geqslant 2, m$ is a positive integer. Let $n = \frac{q^2+1}{\rho}$, $s = \frac{q^2+1}{2}$. If $\mathscr{C}$ is an η -constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set $\mathscr{Z} = \bigcup_{j=0}^{\delta} C_{s-(q+1)j}$, where $0 \leqslant \delta \leqslant \frac{(2a+1)q-1}{2\rho} - 1$, then $\mathscr{C}^{\perp_H} \subseteq \mathscr{C}$.*

Proof The proof is similar to Lemma 3, we omit it here.

Lemma 7 *Let q be an odd prime power with the form $q = 2\rho m - 2a - 1$, where $\rho = a^2 + (a+1)^2$, and $a \geqslant 2, m$ is a positive integer. Let $n = \frac{q^2+1}{\rho}$, $s = \frac{q^2+1}{2}$. Then*

(1) $-qC_{s-\frac{(2a+1)q-1}{2\rho}(q+1)} = C_{s-\frac{q+2a+1}{2\rho}(q+1)}$;
(2) $-qC_{s-\frac{(4a+1)q-2a-3}{2\rho}(q+1)} = C_{s-\frac{(2a+3)q+4a+1}{2\rho}(q+1)}$.

Proof

(1) $-qC_{s-\frac{(2a+1)q-1}{2\rho}(q+1)} = C_{s-\frac{q+2a+1}{2\rho}(q+1)}$ holds for the following reason

$$\begin{aligned} & -q\left[s \pm \frac{(2a+1)q-1}{2\rho}(q+1)\right] \\ = & -qs \mp \frac{(2a+1)q^2-q}{2\rho}(q+1) \\ \equiv & s - \frac{q+1}{2}n \mp \frac{(2a+1)(q^2+1)-q-2a-1}{2\rho}(q+1) \mod (q+1)n \\ \equiv & s \pm \frac{q+2a+1}{2\rho}(q+1) \mod (q+1)n. \end{aligned}$$

(2) $-qC_{s-\frac{(4a+1)q-2a-3}{2\rho}(q+1)} = C_{s-\frac{(2a+3)q+4a+1}{2\rho}(q+1)}$ also holds for the following reason

$$\begin{aligned}
&-q\left[s \pm \frac{(4a+1)q-2a-3}{2\rho}(q+1)\right]\\
=&-qs \mp \frac{(4a+1)q^2-(2a+3)q}{2\rho}(q+1)\\
\equiv& s - \frac{q+1}{2}n \mp \frac{(4a+1)(q^2+1)-(2a+3)q-4a-1}{2\rho}(q+1) \mod (q+1)n\\
\equiv& s \pm \frac{(2a+3)q+4a+1}{2\rho}(q+1) \mod (q+1)n.
\end{aligned}$$

Similar to Lemma 5 and Theorem 4, we have the following results.

Lemma 8 *Let q be an odd prime power with the form $q = 2\rho m - 2a - 1$, where $\rho = a^2 + (a+1)^2$, and $a \geqslant 2, m$ is a positive integer. Let $n = \frac{q^2+1}{\rho}$, $s = \frac{q^2+1}{2}$. If $\mathscr{C}$ is an η-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set $\mathscr{Z} = \bigcup_{j=0}^{\delta} C_{s-(q+1)j}$, then*

$$|\mathscr{Z}^{-q} \bigcap \mathscr{Z}| = \begin{cases} 0, & 0 \leqslant \delta \leqslant \frac{(2a+1)q-1}{2\rho} - 1; \\ 4, & \frac{(2a+1)q-1}{2\rho} \leqslant \delta \leqslant \frac{(4a+1)q-2a-3}{2\rho} - 1; \\ 8, & \frac{(4a+1)q-2a-3}{2\rho} \leqslant \delta \leqslant \frac{(4a+3)q+(2a-1)}{2\rho} - 1. \end{cases}$$

Theorem 5 *Let q be an odd prime power with the form $q = 2\rho m - 2a - 1$, where $\rho = a^2 + (a+1)^2$, and $a \geqslant 2, m$ is a positive integer. Let $n = \frac{q^2+1}{\rho}$. Then there exist q-ary EAQMDS codes with the following parameters*:

(1) $[[n, n-2d+2, d]]$, *where* $2 \leqslant d \leqslant \frac{(2a+1)q-1}{\rho}$ *is even*;
(2) $[[n, n-2d+6, d; 4]]$, *where* $\frac{(2a+1)q-1}{\rho} + 2 \leqslant d \leqslant \frac{(4a+1)q-2a-3}{\rho}$ *is even*;
(3) $[[n, n-2d+10, d; 8]]$, *where* $\frac{(4a+1)q-2a-3}{\rho} + 2 \leqslant d \leqslant \frac{(4a+3)q+2a-1}{\rho}$ *is even.*

Remark 1 Quantum MDS codes of length $n = \frac{q^2+1}{(m^2+1)/2}$ with $m \geqslant 3$ is odd had been studied in [17]. Let $m = 2a+1$, then it is indeed the quantum MDS codes of length $n = \frac{q^2+1}{\rho}$, where $\rho = a^2 + (a+1)^2$, and a is a positive integer. We have got such quantum MDS codes with the same parameters in [17].

Remark 2 Let $a = 2$, then $\rho = 13$, $n = \frac{q^2+1}{13}$. EAQMDS codes of length $n = \frac{q^2+1}{13}$ with $c = 4$ and $c = 8$ had been also constructed in [43] from constacyclic codes (please see Table 1), where $q = 26m + 5$ and $26m + 21$. It is easy to see that our results coincide with theirs, in other words, we generalize the results in [43].

Example 1 Let $a = 3$, then $\rho = 25$, $n = \frac{q^2+1}{25}$. EAQMDS code of length $n = \frac{q^2+1}{25}$ are constructed. We list some new EAQMDS codes obtained from Theorems 4 and 5 in Table 3.

Table 3 New entanglement-assisted quantum MDS codes

n	q	Parameters $[[n,k,d;c]]_q$	d
$\frac{q^2+1}{25}$	43	$[[74,80-2d,d;4]]_{43}$	$14 \leqslant d \leqslant 22$ is even
		$[[74,84-2d,d;8]]_{43}$	$24 \leqslant d \leqslant 26$ is even
	57	$[[130,136-2d,d;4]]_{57}$	$18 \leqslant d \leqslant 30$ is even
		$[[130,140-2d,d;8]]_{57}$	$32 \leqslant d \leqslant 34$ is even
	107	$[[458,464-2d,d;4]]_{107}$	$32 \leqslant d \leqslant 56$ is even
		$[[458,468-2d,d;8]]_{107}$	$58 \leqslant d \leqslant 64$ is even
	157	$[[986,992-2d,d;4]]_{157}$	$46 \leqslant d \leqslant 82$ is even
		$[[986,996-2d,d;8]]_{157}$	$84 \leqslant d \leqslant 94$ is even
$\frac{q^2+1}{41}$	73	$[[130,136-2d,d;4]]_{73}$	$18 \leqslant d \leqslant 30$ is even
		$[[130,140-2d,d;8]]_{73}$	$32 \leqslant d \leqslant 34$ is even
	173	$[[730,736-2d,d;4]]_{173}$	$40 \leqslant d \leqslant 72$ is even
		$[[730,740-2d,d;8]]_{173}$	$74 \leqslant d \leqslant 80$ is even
	337	$[[2770,2776-2d,d;4]]_{337}$	$76 \leqslant d \leqslant 140$ is even
		$[[2770,2780-2d,d;8]]_{337}$	$142 \leqslant d \leqslant 156$ is even
	401	$[[3922,3928-2d,d;4]]_{401}$	$90 \leqslant d \leqslant 166$ is even
		$[[3922,3932-2d,d;8]]_{401}$	$168 \leqslant d \leqslant 186$ is even

4 Entanglement-Assisted Quantum MDS Codes derived from Cyclic Codes

In this section, we will construct some EAQMDS codes of length $n = \frac{q^2+1}{\rho}$ from cyclic codes, where $\rho = a^2 + (a+1)^2$, and $a \geqslant 2$ is a positive integer. We first give the following useful lemma, which will be used in the sequel.

Lemma 9 [23] *Let $n \mid (q^2+1)$ and $s = \lfloor \frac{n}{2} \rfloor$. If n is odd, then the q^2-cyclotomic cosets modulo n containing integers from 0 to n are: $C_0 = \{0\}, C_i = \{i, -i\} = \{i, n-i\}$, where $1 \leqslant i \leqslant s$. If n is even, then the q^2-cyclotomic cosets modulo n containing integers from 0 to n are: $C_0 = \{0\}, C_s = \{s\}$ and $C_i = \{i, -i\} = \{i, n-i\}$, where $1 \leqslant i \leqslant s-1$.*

It can be easily checked that n is even if $q = 2\rho m \pm (2a+1)$, i.e. q is an odd prime power. We first consider the case $q = 2\rho m + 2a + 1$. Due to Lemma 9, we have the following results.

Lemma 10 *Let q be an odd prime power with the form $q = 2\rho m + 2a + 1$, where $\rho = a^2 + (a+1)^2$, and $a \geqslant 2, m$ is a positive integer. Let $n = \frac{q^2+1}{\rho}$, $s = \frac{n}{2}$. Then*

(1) $-qC_s = C_s$;
(2) $-qC_{s-\frac{(a+1)q-a}{\rho}} = C_{s-\frac{aq+a+1}{\rho}}$;
(3) $-qC_{s-\frac{(2a+1)q+1}{\rho}} = C_{s-\frac{q-(2a+1)}{\rho}}$.

Proof

(1) It is obvious that $-qs \equiv s \mod n$. Hence, $-qC_s = C_s$.
(2) $-qC_{s-\frac{(a+1)q-a}{\rho}} = C_{s-\frac{aq+a+1}{\rho}}$ holds for the following reason

$$\begin{aligned}
&-q\left[s \pm \frac{(a+1)q-a}{\rho}\right]\\
=&-qs \mp \frac{(a+1)q^2-aq}{\rho}\\
\equiv& s \mp \frac{(a+1)(q^2+1)-aq-(a+1)}{\rho} \mod n\\
\equiv& s \pm \frac{aq+a+1}{\rho} \mod n.
\end{aligned}$$

(3) $-qC_{s-\frac{(2a+1)q+1}{\rho}} = C_{s-\frac{q-(2a+1)}{\rho}}$ also holds for the following reason

$$\begin{aligned}
&-q\left[s \pm \frac{(2a+1)q+1}{\rho}\right]\\
=&-qs \mp \frac{(2a+1)q^2+q}{\rho}\\
\equiv& s \mp \frac{(2a+1)(q^2+1)+q-(2a+1)}{\rho} \mod n\\
\equiv& s \mp \frac{q-(2a+1)}{\rho} \mod n.
\end{aligned}$$

Lemma 11 *Let q be an odd prime power with the form $q = 2\rho m + 2a + 1$, where $\rho = a^2 + (a+1)^2$, and $a \geqslant 2, m$ is a positive integer. Let $n = \frac{q^2+1}{\rho}$, and $s = \frac{n}{2}$. If $\mathscr{C}$ is a cyclic code of length n over $\mathbb{F}_{q^2}$ with defining set $\mathscr{Z} = \bigcup_{i=0}^{\delta} C_{s-i}$, then*

$$|\mathscr{Z}^{-q} \bigcap \mathscr{Z}| = \begin{cases} 1, & 0 \leqslant \delta \leqslant \frac{(a+1)q-a}{\rho} - 1;\\ 5, & \frac{(a+1)q-a}{\rho} \leqslant \delta \leqslant \frac{(2a+1)q+1}{\rho} - 1;\\ 9, & \frac{(2a+1)q+1}{\rho} \leqslant \delta \leqslant \frac{(2a+2)q-2a}{\rho} - 1. \end{cases}$$

Proof (1) Let $\mathscr{Z} = C_s \bigcup \mathscr{Z}_1$, where $\mathscr{Z}_1 = \bigcup_{i=1}^{\delta} C_{s-i}$ and $1 \leqslant \delta \leqslant \frac{(a+1)q-a}{\rho} - 1$. As $-qC_s = C_s$, according to Lemma 1, we only need to consider that $\mathscr{Z}_1 \bigcap \mathscr{Z}_1^{-q} = \emptyset$. Suppose that $\mathscr{Z}_1 \bigcap \mathscr{Z}_1^{-q} \neq \emptyset$, then there exist two integers i and j, where $1 \leqslant i,j \leqslant \frac{(a+1)q-a}{\rho} - 1$, such that

$$s - i \equiv -q(s-j)q^{2k} \mod n,$$

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

(I) If $k = 0$, one obtains that $s - i \equiv -q(s-j) \mod n$, which is equivalent to

$$\rho(qj + i) \equiv 0 \mod q^2 + 1.$$

As $1 \leqslant i,j \leqslant \frac{(a+1)q-a}{\rho} - 1$, one gets $\rho \leqslant \rho i, \rho j \leqslant (a+1)q - a - \rho$. We now divide into the following subcases.

(i) If $\rho \leqslant \rho j \leqslant q - a - 1$, then

$$1 < \rho(q+1) \leqslant \rho(qj+i) \leqslant q^2 - a - \rho < q^2 + 1,$$

which is a contradiction.

(ii) If $wq - a \leqslant \rho j \leqslant (w+1)q - a - 1$, where $w = 1, 2, \ldots, a-1$. Then

$$wq^2 - aq + \rho \leqslant \rho(qj + i) \leqslant (w+1)q^2 - a - \rho.$$

Hence,

$$-(q^2+1) \leqslant -aq + \rho - w \leqslant \rho(qj+i) - w(q^2+1) \leqslant q^2 - a - w - \rho < q^2 + 1.$$

Writing ρi in the form $\rho i = uq + v$, where $u = 0$, $\rho \leqslant v \leqslant q-1$; $1 \leqslant u \leqslant a-1$, $0 \leqslant v \leqslant q-1$; $u = a$, $0 \leqslant v \leqslant q - a - \rho$. Hence, $w(q^2+1) = (\rho j + u)q + v$. By the division algorithm, it must be $wq = \rho j + u$, which contradicts to the form of q.

(iii) If $aq - a - 1 \leqslant \rho j \leqslant (a+1)q - a - \rho$, then

$$aq^2 - (a+1)q + \rho \leqslant \rho(qj+i) \leqslant (a+1)q^2 - (\rho - 1)q - a - \rho,$$

Hence,

$$-(q^2+1) < -(a+1)q + \rho - a \leqslant \rho(qj+i) - a(q^2+1) \leqslant q^2 - (\rho-1)q - 2a - \rho < q^2 + 1,$$

which means that $a(q^2+1) = \rho(qj+i) = (\rho j + u)q + v$. Therefore, $aq = \rho j + u$, which also contradicts to the form of q.

(II) If $k = 1$, one obtains that $s - i \equiv -q(s-j)q^2 \mod n$, which is equivalent to

$$\rho qj \equiv \rho i \mod q^2 + 1.$$

As $1 \leqslant i, j \leqslant \frac{(a+1)q-a}{\rho} - 1$, one gets $\rho \leqslant \rho i, \rho j \leqslant (a+1)q - a - \rho$. We now divide into the following subcases.

(i) If $\rho \leqslant \rho j \leqslant q - 1$, then

$$\rho q \leqslant \rho qj \leqslant q^2 - q < q^2 + 1,$$

while $\rho \leqslant \rho i \leqslant (a+1)q - a - \rho < \rho q$. This is a contradiction.

(ii) If $wq \leqslant \rho j \leqslant (w+1)q - 1$, where $w = 1, 2, \ldots, a-1$. Then

$$wq^2 \leqslant \rho qj \leqslant (w+1)q^2 - q.$$

If $wq^2 \leqslant \rho qj \leqslant w(q^2+1) + (a+1)q - a - \rho$, then $-w \leqslant \rho qj - w(q^2+1) \leqslant (a+1)q - a - \rho$, which means that $\rho qj - w(q^2+1) = \rho i$. Writing ρi in the form $\rho i = uq + v$, where $u = 0$, $\rho \leqslant v \leqslant q-1$; $1 \leqslant u \leqslant a-1$, $0 \leqslant v \leqslant q-1$; $u = a$, $0 \leqslant v \leqslant q - a - \rho$. Hence, $w(q^2+1) = \rho qj - \rho i = (\rho j - u)q - v$. By the division algorithm, it must be $wq = \rho j - u$, which contradicts to the form of q. If $w(q^2+1) + (a+1)q - a - \rho + 1 \leqslant \rho qj \leqslant (w+1)q^2 - q$, then $\rho i < (a+1)q - a - \rho + 1 \leqslant \rho qj - w(q^2+1) \leqslant q^2 - q - w < q^2 + 1$, which is a contradiction.

(iii) If $aq \leqslant \rho j \leqslant (a+1)q - a - \rho$, then

$$aq^2 \leqslant \rho qj \leqslant (a+1)q^2 - (a+\rho)q.$$

If $aq^2 \leqslant \rho qj \leqslant a(q^2+1) + (a+1)q - a - \rho$, then $-a \leqslant \rho qj - a(q^2+1) \leqslant (a+1)q - a - \rho$, which means that $\rho qj - a(q^2+1) = \rho i$. Hence, $a(q^2+1) = \rho qj - \rho i = (\rho j - u)q - v$. By the division algorithm, it must be $aq = \rho j - u$, which also contradicts to the form of q. If $a(q^2+1) + (a+1)q - a - \rho + 1 \leqslant \rho qj \leqslant (a+1)q^2 - (a+\rho)q$, then $\rho i < (a+1)q - a - \rho + 1 \leqslant \rho qj - a(q^2+1) \leqslant q^2 - (a+\rho)q - a < q^2 + 1$, which is a contradiction.

Therefore, $\mathscr{Z}^{-q} \bigcap \mathscr{Z} = C_s = \{s\}$, which means that $|\mathscr{Z}^{-q} \bigcap \mathscr{Z}| = 1$.

(2) Let $\mathscr{Z}= C_s \bigcup \mathscr{Z}_1 \bigcup C_{s-\frac{(a+1)q-a}{\rho}} \bigcup \mathscr{Z}_2$, where $\mathscr{Z}_1 = \bigcup_{i=1}^{\frac{(a+1)q-a}{\rho}-1} C_{s-i}$, $\mathscr{Z}_2 = \bigcup_{i=\frac{(a+1)q-a}{\rho}+1}^{\delta} C_{s-i}$, and $\frac{(a+1)q-a}{\rho} + 1 \leqslant \delta \leqslant \frac{(2a+1)q+1}{\rho} - 1$. Then

$$\begin{aligned}
\mathscr{Z}^{-q} \bigcap \mathscr{Z} =& \left(-qC_s \bigcup \mathscr{Z}_1^{-q} \bigcup -qC_{s-\frac{(a+1)q-a}{\rho}} \bigcup \mathscr{Z}_2^{-q}\right) \bigcap \left(C_s \bigcup \mathscr{Z}_1 \bigcup C_{s-\frac{(a+1)q-a}{\rho}} \bigcup \mathscr{Z}_2\right) \\
=& \left(-qC_s \bigcap C_s\right) \bigcup \left(-qC_s \bigcap \mathscr{Z}_1\right) \bigcup \left(-qC_s \bigcap C_{s-\frac{(a+1)q-a}{\rho}}\right) \bigcup \left(-qC_s \bigcap \mathscr{Z}_2\right) \\
& \left(\mathscr{Z}_1^{-q} \bigcap \mathscr{Z}_1\right) \bigcup \left(\mathscr{Z}_1^{-q} \bigcap \mathscr{Z}_2\right) \bigcup \left(\mathscr{Z}_1^{-q} \bigcap C_s\right) \bigcup \left(\mathscr{Z}_1^{-q} \bigcap C_{s-\frac{(a+1)q-a}{\rho}}\right) \\
& \left(-qC_{s-\frac{(a+1)q-a}{\rho}} \bigcap \mathscr{Z}_1\right) \bigcup \left(-qC_{s-\frac{(a+1)q-a}{\rho}} \bigcap \mathscr{Z}_2\right) \bigcup \left(-qC_{s-\frac{(a+1)q-a}{\rho}} \bigcap C_s\right) \bigcup \\
& \left(-qC_{s-\frac{(a+1)q-a}{\rho}} \bigcap C_{s-\frac{(a+1)q-a}{\rho}}\right) \bigcup \left(\mathscr{Z}_2^{-q} \bigcap C_s\right) \bigcup \left(\mathscr{Z}_2^{-q} \bigcap C_{s-\frac{(a+1)q-a}{\rho}}\right) \bigcup \\
& \left(\mathscr{Z}_2^{-q} \bigcap \mathscr{Z}_1\right) \bigcup \left(\mathscr{Z}_2^{-q} \bigcap \mathscr{Z}_2\right)
\end{aligned}$$

From (1), one knows that $\mathscr{Z}_1^{-q} \bigcap \mathscr{Z}_1 = \emptyset$. It follows from Lemma 10, one obtains that

$$\begin{aligned}
&-qC_s \bigcap C_s = C_s, \quad -qC_s \bigcap \mathscr{Z}_1 = \emptyset, \\
&-qC_s \bigcap C_{s-\frac{(a+1)q-a}{\rho}} = \emptyset, \quad -qC_s \bigcap \mathscr{Z}_2 = \emptyset, \\
&\mathscr{Z}_1^{-q} \bigcap C_s = \emptyset, \quad \mathscr{Z}_1^{-q} \bigcap C_{s-\frac{(a+1)q-a}{\rho}} = C_{s-\frac{(a+1)q-a}{\rho}}, \\
&-qC_{s-\frac{(a+1)q-a}{\rho}} \bigcap \mathscr{Z}_1 = C_{s-\frac{aq+a+1}{\rho}}, \quad -qC_{s-\frac{(a+1)q-a}{\rho}} \bigcap \mathscr{Z}_2 = \emptyset, \\
&-qC_{s-\frac{(a+1)q-a}{\rho}} \bigcap C_s = \emptyset, \quad -qC_{s-\frac{(a+1)q-a}{\rho}} \bigcap C_{s-\frac{(a+1)q-a}{\rho}} = \emptyset, \\
&\mathscr{Z}_2^{-q} \bigcap C_s = \emptyset, \quad \mathscr{Z}_2^{-q} \bigcap C_{s-\frac{(a+1)q-a}{\rho}} = \emptyset.
\end{aligned}$$

Now we only have to prove that $\mathscr{Z}_1^{-q} \bigcap \mathscr{Z}_2 = \mathscr{Z}_2^{-q} \bigcap \mathscr{Z}_1 = \emptyset$ and $\mathscr{Z}_2^{-q} \bigcap \mathscr{Z}_2 = \emptyset$.

Suppose $\mathscr{Z}_1 \bigcap \mathscr{Z}_2^{-q} \neq \emptyset$, then there exist two integers i and j, where $1 \leqslant i \leqslant \frac{(a+1)q-a}{\rho} - 1$ and $\frac{(a+1)q-a}{\rho} + 1 \leqslant j \leqslant \frac{(2a+1)q+1}{\rho} - 1$ such that

$$s - i \equiv -q(s-j)q^{2k} \mod n,$$

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

(I) If $k = 0$, then it is equivalent to

$$\rho(qj + i) \equiv 0 \mod q^2 + 1.$$

As $1 \leqslant i \leqslant \frac{(a+1)q-a}{\rho} - 1$ and $\frac{(a+1)q-a}{\rho} + 1 \leqslant j \leqslant \frac{(2a+1)q+1}{\rho} - 1$, obviously, $\rho \leqslant \rho i \leqslant (a+1)q - a - \rho$ and $(a+1)q - a + \rho \leqslant \rho j \leqslant (2a+1)q + 1 - \rho$. We now divide into the following subcases.

(i) If $(a+1)q - a + \rho \leqslant \rho j \leqslant (a+2)q - a - 1$, then

$$(a+1)q^2 + (\rho - a)q + \rho \leqslant \rho(qj + i) \leqslant (a+2)q^2 - a - \rho.$$

Hence, $0 < (\rho - a)(q+1) - 1 \leqslant \rho(qj+i) - (a+1)(q^2+1) \leqslant q^2 - 2a - \rho - 1 < q^2 + 1$, which is a contradiction.

(ii) If $wq - a \leqslant \rho j \leqslant (w+1)q - a - 1$, where $w = a+2, a+3, \ldots, 2a-1$. Then

$$wq^2 - aq + \rho \leqslant \rho(qj + i) \leqslant (w+1)q^2 - a - \rho.$$

So $-(q^2+1) < -aq + \rho - w \leqslant \rho(qj+i) - w(q^2+1) \leqslant q^2 - a - \rho - w < q^2 + 1$, which implies that $w(q^2+1) = \rho(qj+i)$. Writing ρi in the form $\rho i = uq + v$, where $u = 0$, $\rho \leqslant v \leqslant q-1$; $1 \leqslant u \leqslant a-1$, $0 \leqslant v \leqslant q-1$; $u = a$, $0 \leqslant v \leqslant q - a - \rho$. Hence, $w(q^2+1) = (\rho j + u)q + v$. By the division algorithm, it must be $wq = \rho j + u$, which contradicts to the form of q.

(iii) If $2aq - a \leqslant \rho j \leqslant (2a+1)q - \rho + 1$, then

$$2aq^2 - aq \leqslant \rho(qj+i) \leqslant (2a+1)q^2 + (a - \rho + 2)q - a - \rho.$$

So $-(q^2+1) < -aq - 2a \leqslant \rho(qj+i) - 2a(q^2+1) \leqslant q^2 + (a - \rho + 2)q - 3a - \rho < q^2 + 1$, which implies that $2a(q^2+1) = \rho(qj+i) = (\rho j + u)q + v$. By the division algorithm, it must be $2aq = \rho j + u$, which also contradicts to the form of q.

(II) If $k = 1$, then $s - i \equiv -(s-j)q^3 \mod n$, which is equivalent to

$$\rho qj \equiv \rho i \mod q^2 + 1.$$

Similar to the above discussion, this case is impossible.

Finally, suppose $\mathscr{Z}_2^{-q} \bigcap \mathscr{Z}_2 \neq \emptyset$, then there exist two integers i and j, where $\frac{(a+1)q-a}{\rho} + 1 \leqslant i,j \leqslant \frac{(2a+1)q+1}{\rho} - 1$ such that

$$s - i \equiv -q(s-j)q^{2k} \mod n,$$

for $k \in \{0, 1\}$. Going on the line of the proofs similar to the above cases, one can get such case is impossible either.

Therefore,

$$\begin{aligned}\mathscr{Z}^{-q} \bigcap \mathscr{Z} =& C_s \bigcup C_{s-\frac{aq+a+1}{\rho}} \bigcup C_{s-\frac{(a+1)q-a}{\rho}}\\ =& \left\{ s, s \pm \frac{aq+a+1}{\rho}, s \pm \frac{(a+1)q-a}{\rho} \right\},\end{aligned}$$

which means that $|\mathscr{Z}^{-q} \bigcap \mathscr{Z}| = 5$.

(3) This case can be proved by using the same method, we omit it here for simplification.

Theorem 6 *Let q be an odd prime power with the form $q = 2\rho m + 2a + 1$, where $\rho = a^2 + (a+1)^2$, and $a \geqslant 2, m$ is a positive integer. Let $n = \frac{q^2+1}{\rho}$. Then there exist q-ary EAQMDS codes with the following parameters*:

(1) $[[n, n - 2d + 3, d; 1]]$, *where* $2 \leqslant d \leqslant \frac{(2a+2)q-2a}{\rho}$ *is even*;

(2) $[[n, n - 2d + 7, d; 5]]$, *where* $\frac{(2a+2)q-2a}{\rho} + 2 \leqslant d \leqslant \frac{(4a+2)q+2}{\rho}$ *is even*;

(3) $[[n, n - 2d + 11, d; 9]]$, *where* $\frac{(4a+2)q+2}{\rho} + 2 \leqslant d \leqslant \frac{(4a+4)q-4a}{\rho}$ *is even.*

Proof Let $\mathscr{C}$ be a cyclic code of length n over $\mathbb{F}_{q^2}$ with defining set $\mathscr{Z} = \bigcup_{i=0}^{\delta} C_{s-i}$, where $0 \leqslant \delta \leqslant \frac{(2a+2)q-2a}{\rho} - 1$. From Lemma 9, we can see that $\mathscr{Z}$ consists of $2\delta + 1$ consecutive integers $\{s - \delta, \ldots, s-1, s, s+1, \ldots, s+\delta\}$, which implies that $\mathscr{C}$ has minimum distance at least $2\delta + 2$ from Theorem 2. Hence, $\mathscr{C}$ is a q^2-ary cyclic code with parameters $[n, n - (2\delta+1), \geqslant 2\delta + 2]$. According to Lemma 11,

$$c=|\mathscr{Z}^{-q}\bigcap\mathscr{Z}|=\begin{cases}1, & 0\leqslant\delta\leqslant\frac{(a+1)q-a}{\rho}-1;\\ 5, & \frac{(a+1)q-a}{\rho}\leqslant\delta\leqslant\frac{(2a+1)q+1}{\rho}-1;\\ 9, & \frac{(2a+1)q+1}{\rho}\leqslant\delta\leqslant\frac{(2a+2)q-2a}{\rho}-1.\end{cases}$$

Combining Theorem 3 with the EA-quantum Singleton bound, there are q-ary EAQMDS codes with parameters as desired. The result follows.

Similar to the discussions of the case $q=2\rho m+2a+1$, we have the following results for $q=2\rho m-2a-1$.

Lemma 12 *Let q be an odd prime power with the form $q=2\rho m-2a-1$, where $\rho=a^2+(a+1)^2$, and $a\geqslant 2, m$ is a positive integer. Let $n=\frac{q^2+1}{\rho}$, $s=\frac{n}{2}$. Then*

(1) $-qC_s=C_s$;
(2) $-qC_{s-\frac{(a+1)q+a}{\rho}}=C_{s-\frac{aq-a-1}{\rho}}$;
(3) $-qC_{s-\frac{(2a+1)q-1}{\rho}}=C_{s-\frac{q+2a+1}{\rho}}$.

Lemma 13 *Let q be an odd prime power with the form $q=2\rho m-2a-1$, where $\rho=a^2+(a+1)^2$, and $a\geqslant 2, m$ is a positive integer. Let $n=\frac{q^2+1}{\rho}$, and $s=\frac{n}{2}$. If $\mathscr{C}$ is a cyclic code of length n over $\mathbb{F}_{q^2}$ with defining set $\mathscr{Z}=\bigcup_{i=0}^{\delta}C_{s-i}$, then*

$$|\mathscr{Z}^{-q}\bigcap\mathscr{Z}|=\begin{cases}1, & 0\leqslant\delta\leqslant\frac{(a+1)q+a}{\rho}-1;\\ 5, & \frac{(a+1)q+a}{\rho}\leqslant\delta\leqslant\frac{(2a+1)q-1}{\rho}-1;\\ 9, & \frac{(2a+1)q-1}{\rho}\leqslant\delta\leqslant\frac{(2a+2)q+2a}{\rho}-1.\end{cases}$$

Theorem 7 *Let q be an odd prime power with the form $q=2\rho m-2a-1$, where $\rho=a^2+(a+1)^2$, and $a\geqslant 2, m$ is a positive integer. Let $n=\frac{q^2+1}{\rho}$. Then there exist q-ary EAQMDS codes with the following parameters*:

(1) $[[n,n-2d+3,d;1]]$, *where* $2\leqslant d\leqslant\frac{(2a+2)q+2a}{\rho}$ *is even*;
(2) $[[n,n-2d+7,d;5]]$, *where* $\frac{(2a+2)q+2a}{\rho}+2\leqslant d\leqslant\frac{(4a+2)q-2}{\rho}$ *is even*;
(3) $[[n,n-2d+11,d;9]]$, *where* $\frac{(4a+2)q-2}{\rho}+2\leqslant d\leqslant\frac{(4a+4)q+4a}{\rho}$ *is even.*

Remark 3 Let $a=2$, then $\rho=13$, $n=\frac{q^2+1}{13}$. EAQMDS codes of length $n=\frac{q^2+1}{13}$ with $c=1$, $c=5$ and $c=9$ had been also constructed in [43] from cyclic codes (please see Table 1), where $q=26m+5$ and $26m+21$. It is easy to see that our results coincide with theirs, in other words, we also generalize the results in [43].

Example 2 Let $a=3$, then $\rho=25$, $n=\frac{q^2+1}{25}$. EAQMDS code of length $n=\frac{q^2+1}{25}$ are constructed. We list some new EAQMDS codes obtained from Theorems 6 and 7 in Table 4.

Table 4 New entanglement-assisted quantum MDS codes

n	q	Parameters $[[n,k,d;c]]_q$	d
$\frac{q^2+1}{25}$	43	$[[74,77-2d,d;1]]_{43}$	$2 \leqslant d \leqslant 14$ is even
		$[[74,81-2d,d;5]]_{43}$	$16 \leqslant d \leqslant 24$ is even
		$[[74,85-2d,d;9]]_{43}$	$26 \leqslant d \leqslant 28$ is even
	57	$[[130,133-2d,d;1]]_{57}$	$2 \leqslant d \leqslant 18$ is even
		$[[130,137-2d,d;5]]_{57}$	$20 \leqslant d \leqslant 32$ is even
		$[[130,141-2d,d;9]]_{57}$	$34 \leqslant d \leqslant 36$ is even
	107	$[[458,461-2d,d;1]]_{107}$	$2 \leqslant d \leqslant 34$ is even
		$[[458,465-2d,d;5]]_{107}$	$36 \leqslant d \leqslant 60$ is even
		$[[458,469-2d,d;9]]_{107}$	$62 \leqslant d \leqslant 68$ is even
	157	$[[986,989-2d,d;1]]_{157}$	$2 \leqslant d \leqslant 50$ is even
		$[[986,993-2d,d;5]]_{157}$	$52 \leqslant d \leqslant 88$ is even
		$[[986,997-2d,d;9]]_{157}$	$90 \leqslant d \leqslant 100$ is even
$\frac{q^2+1}{41}$	73	$[[130,133-2d,d;1]]_{73}$	$2 \leqslant d \leqslant 18$ is even
		$[[130,137-2d,d;5]]_{73}$	$20 \leqslant d \leqslant 32$ is even
		$[[130,141-2d,d;9]]_{73}$	$34 \leqslant d \leqslant 36$ is even
	173	$[[730,733-2d,d;1]]_{173}$	$2 \leqslant d \leqslant 42$ is even
		$[[730,737-2d,d;5]]_{173}$	$44 \leqslant d \leqslant 76$ is even
		$[[730,741-2d,d;9]]_{173}$	$78 \leqslant d \leqslant 84$ is even
	337	$[[2770,2773-2d,d;1]]_{337}$	$2 \leqslant d \leqslant 82$ is even
		$[[2770,2777-2d,d;5]]_{337}$	$84 \leqslant d \leqslant 148$ is even
		$[[2770,2781-2d,d;9]]_{337}$	$150 \leqslant d \leqslant 164$ is even
	401	$[[3922,3925-2d,d;1]]_{401}$	$2 \leqslant d \leqslant 98$ is even
		$[[3922,3929-2d,d;5]]_{401}$	$100 \leqslant d \leqslant 176$ is even
		$[[3922,3933-2d,d;9]]_{401}$	$178 \leqslant d \leqslant 196$ is even

5 Conclusion

In this paper, EAQMDS codes of length $n = \frac{q^2+1}{\rho}$ have been constructed by exploiting less pre-shared maximally entangled states c, i.e., $c = 0, 1, 4, 5, 8, 9$, where $\rho = a^2 + (a+1)^2$ and $a \geqslant 2$ is a positive integer. Comparing their parameters with all known EAQMDS codes, one can obtain that they are new in the sense that their parameters are not covered by the codes available in the literature, except $a = 2$, which is indeed the results obtained in [43].

Author Contributions All authors contributed to the study conception and design. The first draft of the manuscript was written by Sujuan Huang and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding The work was supported by the National Natural Science Foundation of China (12271137, U21A20428, 61972126).

Declarations

Conflicts of interest/Competing interests The authors have no conflicts of interest to declare that are relevant to the content of this article.

References

1. Allahmadi, A., Alkenani, A., Hijazi, R., Muthana, H., Özbudak, F., Solé, P.: New constructions of entanglement-assisted quantum codes. Cryptogr. Commun. **14**, 15–37 (2022)
2. Brun, T.A., Devetak, I., Hsieh, M.H.: Correcting quantum errors with entanglement. Science **314**(5798), 436–439 (2006)
3. Cao, M.: MDS codes with Galois hulls of arbitrary dimensions and the related entanglement-assisted quantum error correction. IEEE Trans. Inf. Theory. **67**(12), 7964–7984 (2021)
4. Chen, J., Chen, Y., Feng, C., Huang, Y., Chen, R.: Some new classes of entanglement-assisted quantum MDS codes derived from constacyclic codes. IEEE Access. **7**, 91679–91695 (2019)
5. Chen, J., Chen, Y., Yu, D., Feng, C., Huang, Y., Chen, R.: Applications of constacyclic codes to some new entanglement-assisted quantum MDS codes. IEEE Access **7**, 136641–136657 (2019)
6. Chen, J., Huang, Y., Feng, C., Chen, R.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. Quantum Inf. Process. **16**(303), 1–22 (2017)
7. Chen, X., Zhu, S., Kai, X.: Entanglement-assisted quantum MDS codes constructed from constacyclic codes. Quantum Inf. Process. **17**, 273 (2018)
8. Chen, X., Zhu, S., Kai, X.: Entanglement-assisted quantum negacyclic BCH codes. Int. J. Theor. Phys. **58**(5), 1509–1523 (2019)
9. Fang, W., Fu, F., Li, L., Zhu, S.: Euclidean and Hermitian hulls of MDS codes and their applications to EAQECCs. IEEE Trans. Inf. Theory **66**(6), 3572–3537 (2020)
10. Fujiwara, Y., Clark, D., Vandendriessche, P., De Boeck, M., Tonchev, V.D.: Entanglement-assisted quantum low-density parity-check codes. Phys. Rev. A **82**, 042338 (2010)
11. Galindo, C., Hernando, F., Matsumoto, R., Ruano, D.: Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. Quantum Inf. Process. **18**, 116 (2019)
12. Gao, Y., Yue, Q., Huang, X., Zhang, J.: Hulls of generalized Reed-Solomon codes via Goppa codes and their applications to quantum codes. IEEE Tran. Inf. Theory **67**(10), 6619–6626 (2021)
13. Grassl, M.: Entanglement-assisted quantum communication beating the quantum Singleton bound. Phys. Rev. A **103**, L060201 (2021)
14. Grassl, M., Huber, F., Winter, A.: Entropic proofs of Singleton bounds for quantum error-correcting codes. IEEE Tran. Inf. Theory **68**(6), 3942–3950 (2022)
15. Guenda, K., Jitman, S., Gulliver, T.A.: Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr. **86**(1), 121–136 (2018)
16. Guo, L., Li, R.: Linear plotkin bound for entanglement-assisted quantum codes. Phys. Rev. A **87**, 032309 (2013)
17. Guo, G., Li, R., Guo, L.: On the construction of quantum MDS codes. Int. J. Theor. Phys. **57**, 3525–3539 (2018)
18. Hsieh, M.H., Brun, T.A., Devetak, I.: Entanglement-assisted quantum quasi-cyclic low-density parity-check codes. Phys. Rev. A **79**, 032340 (2009)
19. Hsieh, M.H., Devetak, I., Brun, T.A.: General entanglement-assisted quantum error-correcting codes. Phys. Rev. A **76**, 064302 (2007)
20. Kai, X., Zhu, S., Li, P.: Constacyclic codes and some new quantum MDS codes. IEEE Trans. Inf. Theory **60**(4), 2080–2086 (2014)
21. Koroglu, M.E.: New entanglement-assisted MDS quantum codes from constacyclic codes. Quantum Inf. Process. **18**, 44 (2019)
22. Krishna, A., Sarwate, D.V.: Pseudocyclic maximum-distance-separable codes. IEEE Trans. Inf. Theory **36**(4), 880–884 (1990)
23. La Guardia, G.G.: New quantum MDS codes. IEEE Trans. Inf. Theory **57**(8), 5551–5554 (2011)
24. Lai, C.Y., Ashikhmin, A.: Linear programming bounds for entanglement-assisted quantum error-correcting codes by split weight enumerators. IEEE Trans. Inf. Theory **64**(1), 622–639 (2018)
25. Lai, C.Y., Brun, T.A.: Entanglement-assisted quantum error-correcting codes with imperfect ebits. Phys. Rev. A **86**, 032319 (2012)
26. Lai, C.Y., Brun, T.A.: Entanglement increases the error-correcting ability of quantum error-correcting codes. Phys. Rev. A **88**, 012320 (2013)
27. Lai, C.Y., Brun, T.A., Wilde, M.M.: Dualities and identities for entanglement-assisted quantum codes. Quantum Inf. Process. **13**, 957–990 (2014)
28. Li, L., Zhu, S., Liu, L., Kai, X.: Entanglement-assisted quantum MDS codes from generalized Reed-Solomon codes. Quantum Inf. Process. **18**(5), 153 (2019)
29. Li, R., Guo, G., Song, H., Liu, Y.: New constructions of entanglement-assisted quantum MDS codes from negacyclic codes. Int. J. Quantum Inf. **17**(3), 1950022 (2019)

30. Liu, X., Yu, L., Hu, P.: New entanglement-assisted quantum codes from *k*-Galois dual codes. Finite Fields Appl. **55**, 21–32 (2019)
31. Liu, Y., Li, R., Lv, L., Ma, Y.: Applications of constacyclic codes to entanglement-assited quantum maximum distance separable codes. Quantum Inf. Process. **17**, 210 (2018)
32. Lu, H., Kai, X., Zhu, S.: Construction of new entanglement-assisted quantum MDS codes via cyclic codes. Quantum Inf. Process. **21**, 206 (2022)
33. Lu, L., Li, R.: Entanglement-assisted quantum codes constructed from primitive quaternary BCH codes. Int. J. Quantum Inf. **12**(3), 1450015 (2014)
34. Lu, L., Li, R., Guo, L., Ma, Y., Liu, Y.: Entanglement-assisted quantum MDS codes from negacyclic codes. Quantum Inf. Process. **17**, 69 (2018)
35. Lu, L., Ma, W., Li, R., Ma, Y., Liu, Y., Cao, H.: Entanglement-assisted quantum MDS codes from constacyclic codes with large minimum distance. Finite Fields Appl. **53**, 309–325 (2018)
36. Luo, G., Cao, X.: Two new families of entanglement-assisted quantum MDS codes from generalized Reed-Solomon codes. Quantum Inf. Process. **18**(3), 89 (2019)
37. Luo, G., Cao, X., Chen, X.: MDS codes with hulls of arbitrary dimensions and their quantum error correction. IEEE Trans. Inf. Theory. **65**(5), 2944–2952 (2019)
38. Qian, J., Zhang, L.: Entanglement-assisted quantum codes from arbitrary binary linear codes. Des. Codes Cryptogr. **77**(1), 193–202 (2015)
39. Qian, J., Zhang, L.: On MDS linear complementary dual codes and entanglement-assisted quantum codes. Des. Codes Cryptogr. **86**(7), 1565–1572 (2018)
40. Qian, J., Zhang, L.: Constructions of new entanglement-assisted quantum MDS and almost MDS codes. Quantum Inf. Process. **18**, 71 (2019)
41. Sari, M., Kolotoğlu, E.: An application of constacyclic codes to entanglement-assisted quantum MDS codes. Computat. Appl. Math. **8**, 75 (2019)
42. Shin, J., Heo, J., Brun, T.A.: Entanglement-assisted codeword stabilized quantum codes. Phys. Rev. A **84**, 062321 (2011)
43. Tian, F., Zhu, S., Sun, Z., Li, F.: Some new entanglement-assisted quantum MDS codes with length $\frac{q^2+1}{13}$. Int. J. Theor. Phys. **60**, 1843–1857 (2021)
44. Wilde, M.M., Brun, T.A.: Optimal entanglement formulas for entanglement-assisted quantum coding. Phys. Rev. A **77**, 064302 (2008)
45. Wang, L., Zhu, S., Sun, Z.: Entanglement-assisted quantum MDS codes from cyclic codes. Quantum Inf. Process. **19**, 65 (2020)

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