Constructions of New Entanglement-Assisted Quantum Codes

Jianfa Qian\textsuperscript{1a}, Lina Zhang\textsuperscript{2b}

\textsuperscript{1}School of Mathematics and Big Data, Huizhou University
Huizhou 516007, Guangdong, P. R. China
\textsuperscript{2}School of Mathematics and Big Data, Huizhou University
Huizhou 516007, Guangdong, P. R. China
\textsuperscript{a}qianjianfa2013@126.com \textsuperscript{b}lina222zhang@126.com

ABSTRACT: Entanglement-assisted quantum error-correcting codes are considered as a new research direction of quantum coding theory. In this work, based on cyclic codes, we present the constructions of new entanglement-assisted quantum error-correcting codes. Several new families of nonbinary entanglement-assisted quantum error-correcting codes with length $n=2(q-1)$ can be efficiently constructed.

1. INTRODUCTION

In the field of quantum error correction, the discovery of entanglement-assisted quantum error-correcting (EAQEC, for short) codes is regarded as an important breakthrough. Over the years, the theory of EAQEC codes has been highly developed. New research methods and theories have been put forward (see, for example, in [1-18], and the relevant references therein).

As is known to all, EAQEC codes use pre-existing entanglement between the sender and receiver to increase the transmission rate. Moreover, any linear code can be used to construct EAQEC codes. However, the ebits $c$ of EAQEC codes is difficult to calculate. Thus, it is very important to design a good method to calculate the ebits $c$.

In this work, based on the forerunners research, we propose the constructions of new entanglement-assisted quantum codes. Several new families of nonbinary entanglement-assisted quantum codes with length $n=2(q-1)$ can be easily constructed, and the ebits $c$ of EAQEC codes can be easily calculated.

The work is organized as follows. In section 2, we state some basic definitions and properties of linear codes and EAQEC codes. In section 3, we construct several new families of EAQEC codes. In section 4, a conclusion of this work is given.

2. PRELIMINARIES

2.1 Classical linear codes

In this subsection, we refer to the literatures [19, 20] for basic concepts and facts about linear codes and cyclic codes.

Let $F_q$ be the Galois field with $q$ elements. Recall that a linear code $C=[n,k,d]_q$ over $F_q$ with length $n$ is a linear subspace of $F_q^n$, where $d$ is the minimum Hamming distance of $C$.

For $x=(x_1,x_2,\cdots,x_n)$ and $y=(y_1,y_2,\cdots,y_n)$ in $F_q^n$, the Euclidean inner product of $x$ and $y$ is defined as
The dual code $C^\perp$ of $C$ is defined by

$$C^\perp = \{ x \mid x \cdot y = 0, \forall y \in C \}.$$ 

In the following, we recall some basic concepts on cyclic codes over the finite field $F_q$ (see [19, 20]).

Recall that a cyclic code $C$ of length $n$ can be generated by a monic polynomial $g(x)$, where $g(x)$ is a factor of $x^n - 1$.

For $0 \leq j \leq n - 1$, let $C_j = \{ j, jq, \ldots, jq^{t-1} \}$ be the $q$-cyclotomic coset $C_j$ modulo $n$, where $t$ is the smallest positive integer such that $jq^t \equiv j \pmod{n}$. As usual, $j$ is the smallest positive integer of this coset. It is easy to check that the defining set $T$ of a cyclic code $C$ is a union of some $q$-cyclotomic cosets modulo $n$.

**Proposition 2.1 (BCH bound) [19, 20]:** Suppose that $C$ is a cyclic code of length $n$ with defining set $T$. Let $d$ be an integer, where $2 \leq d \leq n$. If $T$ contains $d - 1$ consecutive elements, then the minimum distance of $C$ is at least $d$.

**2.2 Entanglement-assisted quantum error-correcting codes**

In this subsection, we refer [4, 7, 12] for basic concepts and facts about EAQEC codes.

Let $Q$ denote an $[[n, k, d; c]]$ EAQEC code. Recall that $Q$ can encode $k$ logical qubits into $n$ physical qubits with the help of $c$ pairs of maximally entangled Bell states, and corrects up to at least $(1 - 1/2^d)$ quantum errors.

EAQEC codes use pre-existing entanglement between the sender and receiver to increase the transmission rate. Research shows that the performance of some EAQEC codes is better than quantum error-correcting codes. However, the ebits $c$ of EAQEC codes is difficult to calculate. Based on the decomposition of defining set of cyclic codes, a new method for constructing EAQEC codes is proposed in [8, 21].

The following Lemma and Theorem show how to construct EAQEC codes derived from the decomposition of defining set of cyclic codes.

**Lemma 2.1 [8, 21]:** Let $C$ be an $[[n, k, d; c]]$ cyclic code with defining set $T$. Suppose the decomposition of $T$ is $T = T_c \cup T_a$, where $T_c = T \cap T_a$ and $T_a = T \setminus T_c$. Denote the cyclic codes with defining set $T_c$ and $T_a$ be $C_c$ and $C_a$, respectively. Then $C_c^\perp \subseteq C_a^\perp$.

**Theorem 2.1 [8, 21]:** Let $C$ be an $[[n, k, d; c]]$ cyclic code with defining set $T$. Suppose the decomposition of $T$ is $T = T_c \cup T_a$, where $T_c = T \cap T_a$ and $T_a = T \setminus T_c$. Then there exists an EAQEC code with parameters $[[n, n-2 | T_c \cap T_a | + | T_c, | T_a, | d, | T_c, |]]_q$.

**3. Construction of EAQEC Codes**

In this section, based on the decomposition of defining set of cyclic codes, we present the constructions of new EAQEC codes of length $n = 2(q-1)$ over $F_q$. Throughout this work, we assume that $q$ is an odd prime power and $n = 2(q-1)$. Note that $q$ is an odd prime power, we have $ord(q) = 2$. This implies that each $q$-cyclotomic coset modulo $n$ contains one or two elements (see [22, 23]). Next, we distinguish two cases for $q = 1 \pmod{4}$ with $q = 3 \pmod{4}$.

A. $q \equiv 1 \pmod{4}$

In this subsection, we construct three classes of new entanglement-assisted quantum codes.

**Theorem 3.1:** Let $n = 2(q-1)$, where $q = 1 \pmod{4}$. Then there exists an EAQEC code with parameters

$$[[n, n-3q-1, \geq q^3/2, 1]]_q.$$ 

**Proof:** Let
Let \( T = C_q \cup C_{1} \cup \cdots \cup C_{(q-3)/2} \) be the defining set of a cyclic code \( C \) of length \( n=2(q-1) \) over \( F_q \). From the BCH bound, we know that the minimum distance is at least \( \frac{q+3}{2} \).

On the other hand, it is easy to check that \( -C_{i+1} = C_{q-i} \) and \( -C_{2j} = C_{a-2j} \), where \( 1 \leq i \leq (q-1)/2 \) and \( 0 \leq j \leq q-2 \).

Thus, one has \( |T|=1 \) and \( |T|=(3q+1)/4 \). By Theorem 2.1, there exists an \( \left[ n, n - \frac{3q-1}{2}, \geq \frac{q+3}{2}, 1 \right]_q \) EAQEC code.

**Theorem 3.2:** Let \( n=2(q-1) \), where \( q \equiv 1(\text{mod} \ 4) \). Then there exists an EAQEC code with parameters \( \left[ n, n - \frac{3q-1}{2}, \geq \frac{q+5}{2}, 5 \right]_q \).

**Proof:** Let
\[
T = C_q \cup C_{1} \cup \cdots \cup C_{(q-1)/2} \cup C_{(q+1)/2}
\]
be the defining set of a cyclic code \( C \) of length \( n=2(q-1) \) over \( F_q \). From the BCH bound for cyclic codes, we know that the minimum distance is at least \( \frac{q+5}{2} \).

It is easy to check that \( -C_{(q-3)/2} = C_{(q+1)/2} \). Thus, one has
\[
|T|=5 \text{ and } |T|=3(q+3)/4 .
\]
By Theorem 2.1, there exists an \( \left[ n, n - \frac{3q-1}{2}, \geq \frac{q+5}{2}, 5 \right]_q \) EAQEC code.

**Theorem 3.3:** Let \( n=2(q-1) \), where \( q \geq 7 \) and \( q \equiv 1(\text{mod} \ 4) \). Then there exists an EAQEC code with parameters \( \left[ n, 1, \geq \frac{q}{2}, q \right]_q \).

**Proof:** Let
\[
T = C_q \cup C_{1} \cup \cdots \cup C_{q-1} \cup C_{q-2}
\]
be the defining set of a cyclic code \( C \) of length \( n=2(q-1) \) over \( F_q \). From the BCH bound, we know that the minimum distance is at least \( q \).

Similar to the proof of Theorem 3.1, we have \( |T|=q \) and \( |T|=3(q-1)/2 \). Thus, by Theorem 2.1, there exists an \( \left[ n, 1, \geq \frac{q}{2}, q \right]_q \) EAQEC code.

Now, let us give an illustrative example.

**Example 3.1:** Let \( q=17 \). Then, \( n=2(q-1)=32 \).

1. Let \( T_1 = C_q \cup C_1 \cup \cdots \cup C_4 \) be the defining set of a cyclic code \( C \). Applying Theorem 3.1, we can obtain an EAQEC code with parameters \( \left[ 32, 7, \geq 10, 1 \right]_q \).

2. Let \( T_2 = C_q \cup C_1 \cup \cdots \cup C_8 \cup C_9 \) be the defining set of a cyclic code \( C \). Applying Theorem 3.2, we can obtain an EAQEC code with parameters \( \left[ 32, 7, \geq 11, 5 \right]_q \).

3. Let \( T_3 = C_q \cup C_1 \cup \cdots \cup C_{16} \) be the defining set of a cyclic code \( C \). Applying Theorem 3.3, we can obtain an EAQEC code with parameters \( \left[ 32, 1, \geq 17, 17 \right]_q \).

**B. \( q \equiv 3(\text{mod} \ 4) \)**

In this subsection, we construct three classes of new entanglement-assisted quantum codes.

**Theorem 3.4:** Let \( n=2(q-1) \), where \( q \equiv 3(\text{mod} \ 4) \). Then there exists an EAQEC code with parameters \( \left[ n, n - \frac{3q-7}{2}, \geq \frac{q+1}{2}, 1 \right]_q \).

**Proof:** Let
\[
T = C_q \cup C_1 \cup \cdots \cup C_{(q-3)/2}
\]
be the defining set of a cyclic code $C$ of length $n=2(q-1)$ over $F_q$. By the BCH bound for cyclic codes, we know that the minimum distance is at least $\frac{q+1}{2}$. Obviously, $-C_{2i-1} = C_{2i-2}$ and $-C_{2i} = C_{2i-1}$, where $1 \leq i \leq (q-1)/2$ and $0 \leq j \leq q-2$.

Thus, one has $|T_1|=1$ and $|T|= (3q-5)/4$. By Theorem 2.1, there exists an $[[n, n-\frac{3q-7}{2}, \geq \frac{q+1}{2}]]_q$ EAQEC code.

**Theorem 3.5:** Let $n=2(q-1)$, where $q \equiv 3 \pmod{4}$. Then there exists an EAQEC code with parameters $[[n, n-\frac{3q-7}{2}, \geq \frac{q+1}{2}]]_q$.

**Proof:** Let $T = C_1 \cup C_2 \cup \cdots \cup C_{(q-1)/2}$ be the defining set of a cyclic code $C$ of length $n=2(q-1)$ over $F_q$. From the BCH bound, we know that the minimum distance is at least $\frac{q+3}{2}$. It is easy to check that $-C_{(q-1)/2} = C_{(q-1)/2}$. Thus, one has $|T|=3$. It is easy to check that $|T|= 3(q+1)/4$. By Theorem 2.1, there exists an $[[n, n-\frac{3q-7}{2}, \geq \frac{q+1}{2}]]_q$ EAQEC code.

**Theorem 3.6:** Let $n=2(q-1)$, where $q \geq 7$ and $q \equiv 3 \pmod{4}$. Then there exists an EAQEC code with parameters $[[n, n-\frac{3q-7}{2}, \geq \frac{q+1}{2}]]_q$.

**Proof:** Let $T = C_1 \cup C_2 \cup \cdots \cup C_{(q-3)/2} \cup C_{q/2}$ be the defining set of a cyclic code $C$ of length $n=2(q-1)$ over $F_q$. From the BCH bound, we know that the minimum distance is at least $q$. Similar to the proof of Theorem 3.4, we have $|T|=q$ and $|T|= 3(q+1)/2$.

Thus, by Theorem 2.1, there exists an $[[n, n-\frac{3q-7}{2}, \geq \frac{q+1}{2}]]_q$ EAQEC code.

Now, let us give an illustrative example.

**Example 3.2:** Let $q=19$. Then, $n=2(q-1)=36$.

1. Let $T_1 = C_1 \cup C_2 \cup \cdots \cup C_q$ be the defining set of a cyclic code $C$. Applying Theorem 3.4, we can obtain an EAQEC code with parameters $[[36, 11, \geq 10; 1]]$.

2. Let $T_2 = C_1 \cup C_2 \cup \cdots \cup C_{q-1} \cup C_q$ be the defining set of a cyclic code $C$. Applying Theorem 3.5, we can obtain an EAQEC code with parameters $[[36, 9, \geq 11; 3]]$.

3. Let $T_3 = C_1 \cup C_2 \cup \cdots \cup C_q$ be the defining set of a cyclic code $C$. Applying Theorem 3.6, we can obtain an EAQEC code with parameters $[[36, 1, \geq 19; 19]]$.

Finally, we present two families of linear complementary dual codes and construct two families of maximal entanglement entanglement-assisted quantum codes.

Recall that a linear code $C$ is called linear complementary dual if $C \cap C^\perp = \{0\}$ (see [24]).

For an $[[n, k, d; c]]$ EAQEC code, if $c=n-k$, it is called a maximal-entanglement EAQEC code (see [10, 11]).

**Theorem 3.7:** Let $n=2(q-1)$, where $q \geq 5$ is an odd prime power.

1. There exists a linear complementary dual code with parameters $[n, n-5, \geq 4]_q$.

2. There exists a linear complementary dual code with parameters $[n, n-7, \geq 6]_q$.

**Proof:** (1) Let $T = C_1 \cup C_{q-1} \cup C_{q+1}$.
be the defining set of a cyclic code $C$ of length $n=2(q-1)$ over $F_q$. Note that

$$C_1 = \{1, q\}, \quad C_2 = \{q - 2, 2q - 3\}, \quad \text{and} \quad C_{q+1} = \{q - 1\}.$$ 

From the BCH bound, we know that the minimum distance is at least 4.

On the other hand, it is easy to check that

$$-C_i = C_{q+2} \quad \text{and} \quad -C_{q+1} = C_{q+1}.$$ 

Thus, one has $T = -T$ and $T_r = T_r$. Then $C \cap C^\bot = \{0\}$. Therefore, there exists a linear complementary dual code with parameters $[n, n-5, \geq 4]_q$.

(2) Let

$$T = C_1 \cup C_{q-3} \cup C_{q-2} \cup C_{q+1} \cup C_{q+1}$$

be the defining set of a cyclic code $C$ of length $n=2(q-1)$ over $F_q$. Note that

$$C_1 = \{1, q\}, \quad C_2 = \{q - 3\}, \quad C_{q-2} = \{q - 2, 2q - 3\}, \quad C_{q+1} = \{q - 1\}, \quad \text{and} \quad C_{q+2} = \{q + 1\}.$$ 

On the other hand, it is easy to check that

$$-C_i = C_{q+2}, \quad -C_{q+1} = C_{q+1}, \quad \text{and} \quad -C_{q-2} = C_{q+1}.$$ 

Similar to the above proof, there exists a linear complementary dual code with parameters $[n, n-7, \geq 6]_q$.

Remark 3.1: In [22], let $n=2(q-1)$, and

$$T = C_q \cup C_1 \cup C_3 \cup C_4,$$

La Guardia obtained a cyclic code with parameters $[n, n-7, \geq 6]_q$. However, our cyclic code with parameters $[n, n-7, \geq 6]_q$ is a linear complementary dual code.

In [10, 11], based on quaternary codes and Hermitian construction, researchers obtained many good binary maximal entanglement EAQEC codes. Here, based on Theorem 2.1 and Theorem 3.7, we will obtain two families of nonbinary maximal entanglement EAQEC codes from linear complementary dual codes.

Theorem 3.8: Let $n=2(q-1)$, where $q \geq 5$ is an odd prime power. Then there exist two $q$-ary maximal entanglement EAQEC codes $[[n, n-5, \geq 4;5]]_q$ and $[[n, n-7, \geq 6;7]]_q$.

4. CONCLUSION

In this work, based on classical cyclic codes, we have presented the constructions of entanglement-assisted quantum codes. Many new nonbinary entanglement-assisted quantum codes can be efficiently constructed.

For further researches, one can use other classes of cyclic codes to construct new entanglement-assisted quantum codes.

ACKNOWLEDGMENTS

This work was supported by the Characteristic Innovation Project of Guangdong Provincial Department of Education (2017KTSCX173) and the Foundation for Professor and Doctoral of Huizhou University (2016JB005).

REFERENCES

[1] Bowen, G. 2002. Entanglement required in achieving entanglement-assisted channel capacities. Phys. Rev. A, 66, 052313(1-9).

[2] Brun, T. A., Devetak, I., and Hsieh, M. H. 2006. Correcting quantum errors with entanglement. Science, 314, 436-439.

[3] Hsieh, M. H., Yen, W. T., and Hsu, L. Y. 2011. High performance entanglement-assisted quantum LDPC codes need little entanglement. IEEE Trans. Inf. Theory, 57, 1761-1769.
[4] Fujiwara, Y., Clark, D., Vandendriessche, P., Boeck, M. D., and Tonchev, V. D. 2010. Entanglement-assisted quantum low-density parity-check codes. Phys. Rev. A, 82, 042338(1-19).

[5] Wilde, M. M., and Brun, T. A. 2008. Optimal entanglement formulas for entanglement-assisted quantum coding. Phys. Rev. A, 77, 064302(1-4).

[6] Hsieh, M. H., Yen, W. T., and Hsu, L. Y. 2011. High performance entanglement-assisted quantum LDPC codes need little entanglement. IEEE Trans. Inf. Theory, 57, 1761-1769.

[7] Lai, C. Y., Brun, T. A., and Wilde, M. M. 2013. Duality in entanglement-assisted quantum error correction. IEEE Trans. Inf. Theory, 59, 4020-4024.

[8] Lu, L., and Li, R. 2014. Entanglement-assisted quantum codes constructed from primitive quaternary BCH codes. Int. J. Quantum Inf., 12, 1450015.

[9] Li, R., Li, X., and Guo, L. 2015. On entanglement-assisted quantum codes achieving the entanglement-assisted Griesmer bound. Quantum Inform. Process., 14, 4427-4447.

[10] Lu, L., Li, R., Guo, L., and Fu, Q. 2015. Maximal entanglement-assisted entanglement-assisted quantum codes constructed from linear codes. Quantum Inform. Process., 14, 165-182.

[11] Guo, L., Fu, Q., Li, R., and Lu, L. 2015. Maximal entanglement-assisted entanglement-assisted quantum codes of distance three. Int. J. Quantum Inf., 13, 1550002 (1-7).

[12] Fan, J., Chen, H., and Xu, J. 2016. Construction of q-ary entanglement-assisted quantum MDS codes with minimum distance greater than q + 1. Quantum Inf. Comput., 16, pp.423-434.

[13] Guenda, K., Jitman, S., and Gulliver, T. A. 2018. Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr., 86, 121-136.

[14] Chen, J., Huang, Y., Feng, C., and Chen, R. 2017. Entanglement-assisted quantum MDS codes constructed from constacyclic codes. Quantum Inform. Process., 16, 303.

[15] Chen, X., Zhu, S., and Kai, X. 2018. Entanglement-assisted quantum MDS codes constructed from constacyclic codes. Quantum Inform. Process., DOI=https://doi.org/10.1007/s11128-018-2044-1.

[16] Liu, Y., Li, R., Lv, L., and Ma, Y. 2018. Application of constacyclic codes to entanglement-assisted quantum maximum distance separable codes. Quantum Inf Process., DOI=https://doi.org/10.1007/s11128-018-1978-7.

[17] Qian, J., and Zhang, L. 2015. Entanglement-assisted quantum codes from arbitrary binary linear codes. Des. Codes Cryptogr., 77, 193-202.

[18] Qian, J., and Zhang, L. 2018. On MDS linear complementary dual codes and entanglement-assisted quantum codes. Des. Codes Cryptogr., 86, 1565-1572.

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

[20] Huffman, W. C., and Pless, V. 2003. Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge.

[21] Li, R., Xu, G., and Lu, L. 2013. Decomposition of defining sets of BCH codes and its applications. J. Air Force Engineering University (Natural Science Edition) (In Chinese), 14, 86-89.

[22] La Guardia, G. G. 2016. On optimal constacyclic codes, Linear Algebra and Its Applications, 496, 594-610.

[23] La Guardia, G. G. 2014. On the construction of nonbinary quantum BCH codes. IEEE Trans. Inf. Theory, 60, 1528-1535.

[24] Massey, J. L. 1992. Linear codes with complementary duals. Discrete Mathematics, 106/107, 337-342.