Application of Complementary Dual AG Codes to Entanglement-Assisted Quantum Codes

Francisco R. F. Pereira*‡, Ruud Pellikaan*, Giuliano G. La Guardia†, and Francisco M. de Assis‡
*Department of Mathematics and Computing Science, TU/e, The Netherlands, {f.r.fernandes.pereira,g.r.pellikaan}@tue.nl
†Department of Mathematics and Statistics, State University of Ponta Grossa, Brazil, gguardia@uepg.br
‡Department of Electrical Engineering, Federal University of Campina Grande, Brazil, fmarcos@dee.ufcg.edu.br

***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 via traditional stabilizer formalism. Such codes are called entanglement-assisted quantum (QUENTA) codes. In this paper, we use algebraic geometry codes to construct two families of QUENTA codes, where one of them has maximal entanglement and is maximal distance separable. In the end, we show that for any asymptotically good tower of algebraic function fields there is an asymptotically good family of maximal entanglement QUENTA codes with nonzero rate, relative minimal distance, and relative amount of entanglement.**

***Index Terms*—Quantum Codes, Algebraic Geometry Codes, Maximal Distance Separable, Maximal Entanglement, Asymptotically Good.**

I. 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. Quantum error correcting codes play the role of suppressing noise and decoherence by introducing redundancy. The capability of correcting errors of such codes can be improved if it is possible to have pre-shared entanglement states. This class of codes is known as Entanglement-Assisted Quantum (QUENTA) codes, traditionally denoted by EAQEC codes in the literature. Additionally, this class of codes can achieve the hashing bound [1], [2] and violate the quantum Hamming bound [3]. The first QUENTA codes were proposed by Bowen [4] followed by the work from Fattal, *et al.* [5]. The stabilizer formalism of QUENTA codes was created by Brun *et al.* [6], where they showed that QUENTA codes paradigm does not require the dual-containing constraint as the standard quantum error-correcting code does [7].

After this landmark paper from Brun *et al.*, many works have focused on the construction of QUENTA codes based on classical linear codes [8]–[12]. However, the analysis of q-ary QUENTA codes was taken into account only recently [9], [11]–[17]. The majority of them utilized constacyclic codes [13]–[15] or negacyclic codes [9], [14] as the classical counterpart. Since the length of the classical codes is normally proportional to the square of the size of the field, most of the quantum codes from the previous works have a length that is proportional to the square of the size of the finite field. On the other hand, Liu *et al.* used k-Galois dual codes [12] and Galois LCD codes [16], which allow quantum codes with length lower than the previous ones mentioned. So, there is no result in the literature with QUENTA codes having length proportional to a greater power of the cardinality of the finite field. In addition, it has not been shown previously that there exists a family of asymptotically good maximal entanglement QUENTA codes. Such a family can be used to achieve the hashing bound. A possible approach to solve both questions is using algebraic geometry codes (AG) codes as the classical counterpart to construct QUENTA codes.

The AG codes were invented by Goppa [18] and have several properties. Two properties important for this paper are that its parameters can be calculated via the degree of a divisor, which allows a direct description of the code, and the intersection of two AG codes can be associated to a linear code that is also an AG code. As will be shown, using AG codes we can derive quantum codes with interesting properties. Before presenting such results, some constructions have been made.

First of all, we introduce the idea of relative hull, which is a generalization of the concept of hull utilized in the construction of Linear Complementary Dual (LCD) codes [19]. With this tool, it is possible to quantify the amount of entanglement in an QUENTA codes in a more direct way if the intersection of two classical codes is known. As will be shown, this is the case for AG codes. An analysis of the lower bound for the minimal distance of some quantum codes constructed demonstrates that this bound differs from the Singleton bound in one unit, leading to the conclusion that it is possible to construct QUENTA codes from AG codes that are almost maximal distance separable (MDS) codes; i.e., they have Singleton defects at maximum equal to one. Furthermore, these codes also have maximal entanglement, which can be employed to achieve entanglement-assisted quantum capacity of a depolarizing channel [4], [20], [21]. We give three examples of families of QUENTA codes with these properties.

The paper is organized as follows. In Section II, we describe what needs to be known about AG codes so that they can be applied to the construction method of Wilde and Brun [8]. Afterwards, a few basic description of how to utilize AG codes to construct QUENTA codes are given in Section III. In this same section, we apply the method proposed to AG codes constructed from Hermitian and Elliptic function fields; the latter function field allows QUENTA codes that are almost MDS. In Section IV, we show that there exists families of QUENTA codes that are asymptotically good in its rate, relative distance and entanglement-assisted rate. Lastly, the conclusion is carried out in Section V.

Notation. Throughout this paper, p denotes a prime number and q is a power of p. Let $F/\mathbb{F}_q$ be 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 utilizes c pre-shared entanglement pairs.

II. Preliminaries

In this section, we introduce some ideas related to linear complementary dual (LCD) codes, algebraic geometry (AG) codes and entanglement-assisted quantum (QUENTA) codes. The first description to be given is that of LCD codes, but first we need to give the definition of the Euclidean dual of a code.

Definition 1: Let C be a linear code over $\mathbb{F}_q^n$. The dual of C is defined as $C^\perp := \{\ \mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x}\cdot\mathbf{c} = 0 \text{ for all } \mathbf{c} \in C\ \}$.

When the intersection between a code and its dual gives only the vector $\mathbf{0}$, the code is called LCD. A formal description can be seen below.

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, $hull(C) = \{\mathbf{0}\}$.

The class of LCD codes gives a possible way to construct QUENTA codes that have maximal entanglement and asymptotically good families (see Sections III and IV).

When we consider two linear codes instead of one, the idea of relative hull and linear complementary pairs emerge. The next definition gives such a description.

Definition 3: Let C_1 and C_2 be two $\mathbb{F}_q$-linear code. The *relative hull* of C_1 over C_2 is defined by $hull(C_1, C_2) := C_1^\perp \cap C_2$. If $hull(C_1, C_2) = \{\mathbf{0}\}$, then C_1 is called a linear C_2-complementary dual code.

For the present paper, the relative hull between two codes will have a direct relation with the amount of entanglement used by an QUENTA code (see Theorem 1).

A. Algebraic-Geometry codes

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 $F/\mathbb{F}_q$. We also define $\mathbb{P}_F := \{P | P \textit{ is a place of } F/\mathbb{F}_q\}$.

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 $supp(D) := \{P \in \mathbb{P}_F | n_p \neq 0\}$ 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 x of $F/\mathbb{F}_q$, we can define a principal divisor of x by $(x) := \sum_{P\in\mathbb{P}_F} \nu_P(x)P$. For $x \in \mathcal{O}_P$, we define $x(P) \in \mathcal{O}_P/P$ to be the residue class of x modulo P; for $x \in F \setminus \mathcal{O}_P$, we put $x(P) := \infty$. For a given divisor G, we denote the Riemann-Roch space associated to G by $\mathcal{L}(G) = \{x \in F | (x) \geq -G\} \cup \{0\}$.

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 which are 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 was shown by Munuera and Pellikaan [22]. Before showing it, we need to define the intersection of two divisors, which is done in the following.

Definition 4: 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

$$G \cap H := \sum_{P\in\mathbb{P}_F} \min\{\nu_P(G), \nu_P(H)\}P. \tag{1}$$

In addition, the union is given by

$$G \cup H := \sum_{P\in\mathbb{P}_F} \max\{\nu_P(G), \nu_P(H)\}P. \tag{2}$$

Proposition 1: [22, 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 the Section III it will be shown that when AG codes are used to construct QUENTA codes, the amount of entanglement used is equal to the dimension of the intersection of the two Riemann-Roch spaces.

For the exactly value of the dimension of a Riemann-Roch space and the construction of the dual code of a AG code, it is necessary to introduce the ideas of differential spaces and canonical divisors. $\Omega_F := \{\omega | \omega \textit{ is a Weil differential of } F/\mathbb{F}_q\}$ be the differential space of $F/\mathbb{F}_q$. Given a nonzero differential ω, we denote by $(\omega) := \sum_{P\in\mathbb{P}_F} \nu_P(\omega)P$ the canonical divisor of ω. All canonical divisors are equivalent and have degree equal to $2g - 2$. Furthermore, for a divisor G we define $\Omega_F(G) := \{\omega \in \Omega_F | \omega = 0 \textit{ or } (\omega) \geq G\}$, and its dimension as an $\mathbb{F}_q$-vector space is denoted by $i(G)$.

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: [23, Thm. 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 $\ell(G) = \deg(G) + 1 - g + \ell(W - G)$, where $\deg(G)$ is the degree of the divisor G.

Now we can define the first AG code utilized in this paper, see Definition 5, and its parameters, see Proposition 3. As can be seen, these parameters are related to the degrees of divisors, genus and number of rational places. So, with simple arithmetic we can create families of codes, even when the algebraic function field is fixed.

Definition 5: 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 $supp(G) \cap supp(D) = \varnothing$. The algebraic-geometry (AG) code $C_{\mathcal{L}}(D, G)$ associated with the divisors D and G is defined as $C_{\mathcal{L}}(D, G) := \{(x(P_1), \ldots, x(P_n)) | x \in \mathcal{L}(G)\}$.

Proposition 3: [23, Cor. 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 a $[n, k, d]$-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 $k = \deg(G) - g + 1$.

Lemma 1: Let $F/\mathbb{F}_q$ be a function field of genus g and let D be a divisor as in Definition 5. If G_1 and G_2 are two divisors such that $suppG_1 \cap suppD = \varnothing$ (resp. $suppG_2 \cap suppD = \varnothing$) 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, let the evaluation map be given by

$$ev_D(x) := (x(P_1), \ldots, x(P_n)) \in \mathbb{F}_q^n. \qquad (3)$$

So, if $c \in C_{\mathcal{L}}(D, G_1) \cap C_{\mathcal{L}}(D, G_2)$, then exist $g_1 \in \mathcal{L}(G_1)$ and $g_2 \in \mathcal{L}(G_2)$ such that $c = ev_D(g_1) = ev_D(g_2)$, which implies in $ev_D(g_1 - g_2) = 0$. Since that $g_1 - g_2 \in \mathcal{L}(G_1 \cup G_2)$ and $\deg(G_1 \cup G_2) < n$, then $f = g$ and, consequently, $c \in C_{\mathcal{L}}(D, G_1 \cap G_2)$. The other inclusion is straightforward. □

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

Definition 6: Let $F/\mathbb{F}_q$ be a function field of genus g and let G and D be divisors as in Definition 5. 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, with parameters $[n, k', d']$, where $k' = i(G - D) - i(G)$ and $d' \geq \deg(G) - (2g - 2)$.

Proposition 4: [23, Thm. 2.2.7]Let $C_{\Omega}(D, G)$ be the AG code from Definition 6. 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 5: [23, Prop. 2.2.10] Let $C_{\mathcal{L}}(D, G)$ be the AG code described in Definition 5. 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 $\eta_{P_i} = 1$ for all $i = 1, \ldots, n$, then $C_{\Omega}(D, G) = C_{\mathcal{L}}(D, D - G + (\eta))$.

It is not hard to see that the divisor of a Weil differential from Proposition 5 can be decomposed as a sum of a divisor proportional of D with one that has its support different from the support of D; i. e., $(\eta) = -D + (\eta')$, where $supp(D) \cap supp((\eta')) = \varnothing$.

B. Entanglement-assisted quantum codes

Definition 7: A quantum code $\mathcal{Q}$ is called an $[[n, k, d; c]]_q$ entanglement-assisted quantum (QUENTA) code if encodes k logical qudits into n physical qudits using c copies of maximally entangle states and can correct $\lfloor (d-1)/2 \rfloor$ quantum errors. The rate of an QUENTA code is given by k/n, relative distance by d/n, and entanglement-assisted rate by c/n. Lastly, an QUENTA code is said to have maximal entanglement when $c = n - k$.

Formulating a stabilizer paradigm for QUENTA codes gives a way to use classical codes to construct this quantum codes [24]. In particular, we have the next procedure by Wilde and Brun [8].

Proposition 6: [8, Corollary 1] Let H_1 and H_2 be parity check matrices of two linear codes with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$, respectively. Then there is an QUENTA code with parameters $[[n, k_1 + k_2 - n + c, \min\{d_1, d_2\}; c]]_q$ that requires $c = \mathrm{rank}(\mathrm{H_1 H_2^T})$ maximally entangled states.

A measurement of goodness for an QUENTA code is the quantum Singleton bound. Let $[[n, k, d; c]]_q$ be an QUENTA code, then the quantum Singleton bound is given by $d \leq \frac{n-k+c}{2} + 1$. The difference between d and the Singleton bound is called Singleton defect. When the Singleton defect is equal to zero (resp. one) the code is called maximum distance separable code (resp. almost maximum distance separable code) and it is denoted MDS code (resp. almost MDS code).

III. New Construction Method for QUENTA Codes

Proposition 6 shows a connection between the entanglement in an QUENTA code and the rank of a matrix, which is the product of parity check matrices of the classical codes utilized to construct such a quantum code. However, such rank can be difficult to calculate in some cases. As it will be shown in Theorem 2, it is possible to, instead of calculating such rank, relate the entanglement with the relative hull between the two classical codes.

Lemma 2: Let C_1 and C_2 be $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ linear codes with parity-check matrices H_1 and H_2, respectively. If $\dim(hull(C_1, C_2)) = l_1$ and $\dim(hull(C_2, C_1)) = l_2$, then $\mathrm{rank}(H_1 H_2^T) = n - \max\{k_1 + l_1, k_2 + l_2\}$.

Observe that for the result in Lemma 2 it was not needed to make any previous consideration. So, the previous result can be seen as a new way to calculate the amount of entanglement used in an QUENTA code.

If the relative hull of a code with respect to other is known, then Lemma 2 can be used instead of Proposition 6 to construct new QUENTA codes in a more direct way. We show in the following that this is the case when considering classical AG codes.

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. If $l_1 = \dim(hull(C_1, C_2))$ and $l_2 = \dim(hull(C_2, C_1))$, with $k_1 + l_1 \geq k_2 + l_2$, then there is an $[[n, k_2 - l_1, \min\{d_1, d_2\}; n - k_1 - l_1]]_q$ QUENTA code.

Proof: From Proposition 6 we have that there exists an QUENTA code with the parameters $[[n, k_1 + k_2 - n + c, \min\{d_1, d_2\}; c]]_q$, where $c = \mathrm{rank}(H_1 H_2^T)$. Since that $\mathrm{rank}(H_1 H_2^T) = n - \max\{k_1 + l_1, k_2 + l_2\}$ by Lemma 2, and by hypothesis we have $k_1 + l_1 \geq k_2 + l_2$, then the parameters of the QUENTA code can be described as $[[n, k_2 - l_1, \min\{d_1, d_2\}; n - k_1 - l_1]]_q$. □

Corollary 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

$hull(C_1, C_2) = \{\mathbf{0}\}$. Then there is an QUENTA code with parameters $[[n, k_2, \min\{d_1, d_2\}; n - k_1]]_q$.

Corollary 2: Let C be a MDS LCD code with parameters $[n, k, d]_q$. Then there is a MDS maximal entanglement QUENTA code with parameters $[[n, k, d; n - k]]_q$.

It is shown in Corollary 2 that for any MDS LCD code in the literature we can construct an QUENTA code that is, simultaneously, MDS and has maximal entanglement.

For AG codes, the property needed in Corollary 1 can be translated to a relation between the divisors used to construct them. The following theorem presents this description and a more general result.

Theorem 2: Let $C_{\mathcal{L}}(D, G_1)$ and $C_{\mathcal{L}}(D, G_2)$ be two AG codes over $\mathbb{F}_q$ derived from divisors D, $G_1 = \sum_{j=1}^{t} a_j Q_j$, and $G_2 = \sum_{j=1}^{t} b_j Q_j$, which follow the construction of Definition 5 with $\deg Q_j = 1$, for $j = 1, \ldots, t$, and $\sum_{j=1}^{t} \max\{a_j, b_j\} < n$. Consider, without loss of generality, that $l_1 + \sum_j a_j \geq l_2 + \sum_j b_j$, where $l_1 = hull(C_1, C_2)$ and $l_2 = hull(C_2, C_1)$. Additionally, assume that the Weil differential η has divisor $(\eta) = -D + (\eta')$. Then, for $\sum_{j=1}^{t} \min\{b_j, \nu_{Q_j}(\eta') - a_j\} \geq 0$ there exists an QUENTA code with parameters $[[n, k, d; c]]_q$, where

$$k = \sum_{j=1}^{t} b_j - \ell\Big(\sum_{j=1}^{t} \min\{b_j, \nu_{Q_j}(\eta') - a_j\} Q_j\Big) - g + 1,$$

$$d = n - \max\Big\{\sum_{j=1}^{t} a_j, \sum_{j=1}^{t} b_j\Big\},$$

and

$$c = n + g - \sum_{j=1}^{t} a_j - \ell\Big(\sum_{j=1}^{t} \min\{b_j, \nu_{Q_j}(\eta') - a_j\} Q_j\Big) - 1.$$

On the other hand, for $\sum_{j=1}^{t} \min\{b_j, \nu_{Q_j}(\eta') - a_j\} < 0$ there exists an QUENTA code with parameters

$$[[n, \sum_j b_j - g + 1, n - \max\{\sum_j a_j, \sum_j b_j\}; n - \sum_j a_j - g + 1]]_q. \tag{4}$$

Proof: From Proposition 5, one has that $C_{\mathcal{L}}^{\perp}(D, G_1) = C_{\mathcal{L}}(D, D - G_1 + (\eta))$, where $(\eta) = -D + (\eta')$ with $supp(D) \cap supp((\eta')) = \varnothing$. Using Lemma 1 we get that $hull(C_{\mathcal{L}}(D, G_1), C_{\mathcal{L}}(D, G_2)) = C_{\mathcal{L}}(D, \sum_{j=1}^{t} \min\{b_j, \nu_{Q_j}(\eta') - a_j\} Q_j)$. Thus, it follows that $l_1 = \ell(\min\{b_j, \nu_{Q_j}(\eta') - a_j\} Q_j)$ if $\min\{b_j, \nu_{Q_j}(\eta') - a_j\} \geq 0$; otherwise $l_1 = 0$. The remaining statements follow from Theorem 1. □

The following theorem shows a construction of QUENTA codes derived from Hermitian function field. Next, Elliptic function field will be used to obtain maximal entanglement QUENTA codes with Singleton defect at most one.

Theorem 3: Let q be a power of a prime and a_1, a_2, b_1, b_2 be positive integers such that $b_1 \leq a_1$, $b_2 \leq a_2$, and $q(q - 1) - 1 \leq b_1 + b_2 \leq a_1 + a_2 < q^3 - 1$. In addition, it is adopted $a_1 > \min\{b_2, q^3 + q(q - 1) - 3 - a_2\}$. Then there exists an QUENTA code with parameters $[[q^3 - 1, b_1 + b_2 - q(q-1)/2 + 1, q^3 - 1 - a_1 - a_2; q^3 - 1 - a_1 - a_2 + q(q - 1)/2 - 1]]_{q^2}$.

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 $q(q-1)/2$. Adopt $D = P_1 + \cdots + P_{q^3-1}$, $G_1 = a_1 P_{q^3} + a_2 P_{\infty}$, and $G_2 = b_1 P_{q^3} + b_2 P_{\infty}$, where P_{∞} is the place at infinity. So, one possible Weil differential satisfying Proposition 5 has divisor $(\eta) = -D + (q^3 - 1 + 2g - 2) P_{\infty}$. Since that $a_1 > \min\{b_2, q^3 + q(q - 1) - 3 - a_2\}$, we have that $l_1 = 0$. Thus, applying Theorem 2, then there is an QUENTA codes with the parameters mentioned. □

Some examples of QUENTA codes created via Theorem 3 are $[[7, 3, 3; 3]]_4$, $[[26, 12, 10; 8]]_9$, and $[[63, 40, 18; 13]]_{16}$.

Theorem 4: Let $F/\mathbb{F}_q$ be an Elliptic function field with $n+2$ rational points. Let a_1, a_2, b_1, b_2 be positive integers such that $b_1 \leq a_1$, $b_2 \leq a_2$, and $1 \leq b_1 + b_2 \leq a_1 + a_2 < n$. In addition, it is adopted $a_1 > \min\{b_2, n - a_1\}$. Then there exists an QUENTA code with parameters $[[n, b_1 + b_2, n - a_1 - a_2; n - a_1 - a_2]]_q$. In particular, if $a_1 = b_1$ and $a_2 = b_2$, then there is a almost MDS maximal entanglement QUENTA code with parameters $[[n, a_1 + a_2, n - a_1 - a_2; n - a_1 - a_2]]_q$.

Proof: It follows the same construction as in the proof of Theorem 3 with observing that the genus of an Elliptic function field is equal to one. □

Using the Theorem 4, we can create almost MDS maximal entanglement QUENTA codes with parameters $[[7, 4, 3; 3]]_4$, $[[12, 7, 5; 5]]_8$, and $[[39, 25, 14; 14]]_{32}$.

IV. Asymptotically Good Maximal Entanglement QUENTA Codes

In this section, we show that from any family of (classical) asymptotically good AG codes, we can construct a family of asymptotically good maximal entanglement QUENTA codes. This is a consequence of the use of the result from Carlet, *et al.* [19] applied to the Corollary 1. Before showing it, we need to define the concept of (classical) asymptotically good codes.

Definition 8: 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_t, with parameters $[n_t, k_t, d_t]_q$, such that $n_t \to \infty$ as $t \to \infty$ and $\delta = \lim_{t\to\infty} d_t/n_t$, $R = \lim_{t\to\infty} k_t/n_t$. If $\delta, R > 0$, then the family is called asymptotically good.

Proposition 7: [19, Corollary 5.5] Let $q \geq 3$ 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. Then there exists a family of LCD codes with

$$\alpha_q^{LCD}(\delta) \geq 1 - \delta - \frac{1}{A(q)}, \text{ for } \delta \in [0, 1 - 1/A(q)]. \tag{5}$$

Theorem 5: Let $q \geq 3$ be a power of a prime and $A(q)$ as defined in Proposition 7. Then there exists a family of asymptotically good maximal entanglement QUENTA codes 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 $\delta \in [0, 1 - 1/A(q)]$.

Proof: Let $\mathcal{C} = \{C_1, C_2, \ldots\}$ be a family of LCD codes as the ones in Proposition 7, where each C_i has parameters $[n_i, k_i, d_i]_q$. If we apply the family $\mathcal{C}$ to construct QUENTA codes, it follows from Corollary 1 that we can construct maximal entanglement QUENTA codes with parameters $[[n_t, k_t, d_t; c_t]]_q$, such that

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

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 that the families in Proposition 7 are asymptotically good, the result follows. □

Remark 1: In a recent paper, Galindo, *et al.* [25] derived the quantum Gilbert-Varschamov bound for QUENTA codes. Using the previous theorem, we can show that exists a family of QUENTA codes with parameters that exceed the mentioned bound.

V. Conclusion

This paper has been devoted to the use of AG codes in the construction of QUENTA codes. We firstly showed that the intersection of two AG codes is also an AG code. This was used in a new description of how to compute the entanglement in an QUENTA code. As a consequence, we constructed two new families of QUENTA codes where one of them is almost MDS. Lastly, it was shown that for any asymptotically good classical family of AG codes, there is a family asymptotically good maximal entanglement QUENTA codes. It is worth mentioning that all the results presented in this paper can be applied to any algebraic function field.

Acknowledgment

This research has been partially supported by the Brazilian Agencies CAPES and CNPq.

References

[1] M. M. Wilde, M.-H. Hsieh, and Z. Babar, "Entanglement-assisted quantum turbo codes," *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 1203–1222, Feb. 2014.

[2] C.-Y. Lai, T. A. Brun, and M. M. Wilde, "Dualities and identities for entanglement-assisted quantum codes," *Quantum Information Processing*, vol. 13, no. 4, pp. 957–990, Apr. 2014.

[3] R. Li, L. Guo, and Z. Xu, "Entanglement-assisted quantum codes achieving the quantum singleton bound but violating the quantum hamming bound," *Quantum Information & Computation*, vol. 14, no. 13, pp. 1107–1116, Oct. 2014.

[4] G. Bowen, "Entanglement required in achieving entanglement-assisted channel capacities," *Physical Review A*, vol. 66, pp. 052 313–1–052 313–8, Nov. 2002.

[5] D. Fattal, T. S. Cubitt, Y. Yamamoto, S. Bravyi, and I. L. Chuang, "Entanglement in the stabilizer formalism," Jun. 2004.

[6] T. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, Oct. 2006.

[7] D. A. Lidar and T. A. Brun, Eds., *Quantum Error Correction*. Cambridge University Press, 2013.

[8] M. M. Wilde and T. A. Brun, "Optimal entanglement formulas for entanglement-assisted quantum coding," *Physical Review A*, vol. 77, no. 6, pp. 064 302–1–064 302–4, Jun. 2008.

[9] J. Chen, Y. Huang, C. Feng, and R. Chen, "Entanglement-assisted quantum MDS codes constructed from negacyclic codes," *Quantum Information Processing*, vol. 16, no. 12, p. 303, Nov. 2017.

[10] L. Lu, R. Li, and L. Guo, "Entanglement-assisted quantum codes from quaternary codes of dimension five," *International Journal of Quantum Information*, vol. 15, no. 3, p. 1750017, April 2017.

[11] K. Guenda, S. Jitman, and T. A. Gulliver, "Constructions of good entanglement-assisted quantum error correcting codes," *Designs, Codes and Cryptography*, vol. 86, no. 1, pp. 121–136, Jan. 2018.

[12] X. Liu, L. Yu, and P. Hu, "New entanglement-assisted quantum codes from k-Galois dual codes," *Finite Fields and Their Applications*, vol. 55, pp. 21–32, Jan. 2019.

[13] J. Fan, H. Chen, and J. Xu, "Constructions of q-ary entanglement-assisted quantum MDS codes with minimum distance greater than $q+1$," *Quantum Information and Computation*, vol. 16, no. 5&6, pp. 423–434, 2016.

[14] L. Lu, W. Ma, R. Li, Y. Ma, Y. Liu, and H. Cao, "Entanglement-assisted quantum MDS codes from constacyclic codes with large minimum distance," *Finite Fields and Their Applications*, vol. 53, pp. 309–325, Sep. 2018.

[15] X. Chen, S. Zhu, and X. Kai, "Entanglement-assisted quantum MDS codes constructed from constacyclic codes," *Quantum Information Processing*, vol. 17, no. 10, p. 273, Oct. 2018.

[16] X. Liu, H. Liu, and L. Yu, "Entanglement-assisted quantum codes from Galois LCD codes," Sep. 2018.

[17] K. Guenda, T. A. Gulliver, S. Jitman, and S. Thipworawimon, "Linear ℓ-intersection pairs of codes and their applications," Oct. 2018.

[18] V. D. Goppa, "Codes on algebraic curves," *Soviet Mathematics Doklady*, vol. 22, no. 1, pp. 170–172, 1981.

[19] C. Carlet, S. Mesnager, C. Tang, Y. Qi, and R. Pellikaan, "Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$," *IEEE Transactions on Information Theory*, vol. 64, no. 4, pp. 3010–3017, Apr. 2018.

[20] I. Devetak, A. W. Harrow, and A. J. Winter, "A resource framework for quantum Shannon theory," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4587–4618, Oct. 2008.

[21] L. Lu, R. Li, L. Guo, and Q. Fu, "Maximal entanglement entanglement-assisted quantum codes constructed from linear codes," *Quantum Information Processing*, vol. 14, no. 1, pp. 165–182, Jan. 2015.

[22] C. Munuera and R. Pellikaan, "Equality of geometric Goppa codes and equivalence of divisors," *Journal of Pure and Applied Algebra*, vol. 90, no. 3, pp. 229–252, Dec. 1993.

[23] H. Stichtenoth, *Algebraic Function Fields and Codes*. Springer, 2009.

[24] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Catalytic quantum error correction," *IEEE Transactions on Information Theory*, vol. 60, no. 6, pp. 3073–3089, Jun. 2014.

[25] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano, "Entanglement-assisted quantum error-correcting codes over arbitrary finite fields," *Quantum Information Processing*, vol. 18, no. 4, p. 116, Apr. 2019.