International Journal of Theoretical and Mathematical Physics 2023, 13(1): 15-19
DOI: 10.5923/j.ijtmp.20231301.03

Some New MDS LCD Codes and Entanglement-Assisted Quantum Codes from Constacyclic Codes

Xiaomeng Li, Shibo Wang, Wenting Chen, Jiantao Li*

School of Mathematics and Statistics, Liaoning University, Shenyang, China

Abstract In this paper, several classes of linear complementary dual codes and entanglement-assisted quantum codes with good parameters are constructed. The parameters of these codes are not covered by existing results.

Keywords Linear complementary dual codes, Entanglement-assisted quantum MDS codes, Constacyclic codes

1. Introduction

Linear complementary dual (LCD) codes are widely used in communication systems, storage systems, cryptography, and consumer electronics. In 1992, Massey [1] introduced the concept of LCD codes. In [2], Sendrier proved that LCD codes meet the asymptotic Gilbert-Varshamov bound. In [3], Yang and Massey provided a sufficient and necessary condition for a cyclic code to be an LCD code. In [4], Dinh showed that if $\lambda^2 \neq 1$, then any λ−constacyclic code over F_q is an LCD code. In [5], J. Qian et al. constructed MDS LCD codes of length q^2+1 and so on. Extensive work has been done on the construction of LCD codes using different methods (see, for example, [6,7]).

In addition, there is a close connection between LCD codes and entanglement-assisted quantum codes. If the intersection of a nontrivial α−constacyclic code and its Hermitian dual code is empty, then maximal entanglement EAQEC codes can be constructed and achieve the EA-hashing bound asymptotically [8]. For more information on EAQEC codes, see [9-14].

In this paper, based on the above results, we first construct three types of maximal distance separable (MDS) linear complementary dual codes. Then we construct some maximal entanglement MDS EAQEC codes from LCD codes.

The paper is organized as follows. In Section 2, some basic definitions and properties of linear codes and constacyclic codes are given. In Section 3, the constructions of MDS LCD codes are presented. In Section 4, some MDS EAQEC codes with maximal entanglement are constructed. Section 5 gives a summary.

* Corresponding author:
lijiantao@lnu.edu.cn (Jiantao Li)
Received: Jun. 29, 2023; Accepted: Jul. 12, 2023; Published: Jul. 24, 2023
Published online at http://journal.sapub.org/ijtmp

2. Preliminaries

Let F_{q^2} be a finite field with q^2 elements, where q is a power of a prime p. Now, we present some basic notions and facts about linear codes and constacyclic codes.

Definition 2.1 A code C is cyclic if for any cyclic shift of a codeword is also a codeword, i.e.,

$c = (c_0, c_1, \cdots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, \cdots, c_2) \in C$.

It is well-known that a cyclic code of length n over F_q can be identified with an ideal in the residue ring $F_q[x]/(x^n - 1)$. It follows that C is generated by a monic polynomial $g(x)$, of lowest degree in C. This polynomial $g(x)$ is called the generator polynomial of C, and $g(x)$ is a monic divisor of $x^n - 1$. The dimension of C is $n - k$, where $k = \deg(g(x))$.

A code C is called a λ-constacyclic code if $(c_0, c_1, \cdots, c_{n-1}) \in C \Rightarrow (\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in C$.

It is well known that the λ-constacyclic code C of length n over F_{q^2} is an ideal of the quotient ring $F_{q^2}[x]/(x^n - \lambda)$. Let r be the order of λ in the multiplicative group $F_{q^2}^*$. Then, there exists a primitive rn-th root β of unity in some extension field of F_{q^2} such that $\beta^n = \lambda$. Therefore, the roots of $x^n - \lambda$ are precisely the elements β^{1+ri}, where $0 \leq i \leq n-1$. Define $\Delta_{r,n} = \{1 + ri \mid 0 \leq i \leq n-1\}$. Let $C = \langle g(x) \rangle$ be an λ-constacyclic code of length n. Then the set $T = \{j \in \Delta_{r,n} \mid g(\beta^j) = 0\}$ is called the defining set of C.

Let n be a positive integer with $\gcd(n, q) = 1$. For $i \in \Delta_{r,n}$, the q^2-cyclotomic coset modulo rn containing an element i is defined as $\mathbb{C}_i = \{i, iq^2, iq^4, \cdots, iq^{2(t-1)}\}$, where t is the smallest positive integer such that $iq^{2t} \equiv i(mod\ rn)$. It is easy to see that the defining set T is a union of some q^2-cyclotomic cosets. The cyclotomic cosets are very important in constructing cyclic codes [15,16].

Definition 2.2 For any $x \in F_{q^2}$, the conjugate $\bar{x}$ of x is defined as x^q. For two vectors $x = (x_1, x_2, \cdots, x_n)$ and $y = (y_1, y_2, \cdots, y_n)$ in $F_{q^2}^n$, their Hermitian inner product is

defined as

$\langle x, y\rangle_h = x_1\bar{y}_1 + x_2\bar{y}_2 + \cdots + x_n\bar{y}_n = x_1y_1^q + x_2y_2^q + \cdots + x_ny_n^q$.

And $C^{\perp_h} = \left\{x \in F_{q^2}^n \mid \langle x, y\rangle_h = 0, y \in C\right\}$ is called the Hermitian dual code of C.

Definition 2.3 If $C \cap C^{\perp_h} = \{0\}$, then the linear code C is called a Hermitian linear complementary dual code.

The following results are often used to construct LCD codes, see [4,5] for example.

Lemma 2.1 Let $\alpha \in F_{q^2}^*$ be a primitive r-th root of unity and C be a nontrivial α- constacyclic code of length n over F_{q^2}. If $\alpha = \bar{\alpha}^{-1}$, i.e., $r \nmid (q+1)$, then $C \cap C^{\perp_h} = \{0\}$.

Proposition 2.1 (Singleton bound) If an $[n, k, d]_q$ linear code C exists, $1 \le d \le n-1$, then $n \ge k + d - 1$.

If $d = n - k + 1$, then C is called a maximum distance separable (MDS, for short) code.

Proposition 2.2 (BCH bound) Assume that n and q are relatively prime. Let C be an α- constacyclic code of length n over F_{q^2}. If the generator polynomial $g(x)$ of C has roots $\{\beta^{1+ri} \mid 0 \le i \le \delta - 2\}$, where β is a primitive rn-th root of unity, then the minimum distance of C is at least δ.

3. Constructions of MDS LCD Codes

3.1. MDS LCD Codes for $q \equiv 1$ (*mod* 4)

In this subsection, assume that $q \equiv 1(mod\ 4)$, $n = \frac{q^2-1}{4}$, $r = 4$. Obviously, $r \nmid (q+1)$, $r|q-1$. Let $\alpha \in F_{q^2}^*$ be a primitive r-th root of unity. Notice that $n = \frac{q^2-1}{4}$, $ord_{rn}(q^2) = 1$, so the q^2-cyclotomic coset modulo rn contains only one element. Let $u = \frac{n}{2}$. Then

$C_u = \{u\},\ C_{u-ri} = \{u - ri\},\ 1 \le i \le \left[\frac{u-1}{r}\right]$.

Theorem 3.1 Let $q \equiv 1(mod\ 4)$, $n = \frac{q^2-1}{4}$, $r = 4$, $\alpha \in F_{q^2}^*$ be a primitive r-th root of unity. Then there exists an α -constacyclic MDS LCD code with parameters $[n, n-\delta-1, \delta+2]_{q^2},\ 0 \le \delta \le \left[\frac{u-1}{r}\right]$.

Proof Let $\alpha \in F_{q^2}^*$ be a primitive r-th root of unity. Let C be an α-constacyclic code with defining set

$T = \cup_{i=0}^{\delta} C_{u-ri},\ 0 \le \delta \le \left[\frac{u-1}{r}\right]$.

It follows from $r \nmid (q+1)$ that C is an LCD code. Note that $C_u = \{u\}$, $C_{u-ri} = \{u - ri\}$. So, the dimension k of C is $n - \delta - 1$. According to Proposition 2.2, the minimum distance $d \ge \delta + 2$. It follows from Proposition 2.1 that $d = \delta + 2$. Hence C is an MDS LCD code with parameters $[n, n-\delta-1, \delta+2]_{q^2}$.

Example 3.1 Let $q = 13$, $n = 42$, $r = 4$, α be a primitive 4-th root of unity. Let C be an α-constacyclic code with defining set $T = \cup_{i=0}^{\delta} C_{21-ri}$, $0 \le \delta \le 5$. Then there exists MDS LCD codes with parameters $[42, 41-\delta, \delta+2]_{q^2}, 0 \le \delta \le 5$. In particular, let $\delta = 5$, we can obtain MDS LCD codes with parameters $[42, 36, 7]$.

3.2. MDS LCD Codes for $q \equiv 3$ (*mod* 4), $q \ne 3$

In this subsection, let $q \equiv 3(mod\ 4)$, $q \ne 3$, $n = \frac{q^2-1}{r}$, $\alpha \in F_{q^2}^*$ be a primitive rth root of unity. Let $r = \frac{q-1}{2}$. Then $r \nmid (q+1)$, $r|q-1$, $ord_{rn}(q^2) = 1$, so the q^2-cyclotomic coset modulo rn contains only one element. Let $u = \frac{n}{2}$. Then $C_u = \{u\},\ C_{u-ri} = \{u - ri\},\ 1 \le i \le \left[\frac{u-1}{r}\right]$.

Theorem 3.2 Let $q \equiv 3(mod 4)$, $q \ne 3$, $n = \frac{q^2-1}{r}$, $r = \frac{q-1}{2}$, $\alpha \in F_{q^2}^*$ be a primitive r-th root of unity. Then there exists an α -constacyclic MDS LCD code with parameters $[n, n-\delta-1, \delta+2]_{q^2},\ 0 \le \delta \le \left[\frac{u-1}{r}\right]$.

Proof Let $\alpha \in F_{q^2}^*$ be a primitive r-th root of unity. Let C be an α-constacyclic code with defining set

$T = \cup_{i=0}^{\delta} C_{u-ri},\ 0 \le \delta \le \left[\frac{u-1}{r}\right]$.

It follows from $r \nmid (q+1)$ that C is a LCD code. Note that $C_u = \{u\}$, $C_{u-ri} = \{u - ri\}$. So, the dimension k of C is $n - \delta - 1$. According to Proposition 2.2, the minimum distance $d \ge \delta + 2$. It follows from Proposition 2.1 that $d = \delta + 2$. Hence C is an MDS LCD code with parameters $[n, n-\delta-1, \delta+2]_{q^2}$.

3.3. MDS LCD Codes for $q = 3^m$ ($m \ge 2$)

In this subsection, let $q = 3^m\ (m \ge 2)$, $n = q^2 + 1$, $\alpha \in F_{q^2}^*$ be a primitive r-th root of unity. Let $r = \frac{3^m-1}{2}$. Then $r \nmid (q+1)$, $r|q-1$, and $ord_m(q^2) = 1\ or\ 2$. So, the q^2-cyclotomic coset modulo rn contains one or two elements. Let $v = \frac{(2r+1)n}{3}$. Then $C_v = \{v\}$, $C_{v-rj} = \{v - rj, v + rj\},\ 1 \le j \le \frac{n-1}{3}$.

Theorem 3.3 Let $q = 3^m\ (m \ge 2)$, $n = q^2 + 1$, $\alpha \in F_{q^2}^*$ be a primitive r-th root of unity. Let $r = \frac{3^m-1}{2}$, $v = \frac{(2r+1)n}{3}$. Then there exists an α-constacyclic MDS LCD code with parameters $[n, n-\delta-1, \delta+2]_{q^2},\ 1 \le \delta \le \frac{n-1}{3}$.

Proof Let $\alpha \in F_{q^2}^*$ be a primitive r-th root of unity. Let C be an α-constacyclic code with defining set

$T = \cup_{j=0}^{\delta} C_{v-rj},\ 0 \le \delta \le \frac{n-1}{3}$.

It follows from $r \nmid (q+1)$ that C is a LCD code. Note that $C_v = \{v\}, C_{v-rj} = \{v - rj, v + rj\}$. So, the dimension k of C is $n - 2\delta - 1$. According to proposition 2.2, the minimum distance $d \ge 2\delta + 2$. It follows from Proposition 2.1 that $d = 2\delta + 2$. Hence C is an MDS LCD code with parameters $[n, n-\delta-1, \delta+2]_{q^2}$.

Example 3.2 Let $m = 2$, $q = 9$, ω be a primitive (q^2-1)-th root of unity. $F_{q^2} = \{0, \omega, \omega^2, \ldots, \omega^{q^2-1}\}$. Assume that $\alpha = \omega^{20}$, α is a primitive 4-th root of unity. Let $r = 4$, C be an α- constacyclic code of length n over F_{q^2} with defining set $T = \cup_{j=0}^{\delta} C_{246-4j}$, $1 \le \delta \le 27$. Then we can get MDS LCD codes with parameters $[n, n-2\delta-1, 2\delta+2],\ 1 \le \delta \le 27$.

In Table 1, some examples of MDS LCD codes from the above three theorems are given.

Table 1. Some α-constacyclic MDS LCD codes

q	r	n	MDS LCD codes	
7	3	16	[16,15- δ, δ+2]	0≤δ≤2
9	4	20	[20,19- δ, δ+2]	0≤δ≤2
15	7	32	[32,31- δ, δ+2]	0≤δ≤2
17	4	72	[72,71- δ, δ+2]	0≤δ≤8
19	9	40	[40,39- δ, δ+2]	0≤δ≤2
21	4	110	[110,109- δ, δ+2]	0≤δ≤13
23	11	48	[48,47- δ, δ+2]	0≤δ≤2
27	13	730	[730,729- 2δ, 2δ+2]	0≤δ≤243
29	4	210	[210,209- δ, δ+2]	0≤δ≤26
33	4	272	[272,271- δ, δ+2]	0≤δ≤33
45	4	506	[506,505- δ, δ+2]	0≤δ≤63
49	4	600	[600,599- δ, δ+2]	0≤δ≤75

4. Constructions of Entanglement-Assisted Quantum MDS Codes

In this section, we will use the MDS LCD codes in section 3 to construct entanglement-assisted quantum MDS codes. Basic concepts and facts about entanglement-assisted quantum error-correcting codes can be referred to [5,9,17-18,20].

Definition 4.1 An EAQEC code, denoted by $[[n,k,d;\ c]]$, encodes k logical qubits into n physical qubits using c copies of maximally entangled Bell states, and d is the minimum distance of the code.

Suppose that $H=(a_{ij})_{k\times n}$ is a $k\times n$ matrix, $\bar{H}$ is defined as $\bar{H}\coloneqq(\bar{a}_{ij})_{k\times n}=(a_{ij}{}^{q})_{k\times n}$, and $H^{\dagger}$ is the transpose matrix of $\bar{H}$.

Lemma 4.1 If $C=[n,k,d]_{q^2}$ is a linear code over F_{q^2} with a parity check matrix H, then there exists an $\left[[n,2k-n+c,d;c]\right]_q$ MDS EAQEC code, where $c=rank(HH^{\dagger})$.

Proposition 4.1 Assume that C is an entanglement-assisted quantum code with parameters $[[n,k,d;c]]_q$. If $d\le(n+2)/2$, then C satisfies the entanglement-assisted Singleton bound $n+c-k\ge 2(d-1)$. If C satisfies the equality $n+c-k=2(d-1)$ for $d\le(n+2)/2$, then it is called an entanglement-assisted quantum MDS code.

Lemma 4.2 If $C=[n,k,d]_{q^2}$ is a linear code over F_{q^2} with parity check matrix H, generator matrix G, then $rank(HH^{\dagger})=n-k-dim\big(Hull_h(C)\big)$, where $Hull_h(C)=C\cap C^{\perp h}$.

Lemma 4.3 Let C is an LCD code over F_{q^2}, then $rank(HH^{\dagger})=n-k$.

Definition 4.2 Let $\left[[n,k,d;c]\right]_q$ be a q-ary EAQEC code. Then the parameters satisfy the Singleton bound for EAQEC codes: $2(d-1)\le n-(k-c)$. An EAQEC code meeting this bound is called an MDS EAQEC code.

Definition 4.3 A q-ary EAQEC code $\left[[n,k,d;c]\right]_q$ with $c=n-k$, is called a maximal entanglement EAQEC code.

Such quantum codes have better properties and efficiency, and can gradually reach the EA-hashing bound [19].

4.1. MDS EAQEC Codes for $q\equiv 1\ (mod\ 4)$

Theorem 4.1 Let $q\equiv 1(mod\ 4)$, $n=\frac{q^2-1}{4}$, $r=4$, $u=\frac{n}{2}$, $\alpha\in F_{q^2}$ be a primitive r-th root of unity. Then there exists a maximal entanglement MDS EAQEC code with parameters $\left[[n,n-\delta-1,\delta+2;\delta+1]\right]_q$, $0\le\delta\le\left[\frac{u-1}{r}\right]$.

Proof According to Theorem 3.1, there exists an α-constacyclic MDS LCD code C with parameters $[n,n-\delta-1,\delta+2]_{q^2}$. Assume the check matrix is H. So, $rank(HH^{\dagger})=n-k=\delta+1$. Then there exists an EAQEC code with parameters $\left[[n,n-\delta-1,\delta+2;\delta+1]\right]_q$, $0\le\delta\le\left[\frac{u-1}{r}\right]$. $n-(k-c)=2(\delta+1)=2(d-1)$ reaches the Singleton bound for EAQEC code, and $c=n-k$.

4.2. MDS EAQEC Codes for $q\equiv 3\ (mod\ 4)$, $q\neq 3$

Theorem 4.2 Let $q\equiv 3(mod\ 4)$, $q\neq 3$, $n=\frac{q^2-1}{r}$, $r=\frac{q-1}{2}$, $u=\frac{n}{2}$, $\alpha\in F_{q^2}$ be a primitive rth root of unity. Then there exists a maximal entanglement MDS EAQEC code with parameters $\left[[n,n-\delta-1,\delta+2;\delta+1]\right]_q$, $0\le\delta\le\left[\frac{u-1}{r}\right]$.

Proof According to Theorem 3.2, there exists an α-constacyclic MDS LCD code C with parameters $[n,n-\delta-1,\delta+2]_{q^2}$. Assume the check matrix is H. Then $rank(HH^{\dagger})=n-k=\delta+1$, there exists an EAQEC code with parameters $\left[[n,n-\delta-1,\delta+2;\delta+1]\right]_q$, $0\le\delta\le\left[\frac{u-1}{r}\right]$. $n-(k-c)=2(2\delta+1)=2(d-1)$ reaches the Singleton bound for EAQEC code, and $c=n-k$.

4.3. MDS EAQEC Codes for $q=3^m$ ($m\ge 2$)

Theorem 4.3 Let $q=3^m(m\ge 2)$, $n=q^2+1$, $r=\frac{3^m-1}{2}$, $v=\frac{(2r+1)n}{3}$, $\alpha\in F_{q^2}^{*}$ be a primitive r-th root of unity. Then there exists a maximal entanglement MDS EAQEC code with parameters $\left[[n,n-2\delta-1,2\delta+2;2\delta+1]\right]_q$ $0\le\delta\le\left[\frac{n-1}{3}\right]$.

Proof According to Theorem 3.3, there exists an α-constacyclic MDS LCD code C with parameters $[n,n-2\delta-1,2\delta+2]_{q^2}$. Assume the check matrix is H. Then $rank(HH^{\dagger})=n-k=2\delta+1$, there exists an EAQEC code with parameters $\left[[n,n-2\delta-1,2\delta+2;2\delta+1]\right]_q$, $0\le\delta\le\left[\frac{n-1}{3}\right]$. $n-(k-c)=2(2\delta+1)=2(d-1)$ reaches the Singleton bound for EAQEC code,

and $c = n - k$.

In Table 2, Some examples of maximal entanglement MDS EAQEC codes from the above theorems are given.

Table 2. Some New maximal entanglement MDS EAQEC codes

q	r	n	MDS EAQEC codes	
7	3	16	[[16,15- δ, δ+2; δ+1]]	0≤δ≤2
9	4	20	[[20,19- δ, δ+2; δ+1]]	0≤δ≤2
11	5	24	[[24,23- δ, δ+2; δ+1]]	0≤δ≤2
17	4	72	[[72,71- δ, δ+2; δ+1]]	0≤δ≤8
19	9	40	[[40,39- δ, δ+2; δ+1]]	0≤δ≤2
25	4	156	[[156,155- δ, δ+2; δ+1]]	0≤δ≤19
27	13	730	[[730,729- 2δ, 2δ+2; 2δ+1]]	0≤δ≤243
29	4	210	[[210,209- δ, δ+2; δ+1]]	0≤δ≤26
37	4	342	[[342,341- δ, δ+2; δ+1]]	0≤δ≤42
41	4	420	[[420,419- δ, δ+2; δ+1]]	0≤δ≤52
49	4	600	[[600,599- δ, δ+2; δ+1]]	0≤δ≤75

5. Conclusions

In this paper, three types of maximal distance separable linear complementary dual codes are constructed as follows:

Table 3. Summary of new MDS LCD codes

q	n	K	d	MDS LCD codes	
$\boldsymbol{q \equiv 1 (mod 4)}$	$n = \frac{q^2-1}{4}$	$n-\delta-1$	$\delta+2$	$[n, n-\delta-1, \delta+2]_{q^2}$	$0 \le \delta \le [\frac{u-1}{r}]$
$\boldsymbol{q \equiv 3 (mod 4)}$ $\boldsymbol{(q \neq 3)}$	$n = \frac{q^2-1}{r}$	$n-\delta-1$	$\delta+2$	$[n, n-\delta-1, \delta+2]_{q^2}$	$0 \le \delta \le [\frac{u-1}{r}]$
$\boldsymbol{q = 3m (m \ge 2)}$	$n = q^2+1$	$n-2\delta-1$	$2\delta+2$	$[n, n-2\delta-1, 2\delta+2]_{q^2}$	$0 \le \delta \le [\frac{n-1}{3}]$

Then we construct some maximal entanglement MDS EAQEC codes by the above LCD codes as follows:

Table 4. Summary of new maximal entanglement MDS EAQEC codes

q	n	d	MDS EAQEC codes	
$\boldsymbol{q \equiv 1 (mod 4)}$	$n = \frac{q^2-1}{4}$	$\delta+2$	$[[n, n-\delta-1, \delta+2; \delta+1]]_q$	$0 \le \delta \le [\frac{u-1}{r}]$
$\boldsymbol{q \equiv 3 (mod 4)}$ $\boldsymbol{(q \neq 3)}$	$n = \frac{q^2-1}{r}$	$\delta+2$	$[[n, n-\delta-1, \delta+2; \delta+1]]_q$	$0 \le \delta \le [\frac{u-1}{r}]$
$\boldsymbol{q = 3m (m \ge 2)}$	$n = q^2+1$	$2\delta+2$	$[[n, n-2\delta-1, 2\delta+2; 2\delta+1]]_q$	$0 \le \delta \le [\frac{n-1}{3}]$

ACKNOWLEDGEMENTS

The research was supported by the general project for the department of Liaoning Education [Grant number: LJKZ0096].

REFERENCES

[1] Massey J.L.: Linear codes with complementary duals. Discret. Math. 106(107), 337–342 (1992).

[2] Sendrier N.: Linear codes with complementary duals meet the Gilbert–Varshamov bound. Discret. Math. 285, 345–347 (2004).

[3] Yang X., Massey J.L.: The necessary and sufficient condition for a cyclic code to have a complementary dual. Discret. Math. 126, 391–393 (1994).

[4] Dinh H.Q.: On repeated-root constacyclic codes of length 4ps. Asian-European J. Math. 6(02), 1350020 (2013).

[5] Qian J, Zhang L. On MDS linear complementary dual codes and entanglement-assisted quantum codes. Designs Codes & Cryptography, 86(7):1565-1572(2018).

[6] Carlet C. and Guilley S.: Complementary dual codes for counter-measures to side- channel attacks. In: Coding Theory and Applications, pp.97-105 (2015).

[7] Esmaeili M., Yari S.: On complementary-dual quasi-cyclic codes. Finite Fields Appl. 15, 375–386 (2009).

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

[9] Brun T.A., Devetak I., Hsieh M.H.: Correcting quantum errors with entanglement. Science 314, 436–439 (2006).

[10] Fujiwara Y., Clark D., Vandendriessche P., Boeck M.D., Tonchev V.D.: Entanglement-assisted quantum low-density parity-check codes. Phys. Rev. A 82, 042338 (2010).

[11] Hsieh M.H., Devetak I., Brun T.A.: General entanglement-assisted quantum error-correcting codes. Phys. Rev. A 76, 062313 (2007).

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

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

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

[15] Giuliano G. La Guardia, Marcelo M.S. Alves, On cyclotomic cosets and code constructions, Linear Algebra and its Applications, Volume 488, Pages 302-319, (2016).

[16] Wong, Denis. Cyclotomic cosets, codes and secret sharing. Malaysian Journal of Mathematical Sciences. 11. 59-73. (2017).

[17] Guenda, K., Jitman, S. Gulliver, T.A. Constructions of good entanglement assisted quantum error correcting codes. Des. Codes Cryptogr. 86, 121–136 (2018).

[18] Wilde, Mark M. et al. Convolutional entanglement distillation. 2010 IEEE International Symposium on Information Theory: 2657-2661 (2007).

[19] Bowen, Garry. Entanglement required in achieving entanglement-assisted channel capacities. Physical Review A, 66 (2002): 052313.

[20] Grassl, M.: Entanglement-assisted quantum communication beating the quantum singleton bound. AQIS, Taiwan (2016).