Designs, Codes and Cryptography (2024) 92:1163–1174
https://doi.org/10.1007/s10623-023-01335-0

New entanglement-assisted quantum error-correcting codes from negacyclic codes

Xiaojing Chen[1] · Xingbo Lu[1] · Shixin Zhu[2,3] · Wan Jiang[4] · Xindi Wang[1]

Received: 15 March 2022 / Revised: 1 November 2023 / Accepted: 3 November 2023 /
Published online: 8 December 2023
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract

Entanglement-assisted quantum error-correcting (EAQEC) codes are a generalization of quantum error-correcting (QEC) codes, which can be constructed from arbitrary classical linear codes by relaxing the dual-containing condition and by using preshared entangled states between the sender and the receiver. In this paper, we investigate EAQEC codes of length $n = \frac{2(q^2+1)}{a}$, where q is an odd prime power, $a = m^2 + 1$ and m is an odd integer. The resulting EAQEC codes are entanglement-assisted quantum maximum-distance-separable (EAQMDS) codes when the minimum distance $d \leq \frac{n+2}{2}$.

Keywords EAQEC codes · Negacyclic codes · EAQMDS codes · Defining set

Mathematics Subject Classification 94B15 · 81T08

Communicated by J. Bierbrauer.

✉ Xindi Wang
xindi.wang@ahu.edu.cn

Xiaojing Chen
chenxiaojing0909@ahu.edu.cn

Xingbo Lu
xingbolu@yeah.net

Shixin Zhu
zhushixin@hfut.edu.cn

Wan Jiang
jiangw000@163.com

[1] School of Internet, Anhui University, Hefei 230039, Anhui, China

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

[3] Key Laboratory of Knowledge Engineering with Big Data, Ministry of Education, Hefei University of Technology, Hefei 230601, Anhui, China

[4] School of Computer and Information, Hefei University of Technology, Hefei 230601, Anhui, China

1 Introduction

As a powerful tool to protect quantum information from decoherence and quantum noise, quantum error-correcting (QEC) codes have been used for a long time. Nowadays, it was shown that QEC codes can be derived from some linear codes satisfying certain dual-containing conditions [3, 32, 33]. However, many classical linear codes with good performance are usually not dual-containing, and they thus cannot be used to produce QEC codes. A natural problem is to construct QEC codes or generalized QEC codes from arbitrary linear codes. In 2006, Brun *et al.* [2] proved that nondual-containing quaternary linear codes can be applied to construct so-called entanglement-assisted quantum error-correcting (EAQEC) codes with the help of preshared entanglement, which contains QEC codes as a special subclass. Generally, we use $[[n, k, d; c]]_q$ to denote a q-ary EAQEC code that encodes k information qubits into n channel qubits with the help of c pairs of maximally entangled states and can correct up to $\lfloor \frac{d-1}{2} \rfloor$ qubit errors, where d is the minimum distance of this EAQEC code.

After that, many interesting methods and EAQEC codes were proposed and constructed in [4, 10–12, 19–21, 27, 30, 34, 37]. Moreover, it should be noted that the key to these methods and constructions is to determine the number of necessary entangled states. One effective way is to decompose the defining set of a linear code, which can transmit the original computational task into determining a subset of the defining set of the underlying codes. The whole process of development of this approach can be summarized as follows. First, by decomposing the defining set of primitive quaternary BCH codes, Lü *et al.* [22] constructed some EAQEC codes with good parameters. Subsequently, Chen *et al.* [5] and Chen *et al.* [6] generalized this method to negacyclic codes and constacyclic codes, respectively. As a result, many EAQEC codes with good parameters have been constructed in this way in the literature (see, for example, [14, 18, 23–26, 36]).

However, one can find that more entangled states need to be employed as the minimum distances of the EAQEC codes increase. Thus, there are always trade-offs among the parameters of an EAQEC code, one of which is the so-called entanglement-assisted quantum Singleton bound (see Lemma 1 in this paper). An $[[n, k, d; c]]_q$ EAQEC code that achieves this bound with equality is called an entanglement-assisted quantum maximum-distance-separable (EAQMDS) code, which has the largest error-correcting ability for fixed n, k, and c. Therefore, there is always a major enthusiasm for constructing new EAQMDS codes. Let us note that much progress has been made on this topic. In [31], Qian *et al.* constructed some EAQMDS codes of length $n = q^2 + 1$. Later, Wang *et al.* [35] further employed constacyclic codes (including cyclic codes) to obtain several classes of EAQMDS codes with more general parameters of length $n = q^2 + 1$; this achievement, contains almost all the known results about EAQMDS codes of the same length. In [38], Zhu *et al.* constructed new EAQMDS codes of length $n = \frac{q^2+1}{5}$. In [7], Chen *et al.* obtained new EAQMDS codes of lengths $n = \frac{q^2+1}{a}$, $n = q^2 + 1$, and $n = \frac{q^2+1}{2}$ from cyclic codes, where $a = m^2 + 1$ ($m \geq 1$ is odd) and q is odd satisfying $a \mid (q + m)$ or $a \mid (q - m)$. Very recently, Pang *et al.* [29] also derived some new EAQMDS codes of lengths $n = q^2 + 1$ and $n = \frac{q^2+1}{2}$ from negacyclic codes and constacyclic codes.

Summarizing the above results, we see easily that the lengths of the known EAQMDS codes are a divisor of $q^2 + 1$. Enlightened by these works, we construct four families of EAQEC codes of length $n = \frac{2(q^2+1)}{a}$ from negacyclic codes, where q is odd, $a = m^2 + 1$ and m is an odd integer. For ease of reference, we list them in Table 1. As a result, many

Table 1 The parameters of EAQEC codes of length $n = \frac{2(q^2+1)}{a}$

$[[n, k, d; c]]_q$	q	m	ξ
$k = n - 4\alpha q + 4(a - m)(\alpha - \xi) + 2a\alpha^2 - 2a + 4m - 1$		$m \equiv 1 \bmod 4$	odd
$d = 2[\alpha q + (a - m)\xi + a - 2m + 1]$	$q = a\xi - m$		
$c = 2\alpha[(a\alpha + 2(a - m)] + 2a - 4m + 1$		$m \equiv 3 \bmod 4$	even
$k = n - 4\alpha q + 4(a - m)(\alpha - \xi) + 2a\alpha^2 - 2a + 4m - 2$		$m \equiv 1 \bmod 4$	even
$d = 2[\alpha q + (a - m)\xi + a - 2m + 1]$	$q = a\xi - m$		
$c = 2\alpha[(a\alpha + 2(a - m)] + 2a - 4m$		$m \equiv 3 \bmod 4$	odd
$k = n - 4\alpha q + 4m(\alpha - \xi) + 2a\alpha^2 - 1$		$m \equiv 1 \bmod 4$	odd
$d = 2(\alpha q + m\xi + 1)$	$q = a\xi + m$		
$c = 2\alpha(a\alpha + 2m) + 1$		$m \equiv 3 \bmod 4$	even
$k = n - 4\alpha q + 4m(\alpha - \xi) + 2a\alpha^2 - 2$		$m \equiv 1 \bmod 4$	even
$d = 2(\alpha q + m\xi + 1)$	$q = a\xi + m$		
$c = 2\alpha(a\alpha + 2m)$		$m \equiv 3 \bmod 4$	odd

EAQMDS codes with minimum distance $d \leq \frac{n+2}{2}$ can be immediately deduced and we present some specific examples in Table 2.

This paper is organized as follows. In Sect. 2, we review some basic results about negacyclic codes. Section 3 contains some basic notation on EAQEC codes. In Sect. 4, we construct four families of new EAQEC codes and EAQMDS codes from negacyclic codes with a unified form. Finally, Sect. 5 concludes the paper.

2 Review of negacyclic codes

In this section, we review some basic concepts and relevant results about negacyclic codes. Throughout this paper, let $\mathbb{F}_{q^2}$ be the finite field with q^2 elements and $\mathbb{F}_{q^2}^n$ be the n-dimensional row vector space over $\mathbb{F}_{q^2}$, where q is the power of a prime p and n is a positive integer. An $[n, k, d]_{q^2}$ linear code $\mathcal{C}$ is a k-dimensional linear subspace of $\mathbb{F}_{q^2}^n$ given by the minimum distance d. A q^2-ary linear code $\mathcal{C}$ of length n is negacyclic if $\mathcal{C}$ is invariant under the permutation of $\mathbb{F}_{q^2}^n$

$$(c_0, c_1, \dots, c_{n-1}) \rightarrow (-c_{n-1}, c_0, \dots, c_{n-2}).$$

One can identify any codeword $\mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$ with its polynomial representation $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in \mathbb{F}_{q^2}[x]/\langle x^n + 1\rangle$; thus, $\mathcal{C}$ is a q^2-ary negacyclic code of length n if and only if $\mathcal{C}$ is an ideal of the quotient ring $\mathbb{F}_{q^2}[x]/\langle x^n + 1\rangle$. Since each ideal of $\mathbb{F}_{q^2}[x]/\langle x^n + 1\rangle$ is principal, it implies that every negacyclic code $\mathcal{C}$ can be generated by a monic divisor $g(x)$ of $x^n + 1$. If there is a monic polynomial $g(x)$ with the minimal degree k that can generate a negacyclic code $\mathcal{C}$, then $g(x)$ is unique, and we call it the generator polynomial of $\mathcal{C}$. In this sense, we further denote $\mathcal{C} = \langle g(x)\rangle$ and note that the dimension of $\mathcal{C}$ is $n - k$.

For any element $a \in \mathbb{F}_{q^2}$, we denote the conjugate of a by $\overline{a} = a^q$. Let $\mathbf{x} = (x_0, x_1, \dots, x_{n-1})$ and $\mathbf{y} = (y_0, y_1, \dots, y_{n-1})$ be any two vectors in $\mathbb{F}_{q^2}^n$. The Hermitian inner product between $\mathbf{x}$ and $\mathbf{y}$ is defined by

$$\langle \mathbf{x}, \mathbf{y}\rangle_h = x_0\overline{y}_0 + x_1\overline{y}_1 + \cdots + x_{n-1}\overline{y}_{n-1}.$$

The vectors $\mathbf{x}$ and $\mathbf{y}$ are called orthogonal with respect to the Hermitian inner product if $\langle \mathbf{x}, \mathbf{y}\rangle_h = 0$. The Hermitian dual code of any linear code $\mathcal{C}$ is given by

$$\mathcal{C}^{\perp_h} = \{\mathbf{y} \in \mathbb{F}_{q^2}^n \mid \langle \mathbf{x}, \mathbf{y}\rangle_h = 0 \text{ for all } \mathbf{x} \in \mathcal{C}\}.$$

A linear code $\mathcal{C}$ is called Hermitian self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^{\perp_h}$, and it is called Hermitian self-dual if $\mathcal{C} = \mathcal{C}^{\perp_h}$.

From now on, we always assume that n is coprime to q (i.e., $\gcd(n, q) = 1$), which guarantees that $x^n + 1$ has no repeated root over $\mathbb{F}_{q^2}$. Let β be a primitive $2n$-th root of unity in $\mathbb{F}_{q^{2m}}$, where m is the multiplicative order of q^2 modulo $2n$. Then it is easily seen that $\gamma = \beta^2$ is a primitive n-th root of unity. Furthermore, all roots of $x^n + 1$ are $\beta\gamma^j = \beta^{1+2j}$ for $0 \leq j \leq n-1$. Let $\mathbb{Z}_{2n} = \{0, 1, \cdots, 2n-1\}$ and Ω_{2n} be the set of all odd integers from 1 to $2n$. For any $i \in \mathbb{Z}_{2n}$, let C_i be the q^2-cyclotomic coset modulo $2n$ containing i, that is,

$$C_i = \{i, iq^2, iq^4, \dots, iq^{2(l_i-1)}\},$$

where l_i is the smallest positive integer such that $iq^{2l_i} \equiv i \mod 2n$. Then, the minimal polynomial $M_i(x)$ of β^i over $\mathbb{F}_{q^2}$ can be expressed as $M_i(x) = \Pi_{t\in C_i}(x - \beta^t)$. For a

Table 2 Some EAQEC codes obtained from Theorems 5 and 7

q	$[[n, k, d; c]]_q$
3	$[[10, 1, 10; 9]]_3$
5	$[[26, 4, 16; 8]]_5$, $[[26, 0, 26; 24]]_5$
7	$[[50, 17, 22; 9]]_7$, $[[50, 5, 36; 25]]_7$, $[[50, 1, 50; 49]]_7$
11	$[[122, 65, 34; 9]]_{11}$, $[[122, 37, 56; 25]]_{11}$, $[[122, 17, 78; 49]]_{11}$
	$[[122, 5, 100; 81]]_{11}$, $[[122, 1, 122; 121]]_{11}$
13	$[[170, 100, 40; 8]]_{13}$, $[[170, 64, 66; 24]]_{13}$, $[[170, 36, 92; 48]]_{13}$
	$[[170, 16, 118; 80]]_{13}$, $[[170, 4, 144; 120]]_{13}$, $[[170, 0, 170; 168]]_{13}$
17	$[[58, 0, 58; 56]]_{17}$
23	$[[106, 21, 60; 33]]_{23}$, $[[106, 1, 106; 105]]_{23}$
31	$[[74, 1, 74; 73]]_{31}$
37	$[[274, 80, 126; 56]]_{37}$, $[[274, 20, 200; 144]]_{37}$, $[[274, 0, 274; 272]]_{37}$
43	$[[370, 181, 112; 33]]_{43}$, $[[370, 81, 198; 105]]_{43}$, $[[370, 21, 284; 217]]_{43}$, $[[370, 1, 370; 369]]_{43}$
47	$[[170, 1, 170; 169]]_{47}$,$[[442, 181, 160; 57]]_{47}$, $[[442, 81, 254; 145]]_{47}$
	$[[442, 21, 348; 273]]_{47}$, $[[442, 1, 442; 441]]_{47}$
73	$[[410, 52, 264; 168]]_{73}$, $[[410, 0, 410; 408]]_{73}$
83	$[[530, 209, 198; 73]]_{83}$, $[[530, 53, 364; 249]]_{83}$, $[[530, 1, 530; 529]]_{83}$
107	$[[458, 101, 244; 129]]_{107}$, $[[458, 1, 458; 457]]_{107}$
109	$[[914, 468, 260; 72]]_{109}$, $[[914, 208, 478; 248]]_{109}$, $[[914, 52, 696; 528]]_{109}$, $[[914, 0, 914; 912]]_{109}$
157	$[[986, 400, 358; 128]]_{157}$, $[[986, 100, 672; 456]]_{157}$, $[[986, 0, 986; 984]]_{157}$
193	$[[1490, 400, 718; 344]]_{193}$, $[[1490, 100, 1104; 816]]_{193}$, $[[1490, 0, 1490; 1488]]_{193}$

negacyclic code $\mathcal{C} = \langle g(x) \rangle$ of length n over $\mathbb{F}_{q^2}$, the set $Z = \{i \in \Omega_{2n} \mid g(\beta^i) = 0\}$ is said to be the defining set of $\mathcal{C}$. It is not difficult to verify that the defining set Z must be a union of some q^2-cyclotomic cosets modulo $2n$ and $\dim(\mathcal{C}) = n - |Z|$, where $|Z|$ denotes the cardinality of the set Z.

Finally, we end this section with two well-known bounds for arbitrary linear codes and negacyclic codes, namely, the Singleton bound and the BCH bound for negacyclic codes.

Theorem 1 [28] (Singleton bound) *Let $\mathcal{C}$ be an $[n, k, d]_{q^2}$ linear code. Then*

$$n - k \geq d - 1.$$

Moreover, if $n - k = d - 1$, then we call $\mathcal{C}$ a maximum-distance-separable (MDS) code.

From the property of pseudocyclic codes in [17], we obtain the following BCH bound of negacyclic codes.

Theorem 2 [17] (BCH bound for negacyclic codes) *We assume that n and q are coprime. Let $\mathcal{C}$ be a q^2-ary negacyclic code and its generator polynomial be $g(x)$. Let β be a primitive $2n$-th root of unity and b be an integer. If $g(x)$ have the elements $\{\beta^{1+2j} \mid b \leq j \leq b+\delta-2\}$ as roots, then the minimum distance of $\mathcal{C}$ is at least δ.*

3 Review of EAQEC codes

Let q be a prime power. A q-ary QEC code Q of length n and size K is a K-dimensional subspace of a q^n-dimensional Hilbert space $\mathbb{H}$=$\mathbb{C}^{q^n}$=$\mathbb{C}^q \otimes ... \otimes \mathbb{C}^q$ (see [1, 3, 16]). Let us recall that an $[[n, k, d; c]]_q$ EAQEC code $\mathcal{Q}$ can encode k information qubits into n channel qubits with the help of c pairs of maximally entangled states and can correct up to $\lfloor \frac{d-1}{2} \rfloor$ qubits errors, where d is the minimum distance of $\mathcal{Q}$. Huber and Grassl [13] proved that the parameters of an EAQEC code obey the following entanglement-assisted quantum Singleton bound. Grassl *et al*. [8] gave a proof of this bound for arbitrary q.

Lemma 1 [8, 13] (Entanglement-assisted quantum Singleton Bound) *Let $\mathcal{Q}$ be an $[[n, k, d; c]]_q$ EAQEC code. Then, the following holds:*

$$k \leq c + \max\{0, n - 2d + 2\}, \tag{1}$$

$$k \leq n - d + 1, \tag{2}$$

$$k \leq \frac{(n - d + 1)(c + 2d - 2 - n)}{3d - 3 - n}, \text{ if } 2d \geq n + 2. \tag{3}$$

An EAQMDS code is referred to as an EAQEC code satisfying Equation (1) or Equation (3) with equality, where $2d \leq n + 2$ or $2d \geq n + 2$, respectively.
As we mentioned before, the key in the construction of EAQEC codes is to determine the number of maximally entangled states, and a possible way is to decompose the defining set of a negacyclic code as follows.

Theorem 3 [14] *Let $\mathcal{C}$ be a q^2-ary negacyclic code of length n with a defining set Z. Suppose that $Z = Z_1 \cup Z_2$ is a decomposition of Z, where $Z_1 = Z \cap (-qZ)$, $Z_2 = Z \backslash Z_1$ and $-qZ = \{2n - qx \mid x \in Z\}$. If $\mathcal{C}$ has parameters $[n, n - |Z|, d]_{q^2}$, then there exists an EAQEC code with parameters $[[n, n - 2|Z| + |Z_1|, d; |Z_1|]]_q$.*

4 Construction of EAQMDS codes with new parameters

The main topic of this section is to give constructions of EAQEC codes with a unified form via classical negacyclic codes. Consequently, a family of new EAQMDS codes of length $n = \frac{2(q^2+1)}{a}$ with general parameters are presented, where q is an odd prime power, $a = m^2 + 1$ and m is an odd integer.

Lemma 2 *Let $n = \frac{2(q^2+1)}{a}$ and $s = \frac{n}{2}$, where q is an odd prime power, $a = m^2 + 1$, m is an odd integer, n is even and $s = n/2$ is odd. Then, the q^2-cyclotomic cosets modulo $2n$ are $C_s = \{s\}$, $C_{3s} = \{3s\}$ and $C_{s-2l} = \{s - 2l, s + 2l\}$ for $1 \le l \le s - 1$.*

Let us note that Lemma 2 is a parallel promotion of Lemma 4.1 in [15], so we omit its proof here for simplification.

We note that if $n = \frac{2(q^2+1)}{a}$, where q is an odd prime power, $a = m^2 + 1$ and $2 \mid a$, it implies that $q \equiv \pm m \bmod a$ and m is an odd integer. Next, we discuss all cases according to the various values of q and m.

Case I $q = a\xi - m$

The following theorem can be used to determine the number of c of an EAQEC code derived from a q^2-ary negacyclic code, where $q = a\xi - m$.

Theorem 4 *Let $n = \frac{2(q^2+1)}{a}$ and $s = \frac{n}{2}$, where $q = a\xi - m$ is an odd prime power, $a = m^2 + 1$ and m is an odd integer. For a nonnegative integer α with $0 \le \alpha \le \xi$, we suppose that $\mathcal{C}$ is a negacyclic code with a defining set Z given by*

$$Z = C_s \cup C_{s+2} \cup \cdots \cup C_{s+2[\alpha q + (a-m)\xi + a - 2m]}.$$

Let us define $Z_1 = Z \cap (-qZ)$. Then the following statements hold.

(1) *If $m \equiv 1 \bmod 4$ and ξ is an odd positive integer or $m \equiv 3 \bmod 4$ and ξ is an even positive integer, then $|Z_1| = 2\alpha[a\alpha + 2(a - m)] + 2a - 4m + 1$;*

(2) *If $m \equiv 1 \bmod 4$ and ξ is an even positive integer or $m \equiv 3 \bmod 4$ and ξ is an odd positive integer, then $|Z_1| = 2\alpha[a\alpha + 2(a - m)] + 2a - 4m$.*

Proof For brevity, we show the case where $m \equiv 1 \bmod 4$ and ξ is an odd positive integer of (1), and the other cases are similar. Since

$$Z = C_s \cup C_{s+2} \cup \cdots \cup C_{s+2[\alpha q + (a-m)\xi + a - 2m]},$$

we have

$$-qZ = -qC_s \cup -qC_{s+2} \cup \cdots \cup -qC_{s+2[\alpha q + (a-m)\xi + a - 2m]}.$$

For each $-qC_s$, by examining the intersection of Z and $-qC_s$, we obtain that

$$|Z \cap (-qZ)| = 2\alpha(a\alpha + 2a - 2m) + 2a - 4m + 1;$$

the detailed proof is technical and can be found in arXiv:2305.08517v1.

Keeping the definition of Z_1 in Theorem 3, we have

$$|Z_1| = |Z \cap (-qZ)| = 2\alpha(a\alpha + 2a - 2m) + 2a - 4m + 1.$$

This completes the proof. □

From Theorem 4 above, we obtain the first construction of EAQEC codes in the following theorem.

Theorem 5 *Let* $n=\frac{2(q^2+1)}{a}$ *and* $s=\frac{n}{2}$*, where* $q=a\xi-m$ *is an odd prime power,* $a=m^2+1$ *and* m *is an odd integer. Let* α *be a nonnegative integer satisfying* $0\le\alpha\le\xi$*. Then, the following statements hold.*

(1) *If* $m\equiv 1 \bmod 4$ *and* ξ *is an odd positive integer or* $m\equiv 3 \bmod 4$ *and* ξ *is an even positive integer, then there are EAQEC codes with parameters* $[[n,k,d;c]]_q$*, where*

$$\begin{aligned} k&=n-4\alpha q+4(a-m)(\alpha-\xi)+2a\alpha^2-2a+4m-1,\\ d&=2[\alpha q+(a-m)\xi+a-2m+1],\\ c&=2\alpha[a\alpha+2(a-m)]+2a-4m+1. \end{aligned}$$

(2) *If* $m\equiv 1 \bmod 4$ *and* ξ *is an even positive integer or* $m\equiv 3 \bmod 4$ *and* ξ *is an odd positive integer, then there are EAQEC codes with parameters* $[[n,k,d;c]]_q$*, where*

$$\begin{aligned} k&=n-4\alpha q+4(a-m)(\alpha-\xi)+2a\alpha^2-2a+4m-2,\\ d&=2[\alpha q+(a-m)\xi+a-2m+1],\\ c&=2\alpha[a\alpha+2(a-m)]+2a-4m. \end{aligned}$$

In addition, they are EAQMDS codes if $d\le\frac{n+2}{2}$.

Proof For brevity, let us just show the case where $m\equiv 1 \bmod 4$ and ξ is an odd positive integer of case (1) and the other cases are similar. For a nonnegative integer α with $0\le\alpha\le\xi$, we suppose that $\mathcal{C}$ is a negacyclic code of length n with a defining set

$$Z=C_s\cup C_{s+2}\cup\cdots\cup C_{s+2[\alpha q+(a-m)\xi+a-2m]},$$

where ξ, a, m, q and s are defined as above.

Then, the dimension of $\mathcal{C}$ is $n-2[\alpha q+(a+m)\xi]+4m-2a-1$. We observe that the negacyclic code $\mathcal{C}$ has $2[\alpha q+(a-m)\xi+a-2m]+1$ consecutive roots. Then, it follows from Theorem 2 that the minimum distance of $\mathcal{C}$ is at least $2[\alpha q+(a-m)\xi+a-2m+1]$. Hence, according to Theorem 1, $\mathcal{C}$ is an MDS code with parameters $[n,n-2[\alpha q+(a+m)\xi]+4m-2a-1,2[\alpha q+(a-m)\xi+a-2m+1]\,]_{q^2}$.

We note from Theorem 4 that $|Z_1|=2\alpha(a\alpha+2a-2m)+2a-4m+1$. Then Theorem 3 can produce EAQEC codes with parameters $[[n,k,d;c]]_q$, where

$$\begin{aligned} k&=n-4\alpha q+4(a-m)(\alpha-\xi)+2a\alpha^2-2a+4m-1,\\ d&=2[\alpha q+(a-m)\xi+a-2m+1],\\ c&=2\alpha[a\alpha+2(a-m)]+2a-4m+1. \end{aligned}$$

Moreover, it can be checked that

$$n+c-k=4[\alpha q+(a-m)\xi+a-2m+1]-2=2(d-1).$$

Therefore, it implies that the EAQEC codes are EAQMDS codes if $d\le\frac{n+2}{2}$ by Lemma 1. □

Case II $q=a\xi+m$

As for the case that $n=\frac{2(q^2+1)}{a}$ and $q=a\xi+m$, where $a=m^2+1$ and m is an odd integer, we can also obtain new EAQEC codes. The proof is similar to that in Case I, so we omit it here.

Theorem 6 *Let $n = \frac{2(q^2+1)}{a}$ and $s = \frac{n}{2}$, where $q = a\xi + m$ is an odd prime power, $a = m^2+1$ and m is an odd integer. For a nonnegative integer α with $0 \leq \alpha \leq \xi$, we suppose that $\mathcal{C}$ is a negacyclic code with a defining set Z given as follows*

$$Z = C_s \cup C_{s+2} \cup \cdots \cup C_{s+2[\alpha q + m\xi]}.$$

Let us define $Z_1 = Z \cap (-qZ)$. Then the following statements hold.

(1) *If $m \equiv 1 \bmod 4$ and ξ is an odd positive integer or $m \equiv 3 \bmod 4$ and ξ is an even positive integer, then $|Z_1| = 2\alpha(a\alpha + 2m) + 1$;*

(2) *If $m \equiv 1 \bmod 4$ and ξ is an even positive integer or $m \equiv 3 \bmod 4$ and ξ is an odd positive integer, then $|Z_1| = 2\alpha(a\alpha + 2m)$.*

Proof For brevity, we show the case $m \equiv 1 \bmod 4$ and ξ is an odd positive integer of case (1) and the other cases are similar. Since

$$Z = C_s \cup C_{s+2} \cup \cdots \cup C_{s+2[\alpha q + m\xi]}.$$

We have

$$-qZ = -qC_s \cup -qC_{s+2} \cup \cdots \cup -qC_{s+2[\alpha q + m\xi]}.$$

For each $-qC_s$, by examining the intersection of Z and $-qC_s$, we obtain that

$$|Z \cap (-qZ)| = 2\alpha(a\alpha + 2m) + 1;$$

the detailed proof is technical and can be found in arXiv:2305.08517v1.

Keeping the definition of Z_1 in Theorem 3, we have

$$|Z_1| = |Z \cap (-qZ)| = 2\alpha(a\alpha + 2m) + 1.$$

This completes the proof. □

From Theorem 6 above, we obtain the second construction of EAQEC codes in the following theorem.

Theorem 7 *Let $n = \frac{2(q^2+1)}{a}$ and $s = \frac{n}{2}$, where $q = a\xi + m$ is an odd prime power, $a = m^2+1$ and m is an odd integer. Let α be a nonnegative integer satisfying $0 \leq \alpha \leq \xi$. Then, the following statements hold.*

(1) *If $m \equiv 1 \bmod 4$ and ξ is an odd positive integer or $m \equiv 3 \bmod 4$ and ξ is an even positive integer, then there are EAQEC codes with parameters $[[n, k, d; c]]_q$, where*

$$\begin{aligned} k &= n - 4\alpha q + 4m(\alpha - \xi) + 2a\alpha^2 - 1, \\ d &= 2(\alpha q + m\xi + 1), \\ c &= 2\alpha(a\alpha + 2m) + 1. \end{aligned}$$

(2) *If $m \equiv 1 \bmod 4$ and ξ is an even positive integer or $m \equiv 3 \bmod 4$ and ξ is an odd positive integer, then there are EAQEC codes with parameters $[[n, k, d; c]]_q$, where*

$$\begin{aligned} k &= n - 4\alpha q + 4m(\alpha - \xi) + 2a\alpha^2 - 2, \\ d &= 2(\alpha q + m\xi + 1), \\ c &= 2\alpha(a\alpha + 2m). \end{aligned}$$

In addition, they are EAQMDS codes if $d \leq \frac{n+2}{2}$.

Proof For brevity, let us just show the case where $m \equiv 1 \bmod 4$ and ξ is an odd positive integer of case (1) and the other cases are similar. For a nonnegative integer α with $0 \le \alpha \le \xi$, we suppose that $\mathcal{C}$ is a negacyclic code of length n with a defining set

$$Z = C_s \cup C_{s+2} \cup \cdots \cup C_{s+2[\alpha q+m\xi]},$$

where ξ, a, m, q and s are defined as above.

Then, the dimension of $\mathcal{C}$ is $n - 2(\alpha q + m\xi) - 1$. We observe that the negacyclic code $\mathcal{C}$ has $2(\alpha q + m\xi) + 1$ consecutive roots. Then, it follows from Theorem 2 that the minimum distance of $\mathcal{C}$ is at least $2(\alpha q + m\xi + 1)$. Hence, according to Theorem 1, $\mathcal{C}$ is an MDS code with parameters $[n, n - 2(\alpha q + m\xi) - 1, 2(\alpha q + m\xi + 1)]_{q^2}$.

We note from Theorem 6 that $|Z_1| = 2\alpha(a\alpha + 2m) + 1$. Then Theorem 3 can produce EAQEC codes with parameters $[[n, k, d; c]]_q$, where

$$\begin{aligned} k = n - 4\alpha q + 4m(\alpha - \xi) + 2a\alpha^2 - 1, \\ d = 2(\alpha q + m\xi + 1), \\ c = 2\alpha(a\alpha + 2m) + 1. \end{aligned}$$

Moreover, it can be checked that

$$n + c - k = 4(\alpha q + m\xi + 1) - 2 = 2(d - 1).$$

Therefore, it implies that the EAQEC codes are EAQMDS codes if $d \le \frac{n+2}{2}$ by Lemma 1.

□

Remark 1 Some EAQEC codes obtained from Theorems 5 and 7 are listed in Table 2.

5 Conclusion

In this study, we construct four families of EAQEC codes with a unified length form $n = \frac{2(q^2+1)}{a}$ derived from negacyclic codes, where q is an odd prime power, a is determined as m^2+1, and m represents an odd integer. Furthermore, our EAQEC codes have larger minimum distances compared to those of the existing codes reported in the literature. This characteristic enhances their capability to detect and correct qubit errors effectively. In particular, new EAQMDS codes can be deduced from these EAQEC codes.

Acknowledgements The authors are grateful to the anonymous reviewers and the Editor, Prof. Saritha Anand, for their comments that much improved the presentation of this article. This research is supported by the National Natural Science Foundation of China (Nos. 12001002, U21A20428, 12171134, 61972126, 62202007, 62302003) and the Natural Science Foundation of Anhui Province (Nos. 2008085QA04, 2108085QA03).

References

1. Ashikhmin A., Knill E.: Nonbinary quantum stabilizer codes. IEEE Trans. Inf. Theory **47**(7), 3065–3072 (2001).
2. Brun T., Devetak I., Hsieh M.H.: Correcting quantum errors with entanglement. Science **314**(5798), 436–439 (2006).
3. Calderbank A.R., Rains E.M., Shor P.W., Sloane N.J.A.: Quantum error correction via codes over *GF*(4). IEEE Trans. Inf. Theory **44**(4), 1369–1387 (1998).

4. 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).
5. Chen J., Huang Y., Feng C., Chen R.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. Quant. Inf. Process. **16**(1–22), 303 (2017).
6. Chen X., Zhu S., Kai X.: Entanglement-assisted quantum MDS codes constructed from constacyclic codes. Quant. Inf. Process. **17**(10), 273(1-18) (2018).
7. Chen X., Zhu S., Jiang W.: Cyclic codes and some new entanglement-assisted quantum MDS codes. Des. Codes Cryptogr. **89**(11), 2533–2551 (2021).
8. Grassl M., Huber F., Winter A.: Entropic proofs of Singleton bounds for quantum error-correcting codes. IEEE Trans. Inf. Theory **68**(6), 3942–3950 (2022).
9. Grassl M.: Entanglement-assisted quantum communication beating the quantum Singleton bound. Phys. Rev. A **103**(1–5), L020601 (2021).
10. Guo L., Li R.: Linear Plotkin bound for entanglement-assisted quantum codes. Phys. Rev. A **87**(3), 032309 (2013).
11. Guenda K., Jitman S., Gulliver T.A.: Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr. **86**(1), 121–136 (2018).
12. Hsieh M.H., Devetak I., Brun T.: General entanglement-assisted quantum error-correcting codes. Phys. Rev. A **76**(6), 062313 (2007).
13. Huber F., Grassl M.: Quantum codes of maximal distance and highly entangled subspaces. Quantum **4**, 284 (2020).
14. Jiang W., Zhu S., Chen X.: Optimal entanglement-assisted quantum codes with larger minimum distance. IEEE Commun. Lett. **25**(1), 45–48 (2021).
15. Kai X., Zhu S.: New quantum MDS codes from negacyclic codes. IEEE Trans. Inf. Theory **59**(2), 1193–1197 (2013).
16. Ketka A., Klappenecker A., Kumar S., Sarvepalli P.K.: Nonbinary stabilizer codes over finite fields. IEEE Trans. Inf. Theory **52**(11), 4892–4914 (2006).
17. Krishna A., Sarwate D.V.: Pseudocyclic maximum-distance-separable codes. IEEE Trans. Inf. Theory **36**(4), 880–884 (1990).
18. Koroglu M.E.: New entanglement-assisted MDS quantum codes from constacyclic codes. Quant. Inf. Process. **18**(1–28), 44 (2019).
19. Luo G., Cao X.: Two new families of entanglement-assisted quantum MDS codes from generalized Reed-Solomon codes. Quant. Inf. Process. **18**(1–12), 89 (2019).
20. 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).
21. Lai C.Y., Brun T.A., Wilde M.M.: Duality in entanglement-assisted quantum error correction. IEEE Trans. Inf. Theory **59**(6), 4020–4024 (2013).
22. Lu L., Li R.: Entanglement-assisted quantum codes constructed from primitive quaternary BCH codes. Int. J. Quant. Inf. **12**(3), 1450015 (1-14) (2014).
23. Lu L., Li R., Guo L., Ma Y., Liu Y.: Entanglement-assisted quantum MDS codes from negacyclic codes. Quant. Inf. Process. **17**(1–23), 69 (2018).
24. 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).
25. Li R., Guo G., Song H., Liu Y.: New constructions of entanglement-assisted quantum MDS codes from negacyclic codes. Int. J. Quant. Inf. **17**(3), 1950022 (2019).
26. Liu Y., Li R., Lu L., Ma Y.: Applications of constacyclic codes to entanglement-assisted quantum maximum distance separable codes. Quant. Inf. Process. **17**(1–19), 210 (2018).
27. Liu X., Yu L., Hu P.: New entanglement-assisted quantum codes from k-Galois dual codes. Finite Fields Appl. **55**, 21–32 (2019).
28. MacWilliams F., Sloane N.: The Theory of Error Correcting Codes. North-Holland, Amsterdam (1977).
29. Pang B., Zhu S., Li F., Chen X.: New entanglement-assisted quantum MDS codes with larger minimum distance. Quant. Inf. Process. **19**(1–18), 207 (2020).
30. Qian J., Zhang L.: On MDS linear complementary dual codes and entanglement-assisted quantum codes. Des. Codes Cryptogr. **86**(7), 1565–1572 (2018).
31. Qian J., Zhang L.: Constructions of new entanglement-assisted quantum MDS and almost MDS codes. Quant. Inf. Process. **18**(1–12), 71 (2019).
32. Steane A.M.: Error correcting codes in quantum theory. Phys. Rev. Lett. **77**(5), 793–797 (1996).
33. Shor P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A **52**(4), 2493–2496 (1995).
34. Wilde M.M., Brun T.A.: Optimal entanglement formulas for entanglement-assisted quantum coding. Phys. Rev. A **77**(6), 064302 (2008).

35. Wang J., Li R., Lv J., Guo G., Liu Y.: Entanglement-assisted quantum error correction codes with length $n = q^2 + 1$. Quant. Inf. Process. **18**(1–21), 292 (2019).
36. Wang L., Zhu S., Sun Z.: Entanglement-assisted quantum MDS codes from cyclic codes. Quant. Inf. Process. **19**(1–18), 265 (2020).
37. Wang G., Tang C.: Application of GRS codes to some entanglement-assisted quantum MDS codes. Quant. Inf. Process. **21**(1–16), 98 (2022).
38. Zhu S., Jiang W., Chen X.: New entanglement-assisted quantum MDS codes with length $\frac{q^2+1}{5}$. Quant. Inf. Process. **19**(7), 211(1-15) (2020).

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

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.