Article

Entanglement-Assisted Quantum Codes from Cyclic Codes

Francisco Revson F. Pereira and Stefano Mancini

Special Issue
Advances in Quantum Computing

Edited by
Dr. Brian R. La Cour and Dr. Giuliano Benenti

Article

Entanglement-Assisted Quantum Codes from Cyclic Codes

Francisco Revson F. Pereira [1],*[ID] and **Stefano Mancini** [2,3][ID]

1   IQM Quantum Computers, Nymphenburger Str. 86, 80636 Munich, Germany
2   School of Science and Technology, University of Camerino, I-62032 Camerino, Italy
3   Istituto Nazionale di Fisica Nucleare, Sezione di Perugia, I-06123 Perugia, Italy
*   Correspondence: revson.ee@gmail.com

Abstract: Entanglement-assisted quantum-error-correcting (EAQEC) codes are quantum codes which use entanglement as a resource. These codes can provide better error correction than the (entanglement unassisted) codes derived from the traditional stabilizer formalism. In this paper, we provide a general method to construct EAQEC codes from cyclic codes. Afterwards, the method is applied to Reed–Solomon codes, BCH codes, and general cyclic codes. We use the Euclidean and Hermitian construction of EAQEC codes. Three families have been created: two families of EAQEC codes are maximal distance separable (MDS), and one is almost MDS or almost near MDS. The comparison of the codes in this paper is mostly based on the quantum Singleton bound.

Keywords: quantum codes; Reed–Solomon codes; BCH codes; maximal distance separable; maximal entanglement

1. Introduction

Practical implementations of most quantum communication schemes and quantum computers will only be possible if such systems incorporate quantum-error-correcting codes. Quantum error correcting codes restore quantum states from corrupted by unwanted noisy action. One of the most known and used methods to create quantum codes from classical block codes is the CSS method [1]. Unfortunately, it requires (Euclidean or Hermitian) duality containing to one of the classical codes used. One way to overcome this constraint is via entanglement shared beforehand by the communicating parties. It is possible to show that such entanglement-assisted construction also improves the error-correction capability of quantum codes. These codes are called entanglement-assisted quantum error-correcting (EAQEC) codes. The first proposals of EAQEC codes were presented by Bowen [2] and Fattal et al. [3]. Then, Brun et al. [4] have developed an entanglement-assisted stabilizer formalism for these codes, which was recently generalized by Galindo et al. [5].

This formalism has created a method to construct EAQEC codes from classical block codes, which has lead to the construction of several families of EAQEC codes [6–13]. The majority of them utilize constacyclic codes [7,9,10,14] or negacyclic codes [8,9] as the classical counterpart. However, only a few of them have used cyclic codes and described the parameters of the quantum code constructed via the defining set of cyclic code. This can lead to a straightforward relation between the parameters of the classical and quantum codes and a method to create MDS EAQEC code. Li et al. used BCH codes to construct EAQEC codes via decomposing the defining set of the BCH code used [15]. Lu and Li constructed EAQEC codes from primitive quaternary BCH codes [16]. Recently, Lu et al. [9], using not cyclic but constacyclic MDS codes as the classical counterpart, proposed four families of MDS EAQEC codes.

Deriving EAQEC codes with different parameters provides a tool for reliable communication through quantum channels. In the quantum communication framework, sender and receiver are physically separated, which makes impossible the use joint unitary transformations. However, one can use other resources in order to maximize the code rate within

the constraint of high minimum distance, such as pre-shared entanglement. Although in a specified communication scenario one may aim at deriving a high rate code with a low error probability for the block code, due to the broad approach followed in this paper (where we do not design codes for a particular type of quantum channel), we shall use the minimum distance as performance measure for EAQEC codes.

The main goal of this paper is to describe any cyclic code, such as Reed–Solomon and BCH codes, under the same framework via defining set description, and to show, using two classical codes from one of these families, how to construct EAQEC codes from them. We use Euclidean and Hermitian methods to construct EAQEC codes. As it will be shown, EAQEC codes from Reed–Solomon codes are MDS codes, and the ones from BCH codes are new in two senses. The first one is that there is no work in the literature with the same parameters. The second one is that we usie two BCH codes to derive the EAQEC code, which gives more freedom in the choice of parameters. Two more families of EAQEC codes are devised using the Hermitian construction. One of these families can generate codes which are almost MDS or almost near MDS; i.e., the Singleton defect for these codes is equal to one or two units. The last family created is maximally entangled and has a length proportional to a high power of the cardinality of the field. This family, when extending the block length, could approach the EA quantum hashing bound similarly to what happens to turbo codes in reference [17]. In fact, it was shown by Lai et al. [18] that maximal-entanglement EAQEC turbo codes get close to the EA quantum hashing bound. (By the EA quantum hashing bound is intended the quantum communication rate given by $1 - \frac{1}{2}[p(\log_2 3 - \log_2 p) - (1-p)\log_2(1-p)]$ for a depolarizing channel characterized by depolarizing parameter p [17].) Lastly, we would like to highlight that the description given in this paper gives a more direct relation between cyclic codes and the entanglement-assisted quantum codes constructed from them. Such a relation can be extended to constacyclic and negacyclic codes with a few adjustments.

The paper is organized as follows. In Section 2, we review Reed–Solomon and BCH codes and describe their parameters via a defining set. Additionally, we show construction methods of EAQEC codes from classical codes. Using these methods for cyclic classical codes, new EAQEC codes are constructed in Section 3. In Section 4, a comparison of these codes is presented via the quantum Singleton bound. In particular, we show families of MDS and almost MDS EAQEC codes. We also create a family of EAQEC codes which could approach the EA quantum hashing bound [17–19]. Lastly, the conclusion is presented in Section 5.

Notation

Throughout this paper, p denotes a prime number and $q \neq 2$ is a power of p. Let $\mathbb{F}_q$ be the finite field with q elements. A linear code C with parameters $[n,k,d]_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum distance d. For cyclic codes, $Z(C)$ denotes the defining set, and $g(x)$ is the generator polynomial. Lastly, an $[[n,k,d;c]]_q$ quantum code is a q^k-dimensional subspace of $\mathbb{C}^{q^n}$ with minimum distance d that utilizes c pre-shared entangled pairs.

2. Preliminaries

In this section, we review some ideas related to linear complementary dual (LCD) codes, cyclic codes, and entanglement-assisted quantum codes. Before giving a description of LCD codes, we need to define the Euclidean and Hermitian dual of a linear code.

Definition 1. *Let C be a linear code over $\mathbb{F}_q$ with length n. The (Euclidean) dual of C is defined as*

$$C^{\perp} = \{ \mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x} \cdot \mathbf{c} = 0 \text{ for all } \mathbf{c} \in C \}. \tag{1}$$

If the finite field has cardinality equal to q^2, an even power of a prime, then we can define the Hermitian dual of C. This dual code is defined by

$$C^{\perp_h} = \{ \mathbf{x} \in \mathbb{F}_{q^2}^n \mid \mathbf{x} \cdot \mathbf{c}^q = 0 \text{ for all } \mathbf{c} \in C \}, \tag{2}$$

where $\mathbf{c}^q = (c_1^q, \ldots, c_n^q)$ for $\mathbf{c} \in \mathbb{F}_{q^2}^n$.

These types of dual codes can be used to derive quantum codes from the stabilizer formalism [1]. The requirement in this formalism is to the classical code to be self-dual; i.e., $C \subseteq C^{\perp}$ or $C \subseteq C^{\perp_H}$. However, there is a different relationship between a code and its (Euclidean or Hermitian) dual that can be interesting for constructing an EAQEC. This relation is complementary duality and is defined in the following.

Definition 2. *The hull of a linear code C is given by $hull(C) = C^{\perp} \cap C$. The code is called linear complementary dual (LCD) code if the hull is trivial; i.e, $hull(C) = \{\mathbf{0}\}$. Similarly, it is defined by $hull_H(C) = C^{\perp_h} \cap C$ and the idea of a Hermitian LCD code.*

Now, we can define cyclic codes and some properties that can be used to extract the parameters of the quantum code constructed from them.

2.1. Cyclic Codes

A linear code C with parameters $[n, k, d]_q$ is called cyclic if for any codeword $(c_0, c_1, \ldots, c_{n-1}) \in C$ implies $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. By defining a map from $\mathbb{F}_q^n$ to $\mathbb{F}_q[x]/(x^n - 1)$, which takes $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ to $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_q[x]/(x^n - 1)$, we can see that a linear code C is cyclic if and only if it corresponds to an ideal of the ring $\mathbb{F}_q[x]/(x^n - 1)$. Since any ideal in $\mathbb{F}_q[x]/(x^n - 1)$ is principal, any cyclic code C is generated by a polynomial $g(x)|(x^n - 1)$, which is called a generator polynomial. This polynomial is monic, and has the smallest degree among all the generators of C.

A characterization of the parameters of a cyclic code can be given from the generator polynomial and its defining set. For the description of this set, consider the following: Let $m = ord_n(q)$, α be a generator of the multiplicative group $\mathbb{F}_{q^m}^*$, and assume $\beta = \alpha^{\frac{q^m-1}{n}}$; i.e., β is a primitive n-th root of unity. Then, the defining set of C, which is denoted by $Z(C)$, is defined as $Z(C) = \{i \in \mathbb{Z}_n : c(\beta^i) = 0 \text{ for all } c(x) \in C\}$.

BCH and Reed–Solomon codes are particular cases of cyclic codes, where the generator polynomial has some additional properties. See Definitions 3 and 5.

Definition 3. *Let $b \geq 0$, $\delta \geq 1$, and $\alpha \in \mathbb{F}_{q^m}$, where $m = ord_n(q)$. A cyclic code C of length n over $\mathbb{F}_q$ is a BCH code with designed distance δ if*

$$g(x) = lcm\{m_b(x), m_{b+1}(x), \ldots, m_{b+\delta-2}(x)\}$$

where $m_i(x)$ is the minimal polynomial of α^i over $\mathbb{F}_q$. If $n = q^m - 1$, then the BCH code is called primitive, and if $b = 1$, it is called narrow-sense.

Before relating the parameters of an BCH code with the defining set, we need to introduce the idea of the cyclotomic coset. It comes from the observation that the minimal polynomial $m_i(x)$ of α^i can be the minimal polynomial of other powers of α. The reason for this is that α belongs to an extension of $\mathbb{F}_q$ while the polynomial $m_i(x) \in \mathbb{F}_q[x]$. The set of all zeros of $m_i(x)$ in the field $\mathbb{F}_{q^m}$ is given by the cyclotomic coset of i. Thus, the defining set of a BCH code C is the union of the cyclotomic cosets of $b, b+1, \ldots, b+\delta-2$. The following definition describes this set.

Definition 4. *The q-ary cyclotomic coset   mod n containing an element i is defined by*

$$\mathbb{C}_i = \{i, iq, iq^2, iq^3, \ldots, iq^{m_i-1}\}, \tag{3}$$

where m_i is the smallest positive integer such that $iq^{m_i} \equiv i \mod n$.

For the parameters of a BCH code, it is shown that the dimension is equal to $n - |Z(C)|$ and the minimal distance of C is at least δ [20]. Thus, we can see that important properties of an BCH codes can be obtained from the defining set. The same characterization happens with Euclidean or Hermitian dual cyclic code. Propositions 1 and 2 focus on this.

Proposition 1 ([20], Proposition 4.3.8). *Let C be a linear code of length n and defining set $Z(C)$. Then, the defining set of $C^\perp$ is given by*

$$Z(C^\perp) = \mathbb{Z}_n \setminus \{-i | i \in Z(C)\}$$

For BCH codes, the generator polynomial is given by the lcm of the minimal polynomials over $\mathbb{F}_q$ of the elements α^j such that $j \in Z(C^\perp)$.

Proposition 2. *Let C be a cyclic code over $\mathbb{F}_{q^2}$ with defining set $Z(C)$. Then,*

$$Z(C^{\perp_h}) = \mathbb{Z}_n \setminus \{-i | i \in qZ(C)\}.$$

Proof. Let $\mathbf{c} \in \mathbb{F}_{q^2}^n$ be a codeword of C. By expressing $\mathbf{c}^q$ as a polynomial, we have that $c^{(q)}(x) = c_0^q + c_1^q x + \cdots + c_{n-1}^q x^{n-1}$. Thus, $i \in \mathbb{Z}_n$ belongs to $Z(C^q)$ if and only if

$$\begin{aligned}
c^{(q)}(\alpha^i) = 0 &\iff c_0^q + c_1^q \alpha^i + \cdots + c_{n-1}^q \alpha^{i(n-1)} = 0 \\
&\iff (c_0^q + c_1^q \alpha^i + \cdots + c_{n-1}^q \alpha^{i(n-1)})^q = 0 \\
&\iff c_0 + c_1 \alpha^{iq} + \cdots + c_{n-1} \alpha^{iq(n-1)} = 0 \\
&\iff iq \in Z(C).
\end{aligned}$$

This shows that $Z(C^q) = qZ(C)$. Since $C^{\perp_h} = (C^q)^\perp$, we have from Proposition 1 that $Z(C^{\perp_h}) = \mathbb{Z}_n \setminus \{-i | i \in qZ(C)\}$. □

The other class of cyclic codes used in this paper, Reed–Solomon codes, can be viewed as a subclass of BCH codes. Thus, a similar characterization in terms of defining set can be given; see Definition 5 and Corollary 1. One property of such codes that makes them important is that they are maximal distance separable (MDS) codes; i.e., fixing the length and the dimension, they have the maximal minimal distance possible. As shown in Section 3, using such codes to construct EAQEC codes will result in MDS quantum codes.

Definition 5. *Let $b \geq 0$, $n = q - 1$, and $1 \leq k \leq n$. A cyclic code $RS_k(n, b)$ of length n over $\mathbb{F}_q$ is a Reed–Solomon code with minimal distance $n - k + 1$ if*

$$g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \cdots (x - \alpha^{b+n-k-1}),$$

where α is a primitive element of $\mathbb{F}_q$.

A particular application of Proposition 1 to Reed–Solomon codes is described in Corollary 1, where the parameters and defining set of an Euclidean dual of a Reed–Solomon are derived.

Corollary 1. *Let $RS_k(n, b)$ be a Reed–Solomon code. Then, its Euclidean dual can be described as*

$$RS_k(n, b)^\perp = RS_{n-k}(n, n - b + 1)$$

In particular, the defining set of $RS_k(n,b)^\perp$ is given by $Z(RS_k(n,b)^\perp) = \{n-b+1, n-b+2, \ldots, n-b+k\}$.

As will be shown in the next subsection, the amount of entanglement in a EAQEC code is computed from the dimension of the intersection between the two codes. Thus, the last proposition of this subsection addresses the subject.

Proposition 3 ([21], Exercise 239, Chapter 4). *Let C_1 and C_2 be cyclic codes with defining sets $Z(C_1)$ and $Z(C_2)$, respectively. Then, the defining set of $C_1 \cap C_2$ is given by $Z(C_1) \cup Z(C_2)$. In particular, $\dim(C_1 \cap C_2) = n - |Z(C_1) \cup Z(C_2)|$.*

2.2. Entanglement-Assisted Quantum Codes

Definition 6. *A quantum code $\mathcal{Q}$ is called an $[[n,k,d;c]]_q$ entanglement-assisted quantum error-correcting (EAQEC) code if it encodes k logical qudits into n physical qudits using c copies of maximally entangled states and can correct $\lfloor (d-1)/2 \rfloor$ quantum errors. A EAQEC code is said to have maximal entanglement when $c = n - k$.*

Formulating a stabilizer paradigm for EAQEC codes gives a way to use classical codes to construct this quantum codes [22]. In particular, we have the next two procedures by Galindo et al. [5].

Proposition 4 ([5], Theorem 4). *Let C_1 and C_2 be two linear codes over $\mathbb{F}_q$ with parameters $[n,k_1,d_1]_q$ and $[n,k_2,d_2]_q$; and parity check matrices H_1 and H_2, respectively. Then, there is a EAQEC code with parameters $[[n, k_1 + k_2 - n + c, d; c]]_q$, where $d = \min\{d_H(C_1 \setminus (C_1 \cap C_2^\perp)), d_H(C_2 \setminus (C_1^\perp \cap C_2))\}$, with d_H as the minimum Hamming weight of the vectors in the set, and*

$$c = \operatorname{rank}(H_1 H_2^T) = \dim C_1^\perp - \dim(C_1^\perp \cap C_2) \tag{4}$$

is the number of required maximally entangled states.

Proposition 5 ([5], Proposition 3 and Corollary 1). *Let C be a linear codes over $\mathbb{F}_{q^2}$ with parameters $[n,k,d]_q$, H be a parity check matrix for C, and H^* be the q-th power of the transpose matrix of H. Then, there is a EAQEC code with parameters $[[n, 2k - n + c, d'; c]]_q$, where $d' = d_H(C \setminus (C \cap C^{\perp_h}))$, with d_H as the minimum Hamming weight of the vectors in the set, and*

$$c = \operatorname{rank}(HH^*) = \dim C^{\perp_h} - \dim(C^{\perp_h} \cap C) \tag{5}$$

is the number of required maximally entangled states.

A measurement of goodness for a EAQEC code is the quantum Singleton bound (QSB). Let $[[n,k,d;c]]_q$ be a EAQEC code. Then, the QSB is given by

$$d \leq \left\lfloor \frac{n-k+c}{2} \right\rfloor + 1. \tag{6}$$

The difference between the QSB and d is called a quantum Singleton defect. When the quantum Singleton defect is equal to zero (resp. one), the code is called the maximum distance separable quantum code (resp. almost maximum distance separable quantum code), and it is denoted the MDS quantum code (resp. almost MDS quantum code).

3. New Entanglement-Assisted Quantum-Error-Correcting Cyclic Codes

In this section is shown the construction of EAQEC codes from the cyclic codes. We are going to make use of Euclidean and Hermitian constructions, which will give codes with different parameters when compared over the same field.

3.1. Euclidean Construction

A straightforward application of cyclic codes to the Proposition 4 via defining set description can produce some interesting results. See Theorem 1 and Corollary 2.

Theorem 1. *Let C_1 and C_2 be two cyclic codes with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$, respectively. Then, there is an EAQEC code with parameters $[[n, k_1 - |Z(C_1^\perp) \cap Z(C_2)|, \min\{d_1, d_2\}; n - k_2 - |Z(C_1^\perp) \cap Z(C_2)|]]_q$.*

Proof. From Proposition 3, we have that $\dim(C_1^\perp \cap C_2) = n - |Z(C_1^\perp) \cup Z(C_2)| = n - |Z(C_2)| - |Z(C_1^\perp)| + |Z(C_1^\perp) \cap Z(C_2)| = k_2 - k_1 + |Z(C_1^\perp) \cap Z(C_2)|$. Thus, the amount of entanglement used in an EAQEC code constructed from these two cyclic codes can be computed from Proposition 4, which is $c = n - k_2 - |Z(C_1^\perp) \cap Z(C_2)|$. By substituting this value of c in the parameters of the EAQEC code in Proposition 4, we obtain an $[[n, k_1 - |Z(C_1^\perp) \cap Z(C_2)|, \min\{d_1, d_2\}; n - k_2 - |Z(C_1^\perp) \cap Z(C_2)|]]_q$ EAQEC code.　$\square$

Corollary 2. *Let C be a LCD cyclic code with parameters $[n, k, d]_q$. Then, there is a maximal entanglement EAQEC code with parameters $[[n, k, d; n - k]]_q$. In particular, if C is MDS, so is the EAQEC code derived from it.*

Proof. Let $C_1 = C_2 = C$ in Theorem 1. Since C is LCD, $|Z(C_1^\perp) \cap Z(C_2)| = 0$. From Theorem 1, we have that there is an EAQEC code with parameters $[[n, k, d; n - k]]_q$.　$\square$

Theorem 2. *Let $C_1 = RS_{k_1}(n, b_1)$ and $C_2 = RS_{k_2}(n, b_2)$ be two Reed–Solomon codes over $\mathbb{F}_q$ with $0 \le b_1 \le k_1$, $b_2 \ge 0$, and $b_1 + b_2 \le k_2 + 1$. Then, we have two possible cases:*

1. *For $k_1 - b_1 \ge b_2$, there is an EAQEC code with parameters*

$$[[n, b_1 + b_2 - 1, n - \min\{k_1, k_2\} + 1; n + b_1 + b_2 - k_1 - k_2 - 1]]_q;$$

2. *For $k_1 - b_1 < b_2$, there is an EAQEC code with parameters*

$$[[n, k_1, n - \min\{k_1, k_2\} + 1; n - k_2]]_q.$$

Proof. From Corollary 1, we have that $Z(C_1^\perp) = \{n - b_1 + 1, n - b_1 + 2, \ldots, n - b_1 + k_1\}$. First of all, notice that the restriction $b_1 + b_2 \le k_2 + 1$ implies that the first element in the defining set of $Z(C_1^\perp)$ comes after the last element in $Z(C_2)$. Since $0 \le b_1 \le k_1$, we have that $n - b_1 + k_1 \ge n$, which implies that the defining set for $C_1^\perp$ equals to $Z(C_1^\perp) = \{n - b_1 + 1, n - b + 2, \ldots, n - 1, 0, 1, \ldots, k_1 - b_1\}$. Thus, $Z(C_1^\perp)$ intersects $Z(C_2)$ if and only if $k_1 - b_1 \ge b_2$. In the case that it does, the intersection is equals to $Z(C_1^\perp) \cap Z(C_2) = k_1 - (b_1 + b_2) + 1$. The missing claims are obtained using these results in Theorem 1.　$\square$

Corollary 3. *Let $C = RS_k(n, b)$ be a Reed–Solomon code over $\mathbb{F}_q$ with $0 < b \le (k+1)/2$ and $0 < k < n \le q$. Then, there is an MDS EAQEC code with parameters $[[n, 2b - 1, n - k + 1; n + 2b - 2k - 1]]_q$. In particular, for $b = (k+1)/2$, there is a maximal entanglement MDS EAQEC code.*

Proof. Let $C_1 = C_2 = RS_k(n, b)$ in Theorem 2. Assuming $0 \le b < (k+1)/2$, we have that the classical codes fall in the first case of Theorem 2; and for $b = (k+1)/2$, we are in the second case of Theorem 2. Thus, substituting the values of k_1, k_2 and b_1, b_2 by k and b, respectively; the result follows.　$\square$

In a similar way, we can use BCH codes to construct EAQEC codes. The advantage in using BCH codes is that the length of the code is not bounded by the cardinality of the finite field used. However, creating classical or quantum codes from BCH codes which are MDS is a difficult task. Our proposal to have BCH codes as the classical counterpart in

this paper is to show how to use two BCH codes to construct EAQEC codes. In addition, it is also constructed maximal entanglement EAQEC codes. In order to do this, we show suitable properties concerning some cyclotomic cosets for $n = q^2 - 1$.

Lemma 1. *Let $n = q^2 - 1$ with $q > 2$. Then, the q-ary coset $\mathbb{C}_0$ has one element, and $\mathbb{C}_i = \{i, iq\}$ for any $1 \leq i \leq q - 1$.*

Proof. The first claim is trivial. For the second one, notice $iq^2 \equiv i \mod (q^2 - 1)$. Thus, the only elements in $\mathbb{C}_i$ are i and iq, for $1 \leq i \leq q - 1$. $\square$

From Lemma 1, we can construct EAQEC codes with length $n = q^2 - 1$. See Theorem 3.

Theorem 3. *Let $n = q^2 - 1$ with $q > 2$. Assume a, b are integers such that $0 \leq a \leq q - 1$ and $1 \leq b \leq q$. Then, there is an EAQEC code with parameters*

- $[[n, 2(q - b) - 1, b + 1; 2(q - a - 1)]]_q$, *if $a \geq q - b$ and $b < q$;*
- $[[n, 2a + 1, b + 1; 2b - \lfloor \frac{b}{q} \rfloor]]_q$, *if $a < q - b$.*

Proof. First of all, assume that $C_1^\perp$ has a defining set given by $Z(C_1^\perp) = \cup_{i=0}^a \mathbb{C}_i$, and the defining set of C_2 is equal to $Z(C_2) = \cup_{i=1}^b \mathbb{C}_{q-i}$. From Lemma 1, we have that $|Z(C_1^\perp)| = 2a + 1$ and $|Z(C_2)| = 2b - \lfloor \frac{b}{q} \rfloor$. Thus, the dimensions of C_1 and C_2 are equal to $k_1 = |Z(C_1^\perp)| = 2a + 1$ and $k_2 = n - |Z(C_2)| = n - 2b + \lfloor \frac{b}{q} \rfloor$, respectively. To compute $|Z(C_1^\perp) \cap Z(C_2)|$, we have to consider two cases. If $a \geq q - b$, then we have that $Z(C_1^\perp) \cap Z(C_2) = \cup_{i=q-b}^a \mathbb{C}_i$, which has cardinality given by $|Z(C_1^\perp) \cap Z(C_2)| = 2(a - (q - b) + 1) - \lfloor \frac{b}{q} \rfloor$, because $|\mathbb{C}_0| = 1$. On the other hand, if $a < q - b$, then $|Z(C_1^\perp) \cap Z(C_2)| = 0$. Lastly, since $a, b \leq q$, $Z(C_1^\perp) = \cup_{i=0}^a \mathbb{C}_i$, and $n = q^2 - 1$ with $q > 2$, we can see that $d_1 > d_2 = b + 1$. Now, using these results in Theorem 1, we have that there is a EAQEC code with parameters $[[n, 2(q - b) - 1 + \lfloor \frac{b}{q} \rfloor, b + 1; 2(q - a - 1)]]_q$, if $a \geq q - b$, or a EAQEC code with parameters $[[n, 2a + 1, b + 1; 2b - \lfloor \frac{b}{q} \rfloor]]_q$. $\square$

3.2. Hermitian Construction

In the same way as before, it possible to use cyclic codes to construct EAQEC codes from the Hermitian construction method of Proposition 5. See the following theorem.

Theorem 4. *Let C be a cyclic code with parameters $[n, k, d]_{q^2}$. Then there is an EAQEC code with parameters $[[n, k - |Z(C^{\perp_h}) \cap Z(C)|, d; n - k - |Z(C^{\perp_h}) \cap Z(C)|]]_q$.*

Proof. First of all, from Proposition 3 we have $\dim(C^\perp \cap C) = n - |Z(C^\perp) \cup Z(C)| = n - |Z(C)| - |Z(C^{\perp_h})| + |Z(C^{\perp_h}) \cap Z(C)| = k - k + |Z(C^{\perp_h}) \cap Z(C)| = |Z(C^{\perp_h}) \cap Z(C)|$. Thus, $c = \dim(C^{\perp_h}) - \dim(C^\perp \cap C) = n - k - |Z(C^{\perp_h}) \cap Z(C)|$. Using a $[n, k, d]_{q^2}$ to construct a EAQEC codes via Proposition 5, we derive a code with parameters $[[n, k - |Z(C^{\perp_h}) \cap Z(C)|, d; n - k - |Z(C^{\perp_h}) \cap Z(C)|]]_q$. $\square$

Corollary 4. *Let C be an LCD cyclic code with parameters $[n, k, d]_{q^2}$. Then there is a maximal entanglement EAQEC code with parameters $[[n, k, d; n - k]]_q$.*

Proof. From the proof of Theorem 4, we have that $\dim(C^{\perp_h} \cap C) = |Z(C^{\perp_h}) \cap Z(C)|$. Since C is LCD, $|Z(C^{\perp_h}) \cap Z(C)| = 0$, and the result follows from Theorem 4. $\square$

Differently from the construction of EAQEC code via Euclidean dual cyclic code, the construction via Hermitian dual can be more delicate, even for Reed–Solomon codes. Even so, we are going to show that is possible to construct EAQEC codes from a particular case of Reed–Solomon codes and some cyclic codes.

Theorem 5. *Let q be a prime power and assume $C = RS_k(n, 1)$ is a Reed–Solomon code over $\mathbb{F}_{q^2}$ with $k = qt + r < q^2$, where $t \geq 1$ and $0 \leq r \leq q - 1$, and $n = q^2$. Then we have the following:*

- *If $t \geq q - r - 1$, then there exists an MDS EAQEC code with parameters*

$$[[q^2, (t+1)^2 - 2(q - r) + 1, q(q - t) - r + 1; (q - t - 1)^2 + 1]]_q.$$

- *If $t < q - r - 1$, then there exists an MDS EAQEC code with parameters*

$$[[q^2, t^2 - 1, q(q - t) - r + 1; (q - t)^2 - 2r - 1)]]_q.$$

Proof. Since $C = RS_k(n, 0)$, we have that $Z(C) = \{0, 1, 2, \ldots, n - k - 1\}$. From the proof of Theorem 2, we also have that $Z(C^{\perp_h}) = qZ(C^\perp) = \{q, 2q, \ldots, kq\}$. From $n = q^2$ and $k = qt + r$, we can rewrite these two defining sets as $Z(C) = \{qi + j | 0 \leq i \leq q - t - 2, 0 \leq j \leq q - 1\} \cup \{(q - t - 1)q + j | 0 \leq j \leq q - r - 2\}$ and $Z(C^{\perp_h}) = \{qi + j | 0 \leq i \leq q - 1, 0 \leq j \leq t - 1\} \cup \{qi + t | 0 \leq i \leq r\}$. Using this description, we can compute $|Z(C) \cap Z(C^{\perp_h})|$. To do so, we have to consider two cases separately, $t \geq q - r - 1$ and $t < q - r - 1$. For the first case, the intersection is given by the following set $Z(C) \cap Z(C^{\perp_h}) = \{qi + j | 0 \leq i \leq q - t - 2, 0 \leq j \leq t\} \cup \{(q - t - 1)q + j | 0 \leq j \leq q - r - 2\}$. Thus, $|Z(C) \cap Z(C^{\perp_h})| = (q - t - 1)(t + 1) + q - r - 1$. Similarly for the case $t < q - r - 1$, we have $Z(C) \cap Z(C^{\perp_h}) = \{qi + j | 0 \leq i \leq q - t - 1, 0 \leq j \leq t - 1\} \cup \{qi + t | 0 \leq i \leq r\}$, which implies $|Z(C) \cap Z(C^{\perp_h})| = (q - t)t + r + 1$. Using these results and the fact that C has parameters $[q^2, k, q^2 - k + 1]_{q^2}$, in Theorem 4, we have that there exists a EAQEC code with parameters

- $[[q^2, (t+1)^2 - 2(q - r) + 1, q(q - t) - r + 1; (q - t - 1)^2 + 1]]_q$, for $t \geq q - r - 1$; and
- $[[q^2, t^2 - 1, q(q - t) - r + 1; (q - t)^2 - 2r - 1)]]_q$, for $t < q - r - 1$.

□

Theorem 6. *Let $n = q^4 - 1$ and $q \geq 3$, a prime power. There exists an EAQEC code with parameters $[[n, n - 4(a - 1) - 3, d \geq a + 1; 1]]_q$, where $2 \leq a \leq q^2 - 1$.*

Proof. Let C_a be a cyclic code with defining set $Z(C_a) = \mathbb{C}_0 \cup \mathbb{C}_{q^2+1} \cup (\cup_{i=2}^a \mathbb{C}_{q^2+a})$, for $2 \leq a \leq q^2 - 1$. From Ref. [23], we have that $\mathbb{C}_{q^2+1} = \{q^2 + 1\}$ and $\mathbb{C}_{q^2+a} = \{q^2 + a, 1 + aq^2\}$. It is trivial to show that $\mathbb{C}_0 = \{0\}$. From $-qZ(C_a) \cap Z(C_a) = \mathbb{C}_0$ [23], we can see that $Z(C_a^{\perp_h}) \cap Z(C_a) = Z(C_a) \setminus \mathbb{C}_0$. Hence, $|Z(C_a^{\perp_h}) \cap Z(C_a)| = 2(a - 1) + 1$. From the assumption of the defining set, the dimension and minimal distance of the classical code are $k = n - 2(a - 1) - 2$ and $d \geq a + 1$, respectively. Thus, using these quantities in Theorem 4, we have that there exists an EAQEC code with parameters $[[n, n - 4(a - 1) - 3, d \geq a + 1; 1]]_q$. □

Two important comments can be made about Theorem 6. Comparing the bound given for the minimal distance and the Singleton bound for EAQEC codes, we see that the difference between these two values is equal to $a - 1$. Thus, for lower values of a (such as $a = 2$ or $a = 3$), the EAQEC codes have a minimal distance, close to the optimum; e.g., if $a = 2$ (or $a = 3$), the family of EAQEC codes is almost MDS (or almost MDS). The second point is that the codes in Theorem 6 can be seen as a generalization of the result by Qian and Zhang [24].

In the following, we use LCD cyclic code to construct maximal entanglement EAQEC codes. The families obtained have an interesting range of possible parameters.

Theorem 7. *Let q be a prime power, $m \geq 2$, $2 \leq \delta \leq q^{2\lceil \frac{m}{2} \rceil} + 1$, and $\kappa = q^{2m} - 2 - 2(\delta - 1 - \lfloor \frac{\delta - 1}{q^2} \rfloor)m$. Then,*

1. *For m odd and $1 \leq u \leq q - 1$, there is a maximal entanglement EAQEC code with parameters $[[q^{2m} - 1, k, d \geq \delta + 1 + \lfloor \frac{\delta-1}{q} \rfloor; q^{2m} - 1 - k]]_q$, where*

$$k = \begin{cases} \kappa, & \text{if } 2 \leq \delta \leq q^m - 1; \\ \kappa + u^2 m, & \text{if } uq^m \leq \delta \leq (u+1)(q^m - 1); \\ \kappa + (u^2 + 2v + 1)m, & \text{if } \delta = (u+1)(q^m - 1) + v + 1 \text{ for } 0 \leq v \leq u - 1; \\ \kappa + q^2 m, & \text{if } \delta = q^{m+1} \text{ or } q^{m+1} + 1. \end{cases} \quad (7)$$

2. *For m even, there is an maximal entanglement EAQEC code with parameters*

$$[[q^{2m} - 1, \kappa, d \geq \delta + 1 + \lfloor \frac{\delta-1}{q} \rfloor; 2(\delta - 1 - \lfloor \frac{\delta-1}{q^2} \rfloor)m + 1]]_q. \quad (8)$$

Proof. From Li [25], we have that there are LCD cyclic codes with parameters $[q^{2m} - 1, k, \delta + 1 + \lfloor \frac{\delta-1}{q} \rfloor]]_{q^2}$, where k is the same as in Equations (7) and (8) for odd and even m, respectively. Thus, by applying this LCD code to Corollary 4, we obtain the mentioned codes. □

4. Code Examples

In Table 1, we present some MDS EAQEC codes obtained from Corollary 3 and Theorem 5. The codes in the first column are obtained from the Euclidean construction and the ones in the second column from the Hermitian construction. As can be seen, the latter one has a higher length within the same field. Thus, it can be used in applications where the underline quantum system has limited dimensions. On the other hand, the codes in the first column can have parameters that the ones from the Hermitian construction cannot. Thus, these two classes of EAQEC codes are suitable for specific applications.

The codes obtained from Corollary 3 and Theorem 5 are maximal entanglement EAQEC codes. We could use the dependency between the cardinality of the finite field and code parameters to derive new codes. In particular, this is not the case for the codes in Ref. [26], where the cardinality of the finite field must be two. Additionally, one cannot find in Ref. [9] codes similar to the ones on the left column of Table 1, since the codes in Ref. [9] request a number c of entangled pairs that can be only equal to one or two. For our codes with $c = 1$ or 4, which can be used in a comparison with the codes in Ref. [9], we see that the codes $[[4, 3, 2; 1]]_4$ and $[[13, 9, 5; 4]]_{13}$ have parameters slightly worse than the codes $[[5, 4, 2; 1]]_7$ and $[[10, 9, 5; 4]]_3$, respectively. Lastly, if we do not take into consideration the cardinality of the field, we continue to see improvements in the code parameters. As an example, the code $[[16, 3, 9; 3]]_4$ has a higher rate (ratio between code dimension and code length) than the similar minimum distance code $[[31, 10, 10; 21]]_4$ given in Ref. [27].

Table 1. Some new MDS EAQEC codes from Reed–Solomon codes. The codes with a star ⋆ are maximal entanglement MDS EAQEC codes.

New EAQEC codes—Corollary 3 $[[n, 2b - 1, n - k + 1; n + 2b - 2k - 1]]_q$ $0 < b \leq (k+1)/2$ and $0 < k < n \leq q$	New EAQEC codes—Theorem 5 $[[q^2, t^2 - 1, q(q - t) - r + 1; (q - t)^2 - 2r - 1)]]_q$ $qt + r < q^2$, where $1 \leq t < q - r - 1$ and $0 \leq r \leq q - 1$
Examples	
⋆$[[3, 1, 3; 2]]_3$	$[[16, 3, 9; 3]]_4$
⋆$[[4, 3, 2; 1]]_4$	$[[64, 35, 17; 3]]_8$
⋆$[[7, 3, 5; 4]]_7$	$[[64, 15, 31; 11]]_8$
⋆$[[8, 5, 4; 3]]_8$	$[[256, 196, 33; 3]]_{16}$
⋆$[[11, 9, 3; 2]]_{11}$	$[[256, 120, 78; 18]]_{16}$
⋆$[[13, 9, 5; 4]]_{13}$	$[[1024, 784, 129; 15]]_{32}$
$[[16, 13, 3; 2]]_{16}$	$[[1024, 624, 220; 38]]_{32}$

One family of EAQEC codes derived from BCH codes has been constructed; see Theorem 3. Some examples of these EAQEC codes are shown in Table 2. As can be seen in Table 1 in Ref. [28] (and the reference there in), the EAQEC codes derived from Theorem 3 have new parameters when compared with EAQEC codes known in the literature. Thus, though not having good parameters as the ones in our Table 1 in terms of quantum Singleton defect, these codes are new. One advantage of our codes with respect to the ones known in the literature is that, since they are constructed from two BCH codes, we have more freedom in the choice of parameters. The family of codes presented in Table 2 could be used in environments with low amounts of resources, since we have more freedom in the code parameters. As an example, the codes in Table 2 are longer than the codes in Table 1 for the same cardinality of the finite field, making the codes in Table 2 more favorable to environments where increasing the size of individual systems is less costly than composing such systems. Looking at the examples of Table 2, we see that there is no counterpart for the codes with parameters $[[63, 7, 5; 8]]_8$ and $[[255, 19, 7; 12]]_{16}$ in Ref. [26]. However, we did not obtain an improvement in rate when comparing the remaining codes in Table 2 with the codes shown in Ref. [29].

Table 2. Some new EAQEC codes from BCH codes.

New EAQEC codes—Theorem 3
$[[q^2 - 1, 2a + 1, b + 1; 2b - \lfloor \frac{b}{q} \rfloor]]_q$
$1 \leq b \leq q$ and $0 \leq a < q - b$
Examples
$[[15, 5, 2; 2]]_4$
$[[48, 9, 3; 4]]_7$
$[[63, 7, 5; 8]]_8$
$[[255, 19, 7; 12]]_{16}$

The remaining EAQEC codes constructed in this paper are the ones derived from cyclic codes that are neither Reed–Solomon nor BCH codes. Two families of such codes were created, both of them using Hermitian construction. Some examples of parameters that can be obtained from these codes are presented in Table 3. Codes in the first column are almost MDS or almost MDS—i.e., the Singleton defect, which is when the difference between the quantum Singleton bound (QSB) presented in Equation (6) and the minimal distance of the code is equal to one or two units. Lastly, we display in the second column of Table 3 some codes from Theorem 7. All codes in Theorem 7 are maximal entanglement. Thus, this family, when extending the block length, could approach the EA quantum hashing bound similarly to what happens to turbo codes in Ref. [17]. Having length proportional to a high power of the cardinality of the field, it is expected to achieve low error probability using these codes.

To compare the codes shown in Tables 2 and 3, we are going to use the concepts of ratio, given by k/n, and net ratio, given by $(k - c)/n$, where k, c, and n are the code dimension, the number of maximally entangled states, and code length, respectively. For the code $[[80, 50, 10; 30]]_3$, we see significant improvements in rate and net rate when comparing with the codes $[[73, 36, 10; 37]]_4$ and $[[89, 44, 10; 45]]_4$ shown in Ref. [27]. A similar conclusion is obtained for the comparison between our $[[255, 237, 7; 18]]_4$ and the code $[[217, 186, 6; 31]]_4$ shown in Ref. [27]. Lastly, we also have codes with no counterpart in Ref. [27], such as $[[80, 73, 3; 1]]_3$ and $[[255, 248, 3; 1]]_4$, due to large discrepancy in code parameters.

Table 3. Some EAQEC codes from cyclic codes via Hermitian construction.

New EAQEC codes—Theorem 6	New EAQEC codes—Theorem 7
Examples	
$[[80, 73, 3; 1]]_3$	$[[80, 42, 14; 38]]_3$
$[[80, 69, 4; 1]]_3$	$[[80, 50, 10; 30]]_3$
$[[255, 248, 3; 1]]_4$	$[[255, 193, 20; 62]]_4$
$[[255, 244, 4; 1]]_4$	$[[255, 237, 7; 18]]_4$

5. Conclusions

This paper has been devoted to the use of cyclic codes in the construction of EAQEC codes. General construction methods of EAQEC codes from cyclic codes via defining sets have been presented, using both Euclidean and Hermitian duals of the classical codes. As an application of these methods, five families of EAQEC codes were created. Two of them were derived from Reed–Solomon codes, which resulted in MDS codes. An additional family of almost MDS or near almost MDS EAQEC codes was derived from general cyclic codes. One of the remaining family used BCH codes as the classical counterpart. The construction of this family of EAQEC code used two BCH codes, which provided more freedom in the parameters of the quantum code. Lastly, we conjecture that the family of constructed EAQEC codes can achieve the hashing bound when extending their length. This is supported by the fact that the codes derived have maximal entanglement. Investigations (mainly numerical) along this line are left for future work.

References

1. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2011.
2. Bowen, G. Entanglement required in achieving entanglement-assisted channel capacities. *Phys. Rev. A* **2002**, *66*, 052313-1–052313-8. [CrossRef]
3. Fattal, D.; Cubitt, T.S.; Yamamoto, Y.; Bravyi, S.; Chuang, I.L. Entanglement in the stabilizer formalism. *arXiv* **2004**, arXiv:quant-ph/0406168.
4. Brun, T.; Devetak, I.; Hsieh, M.H. Correcting Quantum Errors with Entanglement. *Science* **2006**, *314*, 436–439. [CrossRef] [PubMed]
5. Galindo, C.; Hernando, F.; Matsumoto, R.; Ruano, D. Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. *Quantum Inf. Process.* **2019**, *18*, 116. [CrossRef]
6. Wilde, M.M.; Brun, T.A. Optimal entanglement formulas for entanglement-assisted quantum coding. *Phys. Rev. A* **2008**, *77*, 064302-1–064302-4. [CrossRef]
7. Fan, J.; Chen, H.; Xu, J. Constructions of q-ary Entanglement-Assisted Quantum MDS Codes with Minimum Distance Greater than $q + 1$. *Quantum Inf. Comput.* **2016**, *16*, 423–434. [CrossRef]

8. Chen, J.; Huang, Y.; Feng, C.; Chen, R. Entanglement-assisted quantum MDS codes constructed from negacyclic codes. *Quantum Inf. Process.* **2017**, *16*, 303. [CrossRef]
9. 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 Their Appl.* **2018**, *53*, 309–325. [CrossRef]
10. Chen, X.; Zhu, S.; Kai, X. Entanglement-assisted quantum MDS codes constructed from constacyclic codes. *Quantum Inf. Process.* **2018**, *17*, 273. [CrossRef]
11. Lu, L.; Li, R.; Guo, L. Entanglement-assisted quantum codes from quaternary codes of dimension five. *Int. J. Quantum Inf.* **2017**, *15*, 1750017. [CrossRef]
12. Guenda, K.; Jitman, S.; Gulliver, T.A. Constructions of good entanglement-assisted quantum error correcting codes. *Des. Codes Cryptogr.* **2018**, *86*, 121–136. [CrossRef]
13. Liu, X.; Yu, L.; Hu, P. New entanglement-assisted quantum codes from *k*-Galois dual codes. *Finite Fields Their Appl.* **2019**, *55*, 21–32. [CrossRef]
14. Koroglu, M.E. New entanglement-assisted MDS quantum codes from constacyclic codes. *Quantum Inf. Process.* **2019**, *18*, 44. [CrossRef]
15. Li, R.; Zuo, F.; Liu, Y. A study of skew asymmetric q^2-cyclotomic coset and its application. *J. Air Force Eng. Univ. (Nat. Sci. Ed.)* **2011**, *12*, 87–89.
16. Lu, L.; Li, R. Entanglement-assisted quantum codes constructed from primitive quaternary BCH codes. *Int. J. Quantum Inf.* **2014**, *12*, 1450015. [CrossRef]
17. Wilde, M.M.; Hsieh, M.H.; Babar, Z. Entanglement-Assisted Quantum Turbo Codes. *IEEE Trans. Inf. Theory* **2014**, *60*, 1203–1222. [CrossRef]
18. Lai, C.Y.; Brun, T.A.; Wilde, M.M. Duality in Entanglement-Assisted Quantum Error Correction. *IEEE Trans. Inf. Theory* **2013**, *59*, 4020–4024. [CrossRef]
19. Li, R.; Guo, L.; Xu, Z. Entanglement-assisted quantum codes achieving the quantum Singleton bound but violating the quantum Hamming bound. *Quantum Inf. Comput.* **2014**, *14*, 1107–1116. [CrossRef]
20. Pellikaan, R.; Wu, X.W.; Bulygin, S.; Jurrius, R. *Codes, Cryptology and Curves with Computer Algebra*; Cambridge University Press: Cambridge, UK, 2017.
21. Huffman, W.C.; Pless, V. *Fundamentals of Error-Correcting Codes*; Cambridge University Press: Cambridge, UK, 2003.
22. Brun, T.A.; Devetak, I.; Hsieh, M.H. Catalytic Quantum Error Correction. *IEEE Trans. Inf. Theory* **2014**, *60*, 3073–3089. [CrossRef]
23. Guardia, G.G.L. Constructions of new families of nonbinary quantum codes. *Phys. Rev. A* **2009**, *80*, 042331-1–042331-11. [CrossRef]
24. Qian, J.; Zhang, L. Constructions of new entanglement-assisted quantum MDS and almost MDS codes. *Quantum Inf. Process.* **2019**, *18*, 71. [CrossRef]
25. Li, C. Hermitian LCD codes from cyclic codes. *Des. Codes Cryptogr.* **2018**, *86*, 2261–2278. [CrossRef]
26. Lu, L.; Li, R.; Guo, L.; Fu, Q. Maximal entanglement entanglement-assisted quantum codes constructed from linear codes. *Quantum Inf. Process.* **2015**, *14*, 165–182. [CrossRef]
27. Lv, L.; Li, R.; Fu, Q.; Li, X.; Li, X. Maximal entanglement entanglement-assisted quantum codes from quaternary BCH codes. In Proceedings of the IEEE Advanced Information Technology, Electronic and Automation Control Conference, Chongqing, China, 19–20 December 2015.
28. Luo, G.; Cao, X. Two new families of entanglement-assisted quantum MDS codes from generalized Reed–Solomon codes. *Quantum Inf. Process.* **2019**, *18*, 89. [CrossRef]
29. Guo, L.; Fu, Q.; Li, R.; Lu, L. Maximal entanglement entanglement-assisted quantum codes of distance three. *Int. J. Quantum Inf.* **2015**, *13*, 1550002-1–1550002-7. [CrossRef]