Entanglement-assisted Quantum Codes from Algebraic Geometry Codes

Francisco Revson F. Pereira[1,2], Ruud Pellikaan[1], Giuliano Gadioli La Guardia[3], and Francisco Marcos de Assis[2]

[1] Department of Mathematics and Computing Science, Eindhoven University of Technology, Eindhoven, The Netherlands.
[2] Department of Electrical Engineering, Federal University of Campina Grande, Campina Grande, Paraíba, Brazil.
[3] Department of Mathematics and Statistics, State University of Ponta Grossa, Ponta Grossa, Paraná, Brazil.
revson.ee@gmail.com

Abstract. Quantum error-correcting codes play the role of suppressing noise and decoherence in quantum systems by introducing redundancy. Some strategies can be used to improve the parameters of these codes. For example, entanglement can provide a way for quantum error-correcting codes to achieve higher rates than the one obtained by means of the traditional stabilizer formalism. Such codes are called entanglement-assisted quantum error-correcting (EAQEC) codes. In this paper, we utilize algebraic geometry codes to construct several families of EAQEC codes derived from the Euclidean and the Hermitian construction. Three families constructed here consist of codes whose quantum Singleton defect is equal to zero, one, or two. We also construct families of EAQEC codes with an encoding rate exceeding the quantum Gilbert-Varshamov bound. Additionally, asymptotically good towers of linear complementary dual codes are used to obtain asymptotically good families of EAQEC codes consuming maximal entanglement. Furthermore, a simple comparison with the quantum Gilbert-Varshamov bound demonstrates that, by utilizing the proposed construction, it is possible to generate an asymptotically family of EAQEC codes that exceeds this bound.[4]

Keywords: Quantum Codes · Algebraic Geometry Codes · Maximal Distance Separable · Maximal Entanglement · Asymptotically Good.

1 Introduction

It is generally accepted that the prospect of practical large-scale quantum computers and the use of quantum communication are only possible with the implementation of quantum error-correcting codes. Suppressing noise and decoherence can be done by means of quantum error-correcting codes. The capability of correcting errors of such codes can be improved if it is possible to have pre-shared entangled states. They are known as Entanglement-Assisted Quantum Error-Correcting (EAQEC) codes. An important feature of such class of codes is that it contains codes that achieve the hasing bound [38,24], and that there are degenerate codes that violate the Hamming bound [25]. The first EAQEC codes were proposed by Bowen [2] followed by the work from Fattal *et al.* [10]. The stabilizer formalism of EAQEC codes was introduced by Brun *et al.* [3], where they showed that EAQEC codes

[4] This paper was presented in part at the 2019 IEEE International Symposium on Information Theory.

paradigm does not require the dual-containing constraint as the standard quantum stabilizer error-correcting code does [26,34]. Wilde and Brun [37] proposed two methods to construct EAQEC codes from classical codes, which are named in this paper as the Euclidean construction method and the Hermitian construction method. These methods were recently generalized by Galindo *et al.* [12].

After these works of Brun *et al.*, many articles have focused attention on the construction of EAQEC codes based on classical linear codes [37,6,29,19,28]. However, the analysis of q-ary EAQEC codes was taken into account only recently [9,6,31,7,19,27,18,28]. The majority of them utilized constacyclic [9,7,31] or negacyclic codes [6,31] as the classical counterpart. Since the length of the classical codes is generally proportional to the square of the field's cardinality, most of the quantum codes obtained from the previous works have length proportional to the square of the size of the finite field. Hence, generating EAQEC codes having length proportional to a power, which is greater than two, of the cardinality of the field is still an open question. In addition, it has not been shown previously the existence of families of asymptotically good EAQEC codes consuming maximal entanglement that attains the quantum Gilbert-Varshamov bound [11,22,12]. Such a family can be used to achieve the hashing bound. A possible approach to solve both questions is by applying algebraic geometry (AG) codes as the classical counterpart in order to construct EAQEC codes.

The AG codes were discovered by Goppa [15]. An essential property of these codes is that its parameters can be computed by means of the degree of a divisor, which allows a direct algebraic description of the code. The first result of this paper comes from these properties. We propose two methods to construct new AG codes from old ones by utilizing intersection and also union of the corresponding divisors. As will be shown, the former "new codes from old" construction is crucial when two AG codes are used to derive EAQEC codes. To derive the EAQEC codes in this paper, it is necessary to define some mathematical tools as well as some relationships between them and the parameters of EAQEC codes.

First, we introduce the idea of intersection and union of divisors and how these concepts can be used to construct new AG codes from old. In addition, it is shown that the amount of entanglement in the Euclidean construction method of EAQEC codes can be described based on the intersection of the two classical codes utilized in the process. The practicality of such a description is presented by applying our method to AG codes derived from three curves: the projective line (rational function field), the Hermitian curve, and elliptic curves. The EAQEC codes derived from the first (third) type of curve are shown to be maximal distance separable (MDS) codes (almost MDS codes), i.e., the minimum distance of these codes achieves the quantum Singleton bound (differs from the quantum Singleton bound by one or two units). These curves are also used to construct EAQEC codes consuming maximal entanglement. Therefore, they can be employed to achieve the entanglement-assisted quantum capacity of a depolarizing channel [2,8,30]. In the case of the Hermitian curve, a comparative analysis with the codes in the literature shows that our codes have better parameters.

The use of AG codes in the Hermitian construction method for EAQEC codes does not follow the same procedure as the Euclidean one. This is because a general characterization of the Hermitian dual code of an AG code still an open question. To determine the parameters of EAQEC codes derived from two AG codes utilized in the process, the intersection of the bases of them is computed. In this construction, the curve utilized to construct the EAQEC codes is the projective line. Here, we also derive almost MDS EAQEC codes, where some of them consume maximal entanglement.

Lastly, asymptotically good families of linear complementary dual codes are used to construct asymptotically good families of EAQEC codes consuming maximal entanglement. By applying AG codes from a tower of function fields that attain the Drinfeld-Vladut bound [35] we show that the EAQEC codes in this paper surpass the quantum Gilbert-Varshamov bound [11,22,12].

The paper is organized as follows. In Section 2, we describe some basic concepts on AG codes necessary for the development of the paper. Moreover, two methods to construct new AG codes from old ones are shown. Afterwards, in Section 3, several new families of EAQEC codes are derived from AG codes. These derivations come from the Euclidean and the Hermitian construction methods for EAQEC codes using three different types of curves. In Section 4, we compare the parameters of our new codes with respect to the quantum Singleton bound and also with other parameters shown in the literature. In particular, it is shown that three families of EAQEC codes constructed are MDS or almost MDS. In Section 5, we show the existence of families of EAQEC codes exceeding the quantum Gilbert-Varshamov bound. Lastly, the final remarks are in Section 6.

Notation. Throughout this paper, p denotes a prime number and q is a power of p. $F/\mathbb{F}_q$ denotes an algebraic function field over $\mathbb{F}_q$ of genus g, where $\mathbb{F}_q$ denotes 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. 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 consumes c pre-shared entangled pairs.

2 Preliminaries

In this section, we recall some concepts of linear complementary dual (LCD) codes, algebraic geometry (AG) codes, and entanglement-assisted quantum error-correcting (EAQEC) codes. Before giving a description of LCD codes, a definition for the Euclidean and the Hermitian dual of a code are presented.

Definition 1. *Let* $\mathbf{a}$ *and* $\mathbf{b}$ *be two vectors in* $\mathbb{F}_q^n$*. The standard or Euclidean inner product of them is defined by*

$$\mathbf{a} \cdot \mathbf{b} = \sum_{i=1}^{n} a_i b_i. \tag{1}$$

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

$$C^{\perp} = \{\mathbf{x} \in \mathbb{F}_q^n | \mathbf{x} \cdot \mathbf{c} = 0 \textit{ for all } \mathbf{c} \in C\}. \tag{2}$$

If C is $\mathbb{F}_{q^2}$-linear, then the Hermitian dual of C is defined by

$$C^{\perp_h} = \{\mathbf{x} \in \mathbb{F}_{q^2}^n | \mathbf{x} \cdot \mathbf{c}^q = 0 \textit{ for all } \mathbf{c} \in C\}, \tag{3}$$

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

In the case that the intersection between a code and its dual results only in the zero vector, the code is called LCD. A formal description is given below.

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

The class of LCD codes is a possible way to construct EAQEC codes consuming maximal entanglement and, at the same time, providing asymptotically good families of EAQEC codes (see Sections 3 and 5, respectively).

2.1 Algebraic Geometry codes

This subsection reviews some mathematical tools from algebraic geometry and how to use them to derive algebraic geometry (AG) codes. See [35] for more details.

Let $F/\mathbb{F}_q$ be an algebraic function field of genus g. A place P of $F/\mathbb{F}_q$ is the maximal ideal of some valuation ring $\mathcal{O}_P$ of $F/\mathbb{F}_q$. See Definition 1.1.4 and Proposition 1.1.5 of Ref. [35] for more details. We also define the set of all places by $\mathbb{P}_F = \{P | P \textit{ is a place of } F/\mathbb{F}_q\}$.

A divisor of $F/\mathbb{F}_q$ is a formal sum of places given by $D = \sum_{P \in \mathbb{P}_F} n_P P$, with $n_P \in \mathbb{Z}$, where almost all $n_P = 0$. The support and degree of D are defined as $\text{supp}(D) = \{P \in \mathbb{P}_F | n_p \neq 0\}$ and $\deg(D) = \sum_{P \in \mathbb{P}_F} n_P \deg(P)$, respectively, where $\deg(P)$ is the degree of the place P. When a place has degree one, it is called a rational place.

The discrete valuation corresponding to a place P is written as ν_P. For every element f of $F/\mathbb{F}_q$, we define the principal divisor of f by $(f) = \sum_{P \in \mathbb{P}_F} \nu_P(f) P$. For $f \in \mathcal{O}_P$, we define $f(P) \in \mathcal{O}_P/P$ to be the residue class of f modulo P; for $f \in F \setminus \mathcal{O}_P$, we put $f(P) = \infty$. For a given divisor G, we denote the Riemann-Roch space associated to G by $\mathcal{L}(G) = \{f \in F^* | (f) \geq -G\} \cup \{0\}$.

The given description of Riemann-Roch spaces shows that when we are talking about such spaces, we deal with functions that obey a set of rules described by the defining divisor. One natural question that could arise is the relation between the intersection of two Riemann-Roch spaces and the respective divisor that defines such a space. Such a result is shown in Ref. [33]. Before showing it, we need to define the intersection and union of two divisors, which is done in the following.

Definition 3. *Let G and H be divisors over $F/\mathbb{F}_q$. If $G = \sum_{P \in \mathbb{P}_F} \nu_P(G) P$ and $H = \sum_{P \in \mathbb{P}_F} \nu_P(H) P$, where $P \in \mathbb{P}_F$ is a place, then the intersection $G \cap H$ of G and H over $F/\mathbb{F}_q$ is defined as follows*

$$G \cap H = \sum_{P \in \mathbb{P}_F} \min\{\nu_P(G), \nu_P(H)\} P. \tag{4}$$

In addition, the union is given by

$$G \cup H = \sum_{P \in \mathbb{P}_F} \max\{\nu_P(G), \nu_P(H)\} P. \tag{5}$$

Proposition 1. *[33, Lemma 2.6] Let G and H be divisors over $F/\mathbb{F}_q$. Then $\mathcal{L}(G) \cap \mathcal{L}(H) = \mathcal{L}(G \cap H)$.*

In Section 3 it will be shown that when AG codes are used to construct EAQEC codes, the amount of entanglement used is related to the dimension of the intersection of the two Riemann-Roch spaces.

For the exact value of the dimension of a Riemann-Roch space and the construction of the dual code of an AG code, it is necessary to introduce the ideas of Weil differential and canonical divisors. Let $\mathcal{A}_F$ be the adele space of $F/\mathbb{F}_q$ (see Section 1.5 of Ref. [35] for more details on adele and adele space). A Weil differential of $F/\mathbb{F}_q$ is a $\mathbb{F}_q$-linear map $\omega \colon \mathcal{A}_F \to \mathbb{F}_q$ vanishing on $\mathcal{A}_F(A) + F$ for some divisor A of F, where $\mathcal{A}_F(A) = \{\alpha \in \mathcal{A}_F | \nu_P(\alpha) \geq -\nu_P(A) \text{ for all } P \in \mathbb{P}_F\}$. The divisor of a nonzero differential ω, denote by $(\omega) = \sum_{P \in \mathbb{P}_F} \nu_P(\omega) P$, is called canonical divisor of ω. All canonical divisors are equivalent and have degree equal to $2g - 2$. The set of Weil differentials of $F/\mathbb{F}_q$ is denoted by Ω_F. Lastly, for a divisor G we define $\Omega_F(G) = \{\omega \in \Omega_F | \omega = 0 \text{ } or \text{ } (\omega) \geq G\}$. It is possible to show that Ω_F is a module and $\Omega_F(G)$ is a vector space over $\mathbb{F}_q$ [35].

The dimension of a Riemann-Roch space can be calculated through its defining divisor, the divisor of a Weil differential, and the genus of a curve.

Proposition 2. *[35, Theorem 1.5.15](Riemann-Roch Theorem) Let W be a canonical divisor of $F/\mathbb{F}_q$. Then for each divisor G, the dimension of $\mathcal{L}(G)$ is given by $\ell(G)$. Further, $\ell(G) = \deg(G) + 1 - g + \ell(W - G)$, where $\deg(G)$ is the degree of the divisor G.*

Now we define the first AG code utilized in this paper, see Definition 4, and its parameters, see Proposition 3. The definition of such AG codes is given as the image of a linear map called the evaluation map. The parameters of the AG codes are related to the degrees of divisors, genus, and the number of rational places. Thus, with simple arithmetic, we can create families of codes, even when the algebraic function field is fixed.

Definition 4. *Let $P_1, \ldots, P_n$ be pairwise distinct rational places of $F/\mathbb{F}_q$ and $D = P_1 + \cdots + P_n$. Choose a divisor G of $F/\mathbb{F}_q$ such that $\operatorname{supp}(G) \cap \operatorname{supp}(D) = \varnothing$. The algebraic geometry (AG) code $C_{\mathcal{L}}(D, G)$ associated with the divisors D and G is defined as the image of the linear map $ev_D \colon \mathcal{L}(G) \to \mathbb{F}_q^n$ called the evaluation map, where $ev_D(f) = (f(P_1), \ldots, f(P_n))$; i.e., $C_{\mathcal{L}}(D, G) = \{(f(P_1), \ldots, f(P_n)) | f \in \mathcal{L}(G)\}$.*

Proposition 3. *[35, Corollary 2.2.3]Let $F/\mathbb{F}_q$ be a function field of genus g. Then the AG code $C_{\mathcal{L}}(D,G)$ is an $[n,k,d]$-linear code over $\mathbb{F}_q$ with parameters $k=\ell(G)-\ell(G-D)$ and $d \geq n-\deg(G)$. If $2g-2<\deg(G)<n$, then $k=\deg(G)-g+1$.*

The next two propositions present a way to construct new AG codes from old AG codes via the intersection and union of divisors. Proposition 4 will be used in Section 3 in order to use AG codes to create EAQEC codes.

Proposition 4. *Let $F/\mathbb{F}_q$ be a function field of genus g and let D be a divisor as in Definition 4. If G_1 and G_2 are two divisors such that* $\text{supp}G_1 \cap \text{supp}D = \varnothing$*, resp.* $\text{supp}G_2 \cap \text{supp}D = \varnothing$*, and* $\deg(G_1 \cup G_2) < n$*, then $C_{\mathcal{L}}(D,G_1) \cap C_{\mathcal{L}}(D,G_2) = C_{\mathcal{L}}(D,G_1 \cap G_2)$.*

Proof. First of all, consider that $\mathbf{c} \in C_{\mathcal{L}}(D,G_1) \cap C_{\mathcal{L}}(D,G_2)$, then there exist $g_1 \in \mathcal{L}(G_1)$ and $g_2 \in \mathcal{L}(G_2)$ such that $\mathbf{c} = ev_D(g_1) = ev_D(g_2)$, which implies $ev_D(g_1-g_2)=0$. Since $g_1-g_2 \in \mathcal{L}(G_1 \cup G_2)$ and $\deg(G_1 \cup G_2) < n$, then $g_1 = g_2 \in \mathcal{L}(G_1 \cap G_2)$ by Proposition 1. Consequently, $\mathbf{c} \in C_{\mathcal{L}}(D,G_1 \cap G_2)$. The converse inclusion is a straightforward consequence of Proposition 1. □

Proposition 5. *Let $F/\mathbb{F}_q$ be a function field of genus g and let D be a divisor as in Definition 4. If G_1 and G_2 are two divisors such that* $\text{supp}G_1 \cap \text{supp}D = \varnothing$, $\text{supp}G_2 \cap \text{supp}D = \varnothing$*, and* $\deg(G_1 \cap G_2) > 2g-2$ *and* $\deg(G_1 \cup G_2) < n$*, then $C_{\mathcal{L}}(D,G_1) + C_{\mathcal{L}}(D,G_2) = C_{\mathcal{L}}(D,G_1 \cup G_2)$.*

Proof. Firstly, consider the inclusion $C_{\mathcal{L}}(D,G_1) + C_{\mathcal{L}}(D,G_2) \subseteq C_{\mathcal{L}}(D,G_1 \cup G_2)$. Since $G_i \leq G_1 \cup G_2$, for $i=1,2$, then $C_{\mathcal{L}}(D,G_i) \subseteq C_{\mathcal{L}}(D,G_1 \cup G_2)$, for $i=1,2$. Hence $C_{\mathcal{L}}(D,G_1) + C_{\mathcal{L}}(D,G_1) \subseteq C_{\mathcal{L}}(D,G_1 \cup G_2)$. On the other hand, notice that $\ell(G_1) + \ell(G_2) = \ell(G_1 \cap G_2) + \ell(G_1 \cup G_2)$, since $\deg(G_1 \cap G_2) > 2g-2$. This implies that $\mathcal{L}(G_1 \cup G_2) = \mathcal{L}(G_1) + \mathcal{L}(G_2)$ by Proposition 1. Now, the proof of the converse inclusion follows from the hypothesis that $\deg(G_1 \cup G_2) < n$ and Proposition 4. □

Another important type of AG code is given in the following.

Definition 5. *Let $F/\mathbb{F}_q$ be a function field of genus g and let G and D be divisors as in Definition 4. Then we define the code $C_{\Omega}(D,G)$ as $C_{\Omega}(D,G) = \{(res_{P_1}(\omega), \ldots, res_{P_n}(\omega)) | \omega \in \Omega_F(G-D)\}$, where $res_{P_i}(\omega)$ denotes the residue of ω at P_i.*

Proposition 6. *[35, Theorem 2.2.7] Let $C_{\Omega}(D,G)$ be the AG code from Definition 5. If* $2g-2 <$ $\deg(G) < n$*, then $C_{\Omega}(D,G)$ is an $[n,k',d']$-linear code over $\mathbb{F}_q$, where* $k' = n+g-1-\deg(G)$ *and* $d' \geq \deg(G)-(2g-2)$*.*

The relationship between the codes $C_{\mathcal{L}}(D,G)$ and $C_{\Omega}(D,G)$ is given in the next proposition.

Proposition 7. *[35, Proposition 2.2.10] Let $C_{\mathcal{L}}(D,G)$ be the AG code described in Definition 4. Then $C_{\Omega}(D,G)$ is its Euclidean dual, i.e., $C_{\mathcal{L}}(D,G)^{\perp} = C_{\Omega}(D,G)$. Additionally, if we have a Weil differential η such that $\nu_{P_i}(\eta) = -1$ and $\eta_{P_i}(1) = 1$ for all $i = 1, \ldots, n$, then $C_{\Omega}(D,G) = C_{\mathcal{L}}(D,G^{\perp})$, where $G^{\perp} = D - G + (\eta)$.*

2.2 Entanglement-assisted quantum codes

An $[[n,k]]_q$ quantum error-correcting code is a q^k-dimensional $\mathbb{C}$-linear subspace of $\mathbb{C}^{q^n}$. Therefore, it encodes k logical qudits into n physical qudits; this means that the encoder $\mathcal{E}$ is an injective map taking a vector $|\psi\rangle \in \mathbb{C}^{q^k}$ to $|\Psi\rangle = \mathcal{E}(|\psi\rangle \otimes \left|0^{n-k}\right\rangle) \in \mathbb{C}^{q^n}$. Let G_n be the error group over $\mathbb{C}^{q^n}$. We define the weight of an error operator $E \in G_n$ to be the number of terms in the tensor product which are not equal to the identity operator. For more details about error groups and error operators, see Refs. [26,34]. The code has minimum distance d if d is the minimum number such that the code can detect every error over $\mathbb{C}^{q^n}$ of weight $d-1$ or less acting nontrivially on the code. This implies that a quantum code of minimum distance d has the error-correction capacity to correct $\lfloor (d-1)/2 \rfloor$ quantum errors [1]. As mentioned before, it is possible to improve the error-correction capacity of a quantum error-correcting code using entanglement. If a quantum code with the previous parameters consumes c pre-shared copies of maximally entangled states, such as Bell states [34], we say that the quantum code is an entanglement-assisted quantum error-correcting (EAQEC) code with parameters $[[n,k,d;c]]_q$. See [3,37,12] for more details. Figure 1 gives a communication scheme which uses an EAQEC code to protect quantum information from a noisy quantum channel. In Figure 1, the state $|\psi\rangle$ represents the logical qudits to be encoded, $\left|0^{n-k-c}\right\rangle$ is the ancilla qudits, which is a tensor product of $n-k-c$ zero vectors, $|\Phi^{\otimes c}\rangle$ denotes c copies of a maximally entangled state pre-shared between the sender and the receiver, and $|\psi'\rangle$ represents the decoded state. The boxes $\mathcal{E}$, $\mathcal{D}$, $\mathcal{N}$, and $\mathrm{id}^{\otimes c}$ represents the encoding map, decoding map, quantum noisy channel, and the assumption that receiver's qudits part of maximally entangled pre-shared states suffer no errors since they do not pass through the noisy channel, respectively.

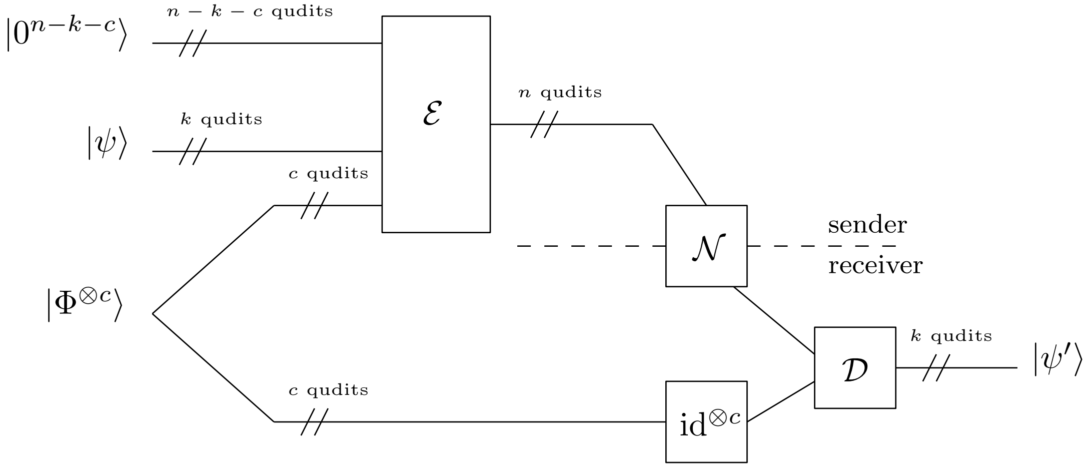

Fig. 1. Communication scheme using an EAQEC code [4].

A formal description of an entanglement-assisted quantum error-correcting code is given below:

Definition 6. *An entanglement-assisted quantum error-correcting (EAQEC) code $\mathcal{Q}$ with parameters $[[n,k,d;c]]_q$ is an q^k-dimensional subspace of $\mathbb{C}^{q^n}$ with minimum distance d that consumes c pre-shared copies of maximally entangled states. The rate of an EAQEC code is given by k/n, relative distance by d/n, and entanglement-assisted rate by c/n. Lastly, an EAQEC code is said to consume or require maximal entanglement when $c = n-k$.*

It is important to mention that through this paper, we assume that the maximally entangled states used in the EAQEC codes are error-free. As described in [3], this can be seen as a physically realistic hypothesis.

A measurement of goodness for an EAQEC code is the quantum Singleton bound (QSB). A general formulation of it for qubits is shown in [23]. In particular, for $d \leq (n+2)/2$ we have

$$k + 2d \leq n + c + 2. \tag{6}$$

Since the examples in this paper where we use the QSB for analyzing their goodness have $d \leq (n+2)/2$, then we attain our attention only to QSB given in Eq. 6. The difference between $n-k+c+2$ and $2d$ is called quantum Singleton defect. Associated with it, we have two definitions. An EAQEC code is called a maximum distance separable (MDS) quantum code if the quantum Singleton defect is zero. On the other hand, when the quantum Singleton defect is equal to one or two, we say that an EAQEC code is an almost MDS quantum code.

Formulating a stabilizer paradigm for EAQEC codes gives a way to use classical codes to construct these quantum codes [4]. In particular, using an appropriate mapping from $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ to subgroups of the error group defined over $\mathbb{C}^{q^n}$, Galindo *et al.* [12] derived the following relations between classical and EAQEC codes. During this paper, we call them the Euclidean and the Hermitian construction methods for Propositions 8 and 9, respectively.

Proposition 8. *[12, 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 an EAQEC code with parameters $[[n, k_1+k_2-n+c, d; c]]_q$, with $d = \min\{d_H(C_1 \setminus (C_1 \cap C_2^{\perp})), d_H(C_2 \setminus (C_1^{\perp} \cap C_2))\}$, where d_H is the minimum Hamming weight of the vectors in the set, and*

$$c = \operatorname{rank}(H_1 H_2^T) = \dim C_1^{\perp} - \dim(C_1^{\perp} \cap C_2) \tag{7}$$

is the number of required maximally entangled states.

A straightforward application of LCD codes to the Proposition 8 can produce some interesting quantum codes. See Theorem 1 and Corollary 1.

Theorem 1. *Let C_1 and C_2 be two linear codes with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$, respectively, with $C_1^\perp \cap C_2 = \{\mathbf{0}\}$. Then there exists an EAQEC code with parameters $[[n, k_2, \min\{d_1, d_2\}; n - k_1]]_q$.*

Proof. Since that $C_1^\perp \cap C_2 = \{\mathbf{0}\}$, from Proposition 8 we have that the EAQEC code constructed from C_1 and C_2 has parameters $[[n, k_2, \min\{d_1, d_2\}; n - k_1]]_q$. □

Corollary 1. *Let C be a LCD code with parameters $[n, k, d]_q$. Then there exists a EAQEC code consuming maximal entanglement with parameters $[[n, k, d; n - k]]_q$. In particular, if C is MDS then the EAQEC codes is also MDS.*

Proof. Let $C_1 = C_2 = C$. Since C is LCD, then $\dim(hull(C)) = 0$. Then, from Theorem 1, we have that there exists an EAQEC code with parameters $[[n, k, d; n - k]]_q$. □

Proposition 9. *[12, Proposition 3 and Corollary 1] Let C be a linear codes over $\mathbb{F}_{q^2}$ with parameters $[n, k, d]_{q^2}$, H be a parity check matrix of C, and H^* be the q-th power entry-wise of the transpose matrix of H. Then there is an EAQEC code with parameters $[[n, 2k - n + c, d'; c]]_q$, where $d' = d_H(C \setminus (C \cap C^{\perp_h}))$, where d_H is the minimum Hamming weight of the vectors in the set, and*

$$c = \operatorname{rank}(HH^*) = \dim C^{\perp_h} - \dim(C^{\perp_h} \cap C) \tag{8}$$

is the number of required maximally entangled states.

In the same way as before, it possible to use Hermitian LCD codes to derive EAQEC codes with interesting properties. See the following theorem.

Theorem 2. *Let C be a Hermitian LCD code with parameters $[n, k, d]_{q^2}$. Then there exists a EAQEC code consuming maximal entanglement with parameters $[[n, k, d; n - k]]_q$. In particular, if C is MDS, then the EAQEC code is also MDS.*

Proof. Since C is a Hermitian LCD code, then $\dim(hull_H(C)) = 0$. Therefore, using C in the Proposition 9, we have that there exists an EAQEC code with parameters $[[n, k, d; n - k]]_q$. □

3 New Construction Methods for EAQEC Codes

3.1 Euclidean Construction

In Proposition 8, the connection between the entanglement in an EAQEC code and the intersection of two codes has been shown. However, the computation of such an intersection can be difficult to calculate in some cases; however, as we are going to show in Theorem 3, this is not the case for AG codes. This result is derived from Proposition 4.

Theorem 3. *Let $P_1, \dots, P_n$ be pairwise distinct rational places of $F/\mathbb{F}_q$ and $D = P_1 + \cdots + P_n$. Choose divisors G_1, G_2 of $F/\mathbb{F}_q$ such that* $\mathrm{supp}(G_1) \cap \mathrm{supp}(D) = \varnothing$ *and* $\mathrm{supp}(G_1) \cap \mathrm{supp}(D) = \varnothing$*. Let $C_1 = C_{\mathcal{L}}(D, G_1)$ and $C_2 = C_{\mathcal{L}}(D, G_2)$. If* $\deg(G_1^{\perp} \cup G_2) < n$*, then* $\dim(C_1^{\perp} \cap C_2) = \ell(G_1^{\perp} \cap G_2)$*.*

Proof. Since $\deg(G_1^{\perp} \cup G_2) < n$, we can use Proposition 4 for the codes $C_{\mathcal{L}}(D, G_1)^{\perp}$ and $C_{\mathcal{L}}(D, G_2)$. Hence, it is easy to see from this proposition that $C_{\mathcal{L}}(D, G_1)^{\perp} \cap C_{\mathcal{L}}(D, G_2) = C_{\mathcal{L}}(D, G_1^{\perp} \cap G_2)$, which implies that $\dim(C_{\mathcal{L}}(D, G_1)^{\perp} \cap C_{\mathcal{L}}(D, G_2)) = \ell(G_1^{\perp} \cap G_2)$. □

Theorem 3 allows us to use AG codes from any function field to construct EAQEC codes, which is given in detail in Theorem 4. In particular, as it will be shown, we can use AG codes to derive MDS quantum codes and asymptotically good EAQEC codes.

Theorem 4. *Let $P_1, \dots, P_n$ be pairwise distinct rational places of $F/\mathbb{F}_q$ and $D = P_1 + \cdots + P_n$. Choose divisors G_1, G_2 of $F/\mathbb{F}_q$ such that* $\mathrm{supp}(G_i) \cap \mathit{supp}(D) = \varnothing$ *and $2g - 2 < \deg(G_i) < n$, for $i = 1, 2$. Let $C_1 = C_{\mathcal{L}}(D, G_1)$ and $C_2 = C_{\mathcal{L}}(D, G_2)$. If* $\deg(G_1^{\perp} \cup G_2) < n$*, then there exists an EAQEC code with parameters* $[[n, \deg(G_1 + G_2) - 2g + 2 - n + c, d; c]]_q$*, where* $d \geq n - \max\{\deg(G_1), \deg(G_2)\}$ *and* $c = n + g - 1 - \deg(G_1) - \ell(G_1^{\perp} \cap G_2)$*.*

Proof. First of all, notice that the parameters of the AG codes $C_{\mathcal{L}}(D, G_1)$ and $C_{\mathcal{L}}(D, G_2)$ are $[n, \deg(G_1) - g + 1, d_1 \geq n - \deg(G_1)]_q$ and $[n, \deg(G_2) - g + 1, d_2 \geq n - \deg(G_2)]_q$, respectively, and the dimension of the Euclidean dual of $C_{\mathcal{L}}(D, G_1)$ is $n + g - 1 - \deg(G_1)$, by Proposition 7. From Theorem 3 we have that $\dim(C_1^{\perp} \cap C_2)) = \ell(G_1^{\perp} \cap G_2)$. Hence, using Proposition 8 we derive the mentioned parameters of the EAQEC code. □

Corollary 2. *Let $P_1, \dots, P_n$ be pairwise distinct rational places of $F/\mathbb{F}_q$ and $D = P_1 + \cdots + P_n$. Choose divisors G_1, G_2 of $F/\mathbb{F}_q$ such that* $\mathrm{supp}(G_i) \cap \mathrm{supp}(\mathrm{D}) = \varnothing$ *and $2g - 2 < \deg(G_i) < n$, for $i = 1, 2$. If* $\deg(G_1^{\perp} \cup G_2) < n$ *and* $\deg(G_1^{\perp} \cap G_2) < 0$*, then there exists an EAQEC code with parameters* $[[n, \deg(G_2) - g + 1, d; c]]_q$*, where* $d \geq n - \max\{\deg(G_1), \deg(G_2)\}$ *and* $c = n + g - 1 - \deg(G_1)$*. In particular, if $G_1 = G_2 = G$, then the EAQEC code has parameters* $[[n, \deg(G) - g + 1, d; n + g - 1 - \deg(G)]]_q$*, where* $d \geq n - \deg(G)$*.*

The first explicit description of a family of EAQEC codes constructed in this paper is shown in the following theorem. The rational function field $\mathbb{F}_q(z)/\mathbb{F}_q$ is used to derive this family.

Theorem 5. *Let q be a power of a prime. Consider a_1, a_2, b_1, b_2 positive integers such that $b_1 \leq a_2$ and $b_2 \leq q - 2 - a_2$, with $a_1 + a_2 < q - 1$ and $b_1 + b_2 < q - 1$, then we have the following:*

- *If $b_2 \geq a_1 + 1$, then there exists an EAQEC code with parameters*

$$[[q - 1, a_1 + b_1 - 1, \geq q - 1 - \max\{a_1 + a_2, b_1 + b_2\}; q - 2 - (a_2 + b_2)]]_q.$$

– *If $b_2 < a_1 + 1$, then there exists an EAQEC code with parameters*

$$[[q-1, b_1+b_2+1, \geq q-1-\max\{a_1+a_2, b_1+b_2\}; q-2-(a_1+a_2)]]_q.$$

Proof. Let $\mathbb{F}_q(z)/\mathbb{F}_q$ be the rational function field. The Weil differential $\eta = \frac{1}{x^q-x}dx$ satisfies the requirements of Proposition 7 and it has divisor given by $(\eta) = (q-2)P_\infty - P_0 - D$, where P_∞ and P_0 are the place at infinity and the origin, respectively, and $D = \sum_{i=1}^{q-1} P_i$, with P_i being the remaining rational places. Assume that $G_1 = a_1P_0 + a_2P_\infty$ and $G_2 = b_1P_0 + b_2P_\infty$ and $C_1 = C_\mathcal{L}(D, G_1)$ and $C_2 = C_\mathcal{L}(D, G_2)$. Since $b_2 \leq q-2-a_2$, we have that $\deg(G_1^\perp \cup G_2) = b_1 + q - 2 - a_2 < q-1$, by the hypothesis $b_1 \leq a_2$, and $G_1^\perp \cap G_2 = (-1-a_1)P_0 + b_2P_\infty$. Thus, we can use Theorem 4. For the first case, we have that $c = q-1-1-(a_1+a_2)-(b_2-a_1) = q-2-(a_2+b_2)$, since $\deg(G_1^\perp \cap G_2) \geq 0$. For the second case, when $b_2 < a_1+1$, we have that $\deg(G_1^\perp \cap G_2) < 0$, which implies $\ell(G_1^\perp \cap G_2) = 0$ and $c = q-2-(a_1+a_2)$. The remaining claims are derived from Theorem 4 and from the observation that $\deg(G_1) = a_1 + a_2$ and $\deg(G_2) = b_1 + b_2$. □

Corollary 3. *If $a_1 \leq a_2 - 1$ and $a_2 \leq (q-2)/2$, there are almost MDS $[[q-1, 2a_1-1, \geq q-1-(a_1+a_2); q-2-2a_2)]]_q$ EAQEC codes. On the other hand, if $a_1 \leq q-2-a_2$ and $a_1+a_2 \leq q-2$, then there exists a MDS $[[q-1, a_1+a_2+1, q-1-(a_1+a_2); q-2-(a_1+a_2)]]_q$ EAQEC codes consuming maximal entanglement.*

Proof. Consider the first case of Theorem 5. Then considering $a_1 \leq a_2 - 1$, $a_2 \leq (q-2)/2$, $b_1 = a_1$, and $b_2 = a_2$, the first family of EAQEC codes follows. For the second one, consider the second case of Theorem 5. Therefore, for $a_1 \leq q-2-a_2$, $b_1 \leq a_2$, $b_2 \leq \min\{q-2-a_2, a_1\}$, and $a_1+a_2 = b_1+b_1 \leq q-2$, there is a family of EAQEC codes with the mentioned parameters. □

The following theorem shows construction of EAQEC codes derived from the Hermitian function field. Next, elliptic function fields will be used to obtain EAQEC codes consuming maximal entanglement with quantum Singleton defect at most two.

Theorem 6. *Let q be a power of a prime and a_1, a_2, b_1, b_2 be positive integers such that $b_1 \leq a_2 - q(q-1)$, $b_2 \leq q^3 + q(q-1) - 2 - a_2$, with $b_1 + b_2 < q^3 - 1$ and $a_1 + a_2 < q^3 - 1$. Then we have the following:*

– *If $b_2 \geq a_1 + 1$, then there exists an EAQEC code with parameters*

$$[[q^3-1, a_1+b_1+1, \geq q^3-1-\max\{a_1+a_2, b_1+b_2\}; q^3-2+q(q-1)-(a_2+b_2)]]_{q^2}.$$

– *If $b_2 < a_1 + 1$, then there exists an EAQEC code with parameters*

$$[[q^3-1, b_1+b_2+1-\frac{q(q-1)}{2}, \geq q^3-1-\max\{a_1+a_2, b_1+b_2\}; q^3-2+\frac{q(q-1)}{2}-(a_1+a_2)]]_{q^2}.$$

Proof. Let $F/\mathbb{F}_{q^2}$ be the Hermitian function field defined by the equation

$$y^q + y = x^{q+1}.$$

Then $F/\mathbb{F}_{q^2}$ has $1+q^3$ rational points and genus $g = q(q-1)/2$. Assume that $D = P_1 + \cdots + P_{q^3-1}$, $G_1 = a_1P_0 + a_2P_\infty$, and $G_2 = b_1P_0 + b_2P_\infty$, where P_∞ and P_0 are the rational places at infinity and the origin, respectively. Thus, one possible Weil differential satisfying Proposition 7 is given by $\eta = \frac{1}{x^{q^2}-x}dx$, which has divisor $(\eta) = -D - P_0 + (q^3 + q(q-1) - 2)P_\infty$. The fact that $b_2 \leq q^3 + q(q-1) - 2 - a_2$ implies $G_1^\perp \cup G_2 = b_1P_0 + (q^3 + q(q-1) - 2 - a_2)P_\infty$. By the hypothesis $b_1 \leq a_2 - q(q-1)$, we have that $\deg(G_1^\perp \cup G_2) < q^3 - 1$, thus we can use Theorem 4. From this theorem, we derive that $G_1^\perp \cap G_2 = (-1 - a_1)P_0 + b_2P_\infty$. Hence, if $b_2 \geq a_1 + 1$ we have that $\deg(G_1^\perp \cap G_2) \geq 0$, which implies $c = q^3 - 1 + \frac{q(q-1)}{2} - 1 - (a_1 + a_2) - (b_2 - a_1) + \frac{q(q-1)}{2} = q^3 - 2 + q(q-1) - (a_2 + b_2)$. On the other hand, if $b_2 < a_1 + 1$ we have that $\deg(G_1^\perp \cap G_2) < 0$, which implies $\ell(G_1^\perp \cap G_2) = 0$ and $c = q^3 - 2 + \frac{q(q-1)}{2} - (a_1 + a_2)$. Since $\deg(G_1) = a_1 + a_2$ and $\deg(G_1) = b_1 + b_2$, using Theorem 4 and the values of c computed, we derive the mentioned parameters for the EAQEC codes. □

Theorem 7. *Let $q = 2^m$, with $m \geq 1$ an integer. Let $F/\mathbb{F}_q$ be an elliptic function field with e rational places and genus $g = 1$ defined by the equation*

$$y^2 + y = x^3 + bx + c, \tag{9}$$

where $b, c \in \mathbb{F}_q$. Let a_1, a_2, b_1, b_2 be positive integers such that $b_1 \leq a_2$, $b_2 \leq e - 1 - a_2$, with $a_1 + a_2 < e - 2$ and $b_1 + b_2 < e - 2$. Then we have the following:

- *If $b_2 \geq a_1 + 1$, then there exists an EAQEC code with parameters*

$$[[e-2, a_1 + b_1 + 1, \geq e - 2 - \max\{a_1 + a_2, b_1 + b_2\}; e - 1 - (a_2 + b_2)]]_q.$$

- *If $b_2 < a_1 + 1$, then there exists an EAQEC code with parameters*

$$[[e-2, b_1 + b_2, \geq e - 2 - \max\{a_1 + a_2, b_1 + b_2\}; e - 2 - (a_1 + a_2)]]_q.$$

Proof. First of all, let $S = \{\alpha \in \mathbb{F}_q | \text{there exists } \beta \in \mathbb{F}_q \text{ such that } \beta^2 + \beta = \alpha^3 + b\alpha + c\}$. For each $\alpha \in S$, there are two $\beta \in \mathbb{F}_q$ satisfying the equation $\beta^2 + \beta = \alpha^3 + b\alpha + c$. Thus, for each $\alpha \in S$, there are two places corresponding to $x-$coordinate equal to α. Hence, the set of all rational places is given by these x and y coordinates and the place at infinity, P_∞. The number of rational places is denoted by e. So $e = |S| + 1$. Now, assume that $D = \sum_{i=1}^{e-2} P_i$, $G_1 = a_1P_0 + a_2P_\infty$, and $G_2 = b_1P_0 + b_2P_\infty$, where $P_0, P_1, \ldots, P_{e-1}$ are pairwise distinct rational places. Additionally, let $\eta = \frac{dx}{\prod_{\alpha_i \in S}(x + \alpha_i)}$, then the divisor of the Weil differential η is given by $(\eta) = (e-1)P_\infty - P_0 - D$. The fact that $b_2 \leq e - 1 - a_2$

implies $G_1^{\perp} \cup G_2 = b_1 P_0 + (e-1-a_2)P_\infty$. By the hypothesis $b_1 \leq a_2$, we have that $\deg(G_1^{\perp} \cup G_2) < e-2$, thus we can use Theorem 4. From this theorem, we derive that $G_1^{\perp} \cap G_2 = (-1-a_1)P_0 + b_2 P_\infty$. Hence, if $b_2 \geq a_1 + 1$ we have that $\deg(G_1^{\perp} \cap G_2) \geq 0$, which implies $c = e - 1 - (a_2 + b_2)$. On the other hand, if $b_2 < a_1 + 1$ we have that $\deg(G_1^{\perp} \cap G_2) < 0$, which implies $\ell(G_1^{\perp} \cap G_2) = 0$ and $c = e - 2 - (a_1 + a_2)$. Since $\deg(G_1) = a_1 + a_2$ and $\deg(G_1) = b_1 + b_2$, using Theorem 4 and the values of c computed, we derive the mentioned parameters for the EAQEC codes. □

Corollary 4. *Suppose that there exists an elliptic curve with e rational places. Then for $a_1 \leq a_2 - 1$ and $a_2 \leq (e-1)/2$, there are almost MDS $[[e-2, 2a_1+1, \geq e-2-(a_1+a_2); e-1-2a_2)]]_q$ EAQEC codes.*

Proof. Consider the first case of Theorem 7. Then considering $a_1 \leq a_2 - 1$, $a_2 \leq (e-1)/2$, $b_1 = a_1$, and $b_2 = a_2$, the result follows. □

It is shown in Table 1 the number of rational points on several elliptic curves as a function of s, the degree of the extension $\mathbb{F}_{2^s}$ [32].

Table 1. Some elliptic curves over $\mathbb{F}_q$ ($q = 2^s$) and their number of rational places

Elliptic curve	s	Number of rational places (e)
$y^2 + y = x^3$	odd s	$q+1$
	$s \equiv 0 \mod 4$	$q+1-2\sqrt{q}$
	$s \equiv 0 \mod 2$	$q+1+2\sqrt{q}$
$y^2+y = x^3+x$	$s \equiv 1, 7 \mod 8$	$q+1+\sqrt{2q}$
	$s \equiv 3, 5 \mod 8$	$q+1-\sqrt{2q}$
$y^2+y = x^3+x+1$	$s \equiv 1, 7 \mod 8$	$q+1-\sqrt{2q}$
	$s \equiv 3, 5 \mod 8$	$q+1+\sqrt{2q}$
$y^2 + y = x^3 + \delta x$ ($Tr(\delta) = 1$)	s even	$q+1$
$y^2 + y = x^3 + \delta$ ($Tr(\delta) = 1$)	$s \equiv 0 \mod 4$	$q+1+2\sqrt{q}$
	$s \equiv 2 \mod 4$	$q+1-2\sqrt{q}$

Remark 1. In this section, two-point AG codes have been used to construct EAQEC codes. The reason for this is that one-point AG codes have trivial values for the dimension of the hull. Therefore, using two-point AG codes allow, at least to some extent, to control the dimension of the hull and the parameters of EAQEC codes derived from them.

3.2 Hermitian Construction

In contrast to the Euclidean dual of an AG code, a general formula describing the Hermitian dual of an AG code, as in Definition 4, is still an open question. However, by describing an AG code via a basis of evaluated elements that belong to a Riemann-Roch space, we can obtain the information that we need from the Hermitian dual code. Before doing that, we approach the dimension of the intersection between an AG code and its Hermitian dual.

Proposition 10. *Let C be a linear code over $\mathbb{F}_{q^2}$ with length n and $C^{\perp_h}$ its dual. Then* $\dim(C \cap C^{\perp_h}) = \dim(C^{\perp} \cap C^q)$.

Proof. Although it is well known that $C^{\perp_h} = (C^{\perp})^q$ [20], we present this result here for completeness

$$\begin{aligned}
\mathbf{x} \in C^{\perp_h} \qquad & \iff \mathbf{x} \cdot \mathbf{c}^q = 0, && \forall \mathbf{c} \in C,\\
& \iff \textstyle\sum_{i=1}^{n} x_i c_i^q = 0, && \forall \mathbf{c} \in C,\\
& \iff \textstyle\sum_{i=1}^{n} x_i^q c_i = 0, && \forall \mathbf{c} \in C, \text{ since } c_i^{q^2} = c_i\\
& \iff \mathbf{x}^q \in C^{\perp},\\
& \iff \mathbf{x} \in (C^{\perp})^q.
\end{aligned}$$

Thus, we see that

$$\begin{aligned}
\dim(C \cap C^{\perp_h}) &= \dim(C \cap (C^{\perp})^q)\\
&= \dim(C^q \cap C^{\perp}).
\end{aligned}$$

Hence, we have $\dim(C \cap C^{\perp_h}) = \dim(C^{\perp} \cap C^q)$. □

Proposition 10 shows a new way to compute the dimension of $C \cap C^{\perp_h}$. To be able to use it for AG codes, we need to describe the linear code C^q. Proposition 11 approaches this by showing that it is possible to compute a basis to C^q from a basis of C.

Proposition 11. *Let C be a linear code over $\mathbb{F}_{q^2}$ with length n and dimension k. If $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ is a basis of C, then a basis of C^q is given by the set $\{\mathbf{x}_1^q, \ldots, \mathbf{x}_k^q\}$.*

Proof. First of all, notice that for any $\mathbf{c}' \in C^q$ there is a unique $\mathbf{c} \in C$ such that $\mathbf{c}' = \mathbf{c}^q$. Since that $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ is a basis for C, then $\mathbf{c} = \sum_{i=1}^{k} c_i \mathbf{x}_i$, for $c_i \in \mathbb{F}_{q^2}$. Therefore, $\mathbf{c}' = \mathbf{c}^q = \sum_{i=1}^{k} c_i^q \mathbf{x}_i^q = \sum_{i=1}^{k} c_i' \mathbf{x}_i^q$. Since that C and C^q are isomorphic, then they have the same dimension which implies that $\{\mathbf{x}_1^q, \ldots, \mathbf{x}_k^q\}$ is a basis for C^q. □

The following result, which is an elementary exercise in Linear Algebra, on the intersection of vector spaces is used in Theorem 8 to determine the parameters of EAQEC codes from the Hermitian construction method.

Lemma 1. *Let B be a basis for $\mathbb{F}_{q^2}^n$ and B_1 and B_2 be two subsets of B. Denoting by V_1 and V_2 the subspaces generated by B_1 and B_2, respectively, then we have that* $\dim(V_1 \cap V_2) = |B_1 \cap B_2|$.

Now, we derive EAQEC codes from the Hermitian construction using AG codes. To illustrate this, we are going to apply the result from Lemma 1 to AG codes derived from rational function field. See Theorem 8.

Theorem 8. *Let q be a prime power and m an integer which is written as $m = qt + r < q^2$, where $t \geq 1$ and $0 \leq r \leq q-1$. Then we have the following:*

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

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

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

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

Proof. Let $F(z)/\mathbb{F}_{q^2}$ be the rational function field, $D = \sum_{i=0}^{q^2-1} P_i$ and $G = mP_\infty$, where $m = qt + r$. Let $C_{\mathcal{L}}(D, G)$ be the AG code derived from D and G with parameters $[q^2, m+1, q^2 - m]_q$. Consider $\boldsymbol{x^i} = ev_D(x^i)$. Let $B = \{\boldsymbol{x^i} | 0 \leq i \leq n-1\}$. Then B is a basis of $\mathbb{F}_{q^2}^n$. A basis for $C_{\mathcal{L}}(D, G)$ is given by a subset, $B' = \{\boldsymbol{x^i} | 0 \leq i \leq m\}$. Thus, a basis of $C_{\mathcal{L}}(D, G)^q$ can be described as $B_1 = \{\boldsymbol{x^{qi}} | 0 \leq i \leq m\}$. Now, notice that $\boldsymbol{x^{q^2+a}} = \boldsymbol{x^{a+1}}$ for all $a \geq 0$. Therefore,

$$B_1 = \{\boldsymbol{x^{qi+j}} | 0 \leq i \leq q-1, 0 \leq j \leq t-1\} \cup \{\boldsymbol{x^{qi+t}} | 0 \leq i \leq r\}.$$

On the other hand, a basis of $C_{\mathcal{L}}(D, G)^\perp$ is given by the set

$$B_2 = \{\boldsymbol{x^i} | 0 \leq i \leq q^2-2-m\} = \{\boldsymbol{x^{qi+j}} | 0 \leq i \leq q-t-2, 0 \leq j \leq q-1\} \cup \{\boldsymbol{x^{(q-t-1)q+j}} | 0 \leq j \leq q-r-2\}.$$

Thus, the exponents of $\boldsymbol{x}$ in the bases B_1 and B_2 can be represented by the sets

$$\left\{\begin{array}{cccccc}
0 & 1 & 2 & \cdots & t-1 & t \\
q & q+1 & q+2 & \cdots & q+t-1 & q+t \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\
rq & rq+1 & rq+2 & \cdots & rq+t-1 & rq+t \\
\vdots & \vdots & \vdots & \cdots & \vdots & \\
(q-1)q & (q-1)q+1 & (q-1)q+2 & \cdots & (q-1)q+t-1 &
\end{array}\right\}.$$

and

$$\left\{\begin{array}{cccccc} 0 & 1 & \cdots & q-r-2 & \cdots & q-1 \\ q & q+1 & \cdots & q+q-r-2 & \cdots & 2q-1 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ (q-t-2)q & (q-t-2)q+1 & \cdots & (q-t-2)q+q-r-2 & \cdots & (q-t-2)q+q-1 \\ (q-t-1)q & (q-t-1)q+1 & \cdots & (q-t-1)q+q-r-2 & & \end{array}\right\},$$

respectively. It is easy to see that B_1 and B_2 are subsets of a basis for $\mathbb{F}_{q^2}^n$. Thus, it is possible to compute the intersection of the codes related to B_1 and B_2 via the computation of the intersection of these sets. 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

$$B_1 \cap B_2 = \{\boldsymbol{x}^{\boldsymbol{qi+j}} | 0 \leq i \leq q-t-2, 0 \leq j \leq t\} \cup \{\boldsymbol{x}^{\boldsymbol{(q-t-1)q+j}} | 0 \leq j \leq q-r-2\}.$$

Thus, $\dim(C_{\mathcal{L}}(D,G)^q \cap C_{\mathcal{L}}(D,G)^{\perp}) = |B_1 \cap B_2| = (q-t-1)(t+1)+q-r-1$. Using the same description for the case $t < q-r-1$, we see that

$$B_1 \cap B_2 = \{\boldsymbol{x}^{\boldsymbol{qi+j}} | 0 \leq i \leq q-t-1, 0 \leq j \leq t-1\} \cup \{\boldsymbol{x}^{\boldsymbol{qi+t}} | 0 \leq i \leq r\},$$

which implies $\dim(C_{\mathcal{L}}(D,G)^q \cap C_{\mathcal{L}}(D,G)^{\perp}) = |B_1 \cap B_2| = (q-t)t+r+1$. Applying the previous computations, and using the fact that $C_{\mathcal{L}}(D,G)$ has parameters $[q^2, m+1, q^2-m]_q$, by Proposition 9, we have that there exists an EAQEC code with parameters

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

□

4 Code Comparison

In Tables 2 and 3, we present some optimal EAQEC codes obtained from Theorems 5, 7 and 8. The EAQEC codes derived from the Euclidean construction are presented in Table 2. We use AG codes obtained from the projective line and elliptic curves to construct these codes. As can be seen, the codes in Table 2 are almost MDS. For Table 3, the EAQEC codes are derived from the Hermitian construction, where rational AG codes were used as the classical code. These codes also have an optimal combination of parameters since they are almost MDS EAQEC codes.

The remaining EAQEC codes that are compared with the literature are the ones derived from the Hermitian curve. The first analysis of the goodness of our codes is via the quantum Singleton defect,

Table 2. Some new almost MDS EAQEC codes from the Euclidean construction

New EAQEC codes – Theorem 5	New EAQEC codes – Theorem 7
$[[q-1, 2a_1-1, q-1-(a_1+a_2); q-2-2a_2]]_q$	$[[e-2, 2a_1+1, \geq e-2-(a_1+a_2); e-1-2a_2]]_q$
$a_1 \leq a_2-2$, and $a_2 \leq (q-2)/2$	$a_1 \leq a_2-1$, $a_2 \leq (e-1)/2$, and e as in Table 1
Examples	
–	$[[7, 3, 4; 4]]_4$
$[[10, 1, 6; 3]]_{11}$	$[[11, 5, 5; 4]]_8$
$[[12, 3, 6; 3]]_{13}$	$[[11, 7, 4; 4]]_8$
$[[12, 1, 8; 5]]_{13}$	$[[23, 19, 4; 4]]_{16}$
$[[15, 5, 7; 4]]_{16}$	$[[23, 15, 8; 8]]_{16}$
$[[31, 21, 7; 4]]_{32}$	$[[39, 27, 8; 4]]_{32}$
$[[31, 13, 15; 12]]_{32}$	$[[39, 27, 12; 12]]_{32}$

Table 3. Some new almost MDS EAQEC codes from the Hermitian construction

New EAQEC codes – Theorem 8
$[[q^2, (t+1)^2+2r+1-2q, q^2-(qt+r); (q-t-1)^2]]_q$
$m = qt+r < q^2$, $t \geq q-r-1$ and $0 \leq r \leq q-1$
Examples
$[[16, 6, 6; 1]]_4$
$[[49, 25, 13; 1]]_7$
$[[49, 11, 24; 9]]_7$
$[[64, 29, 20; 4]]_8$
$[[64, 25, 22; 4]]_8$
$[[81, 33, 29; 9]]_9$
$[[81, 16, 41; 16]]_9$
$[[256, 141, 66; 16]]_{16}$

which is the difference between the quantum Singleton bound (QSB) presented in Eq. 6 and the minimum distance of the code. Recall that an $[[n, k, d; c]]_q$ quantum code satisfies $k + 2d \leq n + c + 2$ (QSB). Hence, the codes derived from Theorem 6 have maximum quantum Singleton defect equal to $q(q-1)+|a_1+a_2-b_1-b_2|$. Some examples of parameters derived are $[[7, 3, 4; 4]]_4$, $[[26, 10, 11; 10]]_9$, and $[[63, 19, 32; 31]]_{16}$ which have quantum Singleton defect 1, 6, and 13, respectively. Comparing these examples with "standard" quantum stabilizer codes, we see that our codes have minimum distance unreachable for the same length and dimension. This can be seen from the quantum Singleton bound for stabilizer codes, which is given by $k + 2d \leq n + 2$ for an $[[n, k, d]]_q$ stabilizer code, and Refs. [16,17]. Thus, even though the codes from Theorem 6 are not MDS, they can be used to attain parameters that are unreachable by quantum stabilizer codes. Additionally, we can construct EAQEC codes that have rate higher than the asymptotic quantum Gilbert-Varshamov bound presented in Section 5, such as $[[63, 39, 23; 32]]_{16}$, $[[124, 51, 54; 53]]_{25}$, and $[[342, 179, 122; 121]]_{49}$ EAQEC codes.

Defining entanglement defect as the difference between the amount of entanglement required for the EAQEC code and $n-k$, we see that the entanglement defect in the family of EAQEC code shown in Theorem 6 for $b_2 < a_1 + 1$ is equal to $2g = q(q-1)$. Lastly, Table 4 shows some other examples of EAQEC codes that have unreachable minimum distance when compared with quantum stabilizer codes.

Table 4. Some new EAQEC codes from the Hermitian Curve

New EAQEC codes – Theorem 6
$[[q^3-1, a_1+b_1+1, q^3-1-\max\{a_1+a_2, b_1+b_2\};$ $q^3+q(q-1)-(a_2+b_2)-2]]_{q^2}$
$b_1 \leq a_2 - q(q-1)$, $a_1+1 \leq b_2 \leq q^3+q(q-1)-2-a_2$, and $a_1+a_2, b_1+b_2 < q^3-1$
Examples
$[[26, 11, 10; 14]]_9$
$[[63, 25, 27; 26]]_{16}$
$[[124, 81, 24; 42]]_{25}$
$[[342, 200, 101; 103]]_{49}$

One possible analysis and comparison of the codes constructed in this paper is via linear programming (LP) bounds for EAQEC codes. However, the only paper in the literature dealing with this is [23]. In there, the authors show LP bounds for binary EAQEC codes. Since our codes are defined over qudits, we cannot use their bounds. Therefore, since a generalization for qudits of the LP bounds derived in [23] seems computationally demanding, we have chosen to analyze and compare our codes using quantum Singleton bound, asymptotic quantum Gilbert-Varshamov bound, and comparing the parameters with “standard” quantum stabilizer codes.

One last but important point about the codes in this paper can be stressed here. The EAQEC codes constructed in the previous sections allow one to vary the number of maximally entangled states required by the code. Therefore, the choice of the code to be used can be made under the assumptions of the physical system. For instance, in a case where using maximally entangled states is not costly, one could use codes with minimum distance higher than the one achievable by any standard quantum stabilizer codes with the same length and dimension.

5 Asymptotically Good EAQEC Codes Consuming Maximal Entanglement

In this section, we show that from any family of (classical) asymptotically good AG codes, we can construct a family of asymptotically good EAQEC codes consuming maximal entanglement. This is a consequence of the use of the result from Carlet, *et al.* [5] applied to the Corollary 1. Before showing it, we need to define the concept of (classical) asymptotically good codes.

Definition 7. *Let q be a prime power and $\alpha_q := \sup\{R \in [0,1] \colon (\delta, R) \in U_q\}$, for $0 \leq \delta \leq 1$. Here U_q denotes the set of all ordered pair $(\delta, R) \in [0,1]^2$ for which there is a family of linear codes that are indexed as C_i, with parameters $[n_i, k_i, d_i]_q$, such that $n_i \to \infty$ as $i \to \infty$ and $\delta = \lim_{i\to\infty} d_i/n_i$, $R = \lim_{i\to\infty} k_i/n_i$. If $\delta, R > 0$, then the family is called asymptotically good.*

Proposition 12. *[5, Corollary 14] Let $q > 3$ be a power of a prime and $A(q) = \limsup_{g\to\infty} \frac{N_q(g)}{g}$, where $N_q(g)$ denotes the maximum number of rational places that a global function field of genus g with full constant field $\mathbb{F}_q$ can have (see Remark 2). Then there exists a family of LCD codes with*

$$\alpha_q^{LCD}(\delta) \geq 1 - \delta - \frac{1}{A(q)}, \text{ for } \delta \in [0,1]. \tag{10}$$

Remark 2. If q is a square, then $A(q) = \sqrt{q} - 1$ by [36,21]. For some numerical examples of attainable $N_q(g)$ that an algebraic function field can achieve, see Refs. [14,13].

Theorem 9. *Let $q > 3$ be a power of a prime and $A(q)$ as defined in Proposition 12. Then there exists a family of asymptotically good EAQEC codes consuming maximal entanglement with parameters $[[n_t, k_t, d_t; c_t]]_q$, such that*

$$\lim_{t\to\infty} \frac{d_t}{n_t} \geq \delta, \qquad \lim_{t\to\infty} \frac{k_t}{n_t} \geq 1 - \delta - \frac{1}{A(q)},$$

and

$$\lim_{t\to\infty} \frac{c_t}{n_t} \in [\delta, \delta + 1/A(q)].$$

for all $\delta \in [0, 1 - 1/A(q)]$.

Proof. Let $\mathcal{C} = \{C_1, C_2, \ldots\}$ be a family of asymptotically good LCD codes as the ones in Proposition 12, where each C_i has parameters $[n_i, k_i, d_i]_q$. If we apply the family $\mathcal{C}$ to construct EAQEC codes, it follows from Corollary 1 that we can construct EAQEC codes consuming maximal entanglement with parameters $[[n_t, k_t, d_t; c_t]]_q$, such that

$$\lim_{t\to\infty} \frac{d_t}{n_t} = \lim_{i\to\infty} \frac{d_i}{n_i} \geq \delta, \qquad \lim_{t\to\infty} \frac{k_t}{n_t} = \lim_{i\to\infty} \frac{k_i}{n_i} \geq 1 - \delta - \frac{1}{A(q)}.$$

Moreover, we have

$$\lim_{t\to\infty} \frac{c_t}{n_t} = \lim_{i\to\infty} \frac{n_i - k_i}{n_i} = \lim_{i\to\infty} 1 - \frac{k_i}{n_i} \leq \delta + \frac{1}{A(q)}$$

and

$$\lim_{t\to\infty}\frac{c_t}{n_t}=\lim_{i\to\infty}\frac{n_i-k_i}{n_i}\geq\lim_{i\to\infty}\frac{d_i-1}{n_i}\geq\delta,$$

for $\delta\in[0,1-1/A(q)]$. Thus, since the families in Proposition 12 are asymptotically good, then the family of EAQEC codes is asymptotically good and consumes maximal entanglement. □

Proposition 13. *[12, Theorem 6] Let R, ϵ and λ be nonnegative real numbers such that $R\leq 1$, $\epsilon<1/2$, and $\lambda\leq(1-R)/2$. Let $h(x):=-x\log_q x-(1-x)\log_q(x-1)$ be the q-ary entropy function. For n sufficiently large, the inequality $h(\epsilon)+\epsilon\log_q(q^2-1)<1-R$ implies the existence of a code $C\subseteq\mathbb{F}_q^{2n}$ over $\mathbb{F}_q$ such that $dimC=\lceil n(1-R)\rceil$, $d_s(C^{\perp_s}\setminus(C^{\perp_s}\cap C))\geq\lfloor n\epsilon\rfloor$ and $dimC-dim(C^{\perp_s}\cap C)=\lfloor 2n\lambda\rfloor$, where $C^{\perp_s}$ is the symplectic dual of C and d_s is the minimum symplectic weight of the vectors in the set.*

Remark 3. The quantum Gilbert-Varshamov bound for standard quantum codes has been derived in the works of Feng and Ma [11], and Ketkar, *et al.* [22]. In a recent paper, Galindo, *et al.* [12] derived the quantum Gilbert-Varshamov bound for EAQEC codes, which is stated in Proposition 13. Using AG codes derived from towers of function fields that attain the Drinfeld-Vladut bound [35] and the previous theorem, we can show that there is a family of EAQEC codes with parameters that exceed the mentioned bound (see Figure 2).

6 Final Remarks

This paper has been devoted to the use of AG codes in the construction of EAQEC codes. We first showed two methods to construct new AG codes from old ones by means of intersection and as well as by union of divisors. Afterward, the former method is applied to construct quantum codes based on the Euclidean construction method for EAQEC codes. Three families derived in this part are MDS or almost MDS and, for some particular range of parameters, consume maximal entanglement. For the EAQEC codes constructed from the Hermitian function field, we have shown that it is possible to achieve higher minimal distance when compared with standard quantum stabilizer codes. Additionally, they have parameters exceeding the entanglement-assisted quantum Gilbert-Varshamov bound. Concerning the Hermitian method for EAQEC codes, we have constructed a family of almost MDS EAQEC codes from AG codes. Lastly, it was shown that for any asymptotically good family of classical codes, there exists a family of asymptotically good EAQEC codes consuming maximal entanglement. Furthermore, it is demonstrated that there are asymptotic EAQEC codes exceeding the quantum Gilbert-Varshamov bound.

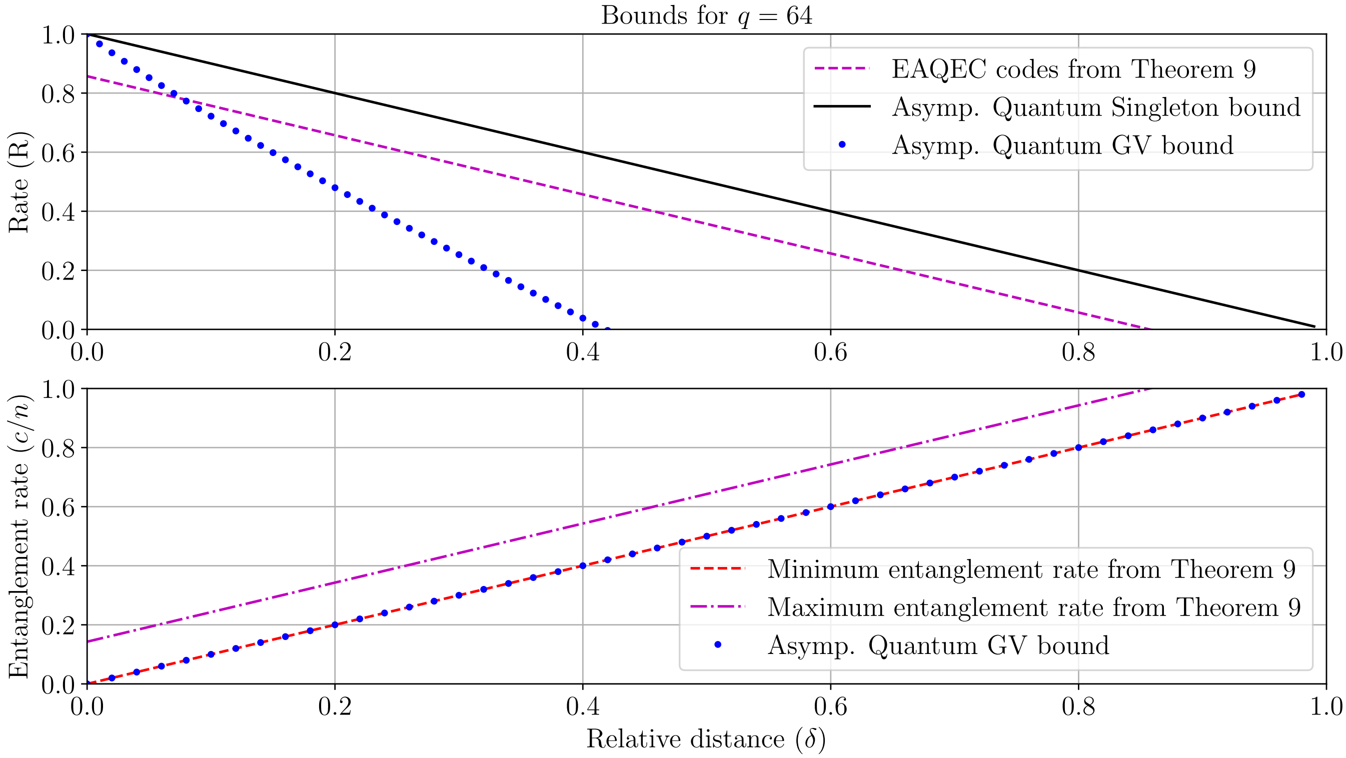

Fig. 2. Comparison between EAQEC codes derived from Theorem 9 and quantum Gilbert-Varshamov bound of [12] via analysis of rate and relative entanglement when $q = 64$.

7 Acknowledgements

This work was supported by the *Conselho Nacional de Desenvolvimento Científico e Tecnológico* (CNPq, Brazil), grant No. 201223/2018-0.

References

1. Ashikhmin, A., Knill, E.: Nonbinary quantum stabilizer codes. IEEE Transactions on Information Theory **47**(7), 3065–3072 (Nov 2001)
2. Bowen, G.: Entanglement required in achieving entanglement-assisted channel capacities. Physical Review A **66**, 052313–1–052313–8 (Nov 2002)
3. Brun, T., Devetak, I., Hsieh, M.H.: Correcting quantum errors with entanglement. Science **314**(5798), 436–439 (Oct 2006)
4. Brun, T.A., Devetak, I., Hsieh, M.H.: Catalytic quantum error correction. IEEE Transactions on Information Theory **60**(6), 3073–3089 (Jun 2014)
5. Carlet, C., Mesnager, S., Tang, C., Qi, Y., Pellikaan, R.: Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$. IEEE Transactions on Information Theory **64**(4), 3010–3017 (Apr 2018)

6. Chen, J., Huang, Y., Feng, C., Chen, R.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. Quantum Information Processing **16**(12), 303 (Nov 2017)
7. Chen, X., Zhu, S., Kai, X.: Entanglement-assisted quantum MDS codes constructed from constacyclic codes. Quantum Information Processing **17**(10), 273 (Oct 2018)
8. Devetak, I., Harrow, A.W., Winter, A.J.: A resource framework for quantum Shannon theory. IEEE Transactions on Information Theory **54**(10), 4587–4618 (Oct 2008)
9. Fan, J., Chen, H., Xu, J.: Constructions of q-ary entanglement-assisted quantum MDS codes with minimum distance greater than $q+1$. Quantum Information and Computation **16**(5&6), 423–434 (2016)
10. Fattal, D., Cubitt, T.S., Yamamoto, Y., Bravyi, S., Chuang, I.L.: Entanglement in the stabilizer formalism (Jun 2004), `arXiv:quant-ph/0406168`
11. Feng, K., Ma, Z.: A finite Gilbert–Varshamov bound for pure stabilizer quantum codes. IEEE Transactions on Information Theory **50**(12), 3323–3325 (dec 2004). https://doi.org/10.1109/tit.2004.838088
12. Galindo, C., Hernando, F., Matsumoto, R., Ruano, D.: Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. Quantum Information Processing **18**(4), 116 (Apr 2019)
13. van der Geer, G., Howe, E.W., Lauter, K.E., Ritzenthaler, C.: Tables of curves with many points (2009), `http://www.manypoints.org`
14. van der Geer, G., van der Vlugt, M.: Tables of curves with many points. Mathematics of Computation **69**(230), 797–810 (Aug 1999)
15. Goppa, V.D.: Codes on algebraic curves. Soviet Mathematics Doklady **22**(1), 170–172 (1981)
16. Grassl, M.: Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de` (Accessed on 2020-02-10)
17. Grassl, M., Rotteler, M.: Quantum MDS codes over small fields. In: 2015 IEEE International Symposium on Information Theory (ISIT) (Jun 2015)
18. Guenda, K., Gulliver, T.A., Jitman, S., Thipworawimon, S.: Linear ℓ-intersection pairs of codes and their applications. Designs, Codes and Cryptography **88**(1), 133–152 (Jan 2020)
19. Guenda, K., Jitman, S., Gulliver, T.A.: Constructions of good entanglement-assisted quantum error correcting codes. Designs, Codes and Cryptography **86**(1), 121–136 (Jan 2018)
20. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. University Press, Cambridge (2003)
21. Ihara, Y.: Some remarks on the number of rational points of algebratic curves over finite fields. Journal of the Faculty of Science, the University of Tokyo. Sect. 1 A, Mathematics **28**, 721–724 (1981)
22. Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.: Nonbinary stabilizer codes over finite fields. IEEE Transactions on Information Theory **52**(11), 4892–4914 (nov 2006). https://doi.org/10.1109/tit.2006.883612
23. Lai, C.Y., Ashikhmin, A.: Linear programming bounds for entanglement-assisted quantum error-correcting codes by split weight enumerators. IEEE Transactions on Information Theory **64**(1), 622–639 (Jan 2018)
24. Lai, C.Y., Brun, T.A., Wilde, M.M.: Dualities and identities for entanglement-assisted quantum codes. Quantum Information Processing **13**(4), 957–990 (Apr 2014)
25. Li, R., Guo, L., Xu, Z.: Entanglement-assisted quantum codes achieving the quantum singleton bound but violating the quantum Hamming bound. Quantum Information & Computation **14**(13), 1107–1116 (Oct 2014)
26. Lidar, D.A., Brun, T.A. (eds.): Quantum Error Correction. Cambridge University Press (2013)
27. Liu, X., Liu, H., Yu, L.: Entanglement-assisted quantum codes from Galois LCD codes (Sep 2018), `arXiv:1809.00568`
28. Liu, X., Yu, L., Hu, P.: New entanglement-assisted quantum codes from k-Galois dual codes. Finite Fields and Their Applications **55**, 21–32 (Jan 2019)
29. Lu, L., Li, R., Guo, L.: Entanglement-assisted quantum codes from quaternary codes of dimension five. International Journal of Quantum Information **15**(3), 1750017 (April 2017)
30. Lu, L., Li, R., Guo, L., Fu, Q.: Maximal entanglement entanglement-assisted quantum codes constructed from linear codes. Quantum Information Processing **14**(1), 165–182 (Jan 2015)
31. 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 and Their Applications **53**, 309–325 (Sep 2018)
32. Menezes, A.: Elliptic Curve Public Key Cryptosystems. The Springer International Series in Engineering and Computer Science, Springer (1993)

33. Munuera, C., Pellikaan, R.: Equality of geometric Goppa codes and equivalence of divisors. Journal of Pure and Applied Algebra (1993)
34. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press (2011)
35. Stichtenoth, H.: Algebraic Function Fields and Codes. Springer (2009)
36. Tsfasman, M.A., Vlădutx, S.G., Zink, T.: Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. Mathematische Nachrichten **109**, 21–28 (1982)
37. Wilde, M.M., Brun, T.A.: Optimal entanglement formulas for entanglement-assisted quantum coding. Physical Review A **77**(6), 064302–1–064302–4 (Jun 2008)
38. Wilde, M.M., Hsieh, M.H., Babar, Z.: Entanglement-assisted quantum turbo codes. IEEE Transactions on Information Theory **60**(2), 1203–1222 (Feb 2014)