

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

Francisco Revson F. Pereira

joint work with Ruud Pellikaan, Giuliano La Guardia, and Francisco M. de Assis

TU/e, the Netherlands

IEEE International Symposium on Information Theory

July 12, 2019

# Content

Motivations

Algebraic Geometry Codes

New QUENTA codes

Asymptotically Good QUENTA codes

# CSS Construction Method<sup>1</sup>

## Proposition

Let  $C_1$  and  $C_2$  denote two classical linear codes with parameters  $[n, k_1, d_1]_q$  and  $[n, k_2, d_2]_q$ , respectively, such that  $C_2^\perp \subseteq C_1$ . Then there exists a  $[[n, k_1 + k_2 - n, d]]_q$  quantum error-correction code with minimum distance  $d \geq \min\{d_1, d_2\}$ .

---

<sup>1</sup>Nielsen, Michael A.; Chuang, Isaac L. (2010). Quantum Computation and Quantum Information (2nd ed.). Cambridge: Cambridge University Press

# CSS Construction Method<sup>1</sup>

## Proposition

Let  $C_1$  and  $C_2$  denote two classical linear codes with parameters  $[n, k_1, d_1]_q$  and  $[n, k_2, d_2]_q$ , respectively, such that  $C_2^\perp \subseteq C_1$ . Then there exists a  $[[n, k_1 + k_2 - n, d]]_q$  quantum error-correction code with minimum distance  $d \geq \min\{d_1, d_2\}$ .

- ▶ **Constraint:** One of the codes needs to be contained

---

<sup>1</sup>Nielsen, Michael A.; Chuang, Isaac L. (2010). Quantum Computation and Quantum Information (2nd ed.). Cambridge: Cambridge University Press

# CSS Construction Method<sup>1</sup>

## Proposition

Let  $C_1$  and  $C_2$  denote two classical linear codes with parameters  $[n, k_1, d_1]_q$  and  $[n, k_2, d_2]_q$ , respectively, such that  $C_2^\perp \subseteq C_1$ . Then there exists a  $[[n, k_1 + k_2 - n, d]]_q$  quantum error-correction code with minimum distance  $d \geq \min\{d_1, d_2\}$ .

- ▶ **Constraint:** One of the codes needs to be contained
- ▶ **Possible way out:** Entanglement!

---

<sup>1</sup>Nielsen, Michael A.; Chuang, Isaac L. (2010). Quantum Computation and Quantum Information (2nd ed.). Cambridge: Cambridge University Press

# Entanglement-Assisted Quantum Error Correcting Codes

- ▶ The first QUENTA code was proposed by Bowen<sup>2</sup>
- ▶ The stabilizer formalism for **qubits** QUENTA code was done by Brun *et al.*<sup>3</sup>
- ▶ It was shown that this class of codes can achieve the hashing bound<sup>4</sup> and violate the quantum Hamming bound<sup>5</sup>

---

<sup>2</sup>Bowen, G.: Entanglement required in achieving entanglement-assisted channel capacities. *Physical Review A* 66, 052313–1–052313–8 (2006)

<sup>3</sup>Brun, T., Devetak, I., Hsieh, M.H.: Correcting quantum errors with entanglement. *Science* 314(5798), 436–439 (2006)

<sup>4</sup>Wilde, M.M., Hsieh, M.H., Babar, Z.: Entanglement-assisted quantum turbo codes. *IEEE Transactions on Information Theory* 60(2), 1203–1222 (2014)

<sup>5</sup>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 (2014)

# Entanglement-Assisted Quantum Error Correcting Codes

- ▶ Recent research focus on constacyclic and negacyclic codes<sup>6 7</sup>  
8 9

---

<sup>6</sup>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)

<sup>7</sup>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 (2018)

<sup>8</sup>Chen, J., Huang, Y., Feng, C., Chen, R.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. *Quantum Information Processing* 16(12), 303 (2017)

<sup>9</sup>Lu, L., Li, R., Guo, L., Ma, Y., Liu, Y.: Entanglement-assisted quantum MDS codes from negacyclic codes. *Quantum Information Processing* 17(3), 69 (2018)

# Entanglement-Assisted Quantum Error Correcting Codes

- ▶ Recent research focus on constacyclic and negacyclic codes<sup>6 7</sup>  
8 9

What about codes with larger length?

---

<sup>6</sup>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)

<sup>7</sup>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 (2018)

<sup>8</sup>Chen, J., Huang, Y., Feng, C., Chen, R.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. *Quantum Information Processing* 16(12), 303 (2017)

<sup>9</sup>Lu, L., Li, R., Guo, L., Ma, Y., Liu, Y.: Entanglement-assisted quantum MDS codes from negacyclic codes. *Quantum Information Processing* 17(3), 69 (2018)



# Entanglement-Assisted Quantum Error Correcting Codes

- ▶ Recent research focus on constacyclic and negacyclic codes<sup>6 7 8 9</sup>

What about codes with larger length? and

Is there asymptotically good QUENTA codes?

---

<sup>6</sup>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)

<sup>7</sup>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 (2018)

<sup>8</sup>Chen, J., Huang, Y., Feng, C., Chen, R.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. *Quantum Information Processing* 16(12), 303 (2017)

<sup>9</sup>Lu, L., Li, R., Guo, L., Ma, Y., Liu, Y.: Entanglement-assisted quantum MDS codes from negacyclic codes. *Quantum Information Processing* 17(3), 69 (2018)

# Content

Motivations

Algebraic Geometry Codes

New QUENTA codes

Asymptotically Good QUENTA codes

## Some Notations

- ▶ Let  $F/\mathbb{F}_q$  be an algebraic function field over  $\mathbb{F}_q$  with genus  $g$

## Some Notations

- ▶ Let  $F/\mathbb{F}_q$  be an algebraic function field over  $\mathbb{F}_q$  with genus  $g$
- ▶ Let  $P_0, P_1, \dots, P_n, P_\infty$  be pairwise distinct rational places of  $F/\mathbb{F}_q$  and  $D = P_1 + \dots + P_n$

## Some Notations

- ▶ Let  $F/\mathbb{F}_q$  be an algebraic function field over  $\mathbb{F}_q$  with genus  $g$
- ▶ Let  $P_0, P_1, \dots, P_n, P_\infty$  be pairwise distinct rational places of  $F/\mathbb{F}_q$  and  $D = P_1 + \dots + P_n$
- ▶ Let  $G, G_1, G_2$  be divisors of  $F/\mathbb{F}_q$  such that
  - ▶  $\text{supp}G \cap \text{supp}D = \emptyset$  and  $\text{supp}G_i \cap \text{supp}D = \emptyset$ , for  $i = 1, 2$
  - ▶  $2g - 2 < \deg(G), \deg(G_1), \deg(G_2) < n$

## Some Notations

- ▶ Let  $F/\mathbb{F}_q$  be an algebraic function field over  $\mathbb{F}_q$  with genus  $g$
- ▶ Let  $P_0, P_1, \dots, P_n, P_\infty$  be pairwise distinct rational places of  $F/\mathbb{F}_q$  and  $D = P_1 + \dots + P_n$
- ▶ Let  $G, G_1, G_2$  be divisors of  $F/\mathbb{F}_q$  such that
  - ▶  $\text{supp}G \cap \text{supp}D = \emptyset$  and  $\text{supp}G_i \cap \text{supp}D = \emptyset$ , for  $i = 1, 2$
  - ▶  $2g - 2 < \deg(G), \deg(G_1), \deg(G_2) < n$
- ▶ And the Riemann-Roch space associated with  $G$  is given by

$$\mathcal{L}(G) = \{x \in F/\mathbb{F}_q \mid (x) \geq -G\} \cup \{0\},$$

where  $\ell(G)$  denotes its dimension

# Algebraic Geometry Codes

## Definition of $C_{\mathcal{L}}(D, G)$

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  $ev_D: \mathcal{L}(G) \rightarrow \mathbb{F}_q^n$  called evaluation map, where  $ev_D(f) = (f(P_1), \dots, f(P_n))$ ; i.e.,  $C_{\mathcal{L}}(D, G) = \{(f(P_1), \dots, f(P_n)) | f \in \mathcal{L}(G)\}$ .

# Algebraic Geometry Codes

## Definition of $C_{\mathcal{L}}(D, G)$

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  $ev_D: \mathcal{L}(G) \rightarrow \mathbb{F}_q^n$  called evaluation map, where  $ev_D(f) = (f(P_1), \dots, f(P_n))$ ; i.e.,  $C_{\mathcal{L}}(D, G) = \{(f(P_1), \dots, f(P_n)) \mid f \in \mathcal{L}(G)\}$ .

- ▶  $C_{\mathcal{L}}(D, G)$  is a linear  $[n, k, d]_q$  with parameters

$$k = \deg(G) - g + 1 \text{ and } d \geq n - \deg(G).$$



# New from Old (Preliminary)

## Definition

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

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

In addition, the union is given by

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

## Proposition<sup>10</sup>

Let  $G$  and  $H$  be divisors over  $F/\mathbb{F}_q$ . Then  $\mathcal{L}(G) \cap \mathcal{L}(H) = \mathcal{L}(G \cap H)$ .

---

<sup>10</sup>Munuera, C., Pellikaan, R.: Equality of geometric Goppa codes and equivalence of divisors. Journal of Pure and Applied Algebra (1993)

# New from Old

## Theorem

Let  $F/\mathbb{F}_q$  be a function field of genus  $g$ . If  $G_1$  and  $G_2$  are two divisors such that  $\deg(G_1 \cup G_2) < n$ , then  $C_{\mathcal{L}}(D, G_1) \cap C_{\mathcal{L}}(D, G_2) = C_{\mathcal{L}}(D, G_1 \cap G_2)$ .

# New from Old

## Theorem

Let  $F/\mathbb{F}_q$  be a function field of genus  $g$ . If  $G_1$  and  $G_2$  are two divisors such that  $\deg(G_1 \cup G_2) < n$ , then  $C_{\mathcal{L}}(D, G_1) \cap C_{\mathcal{L}}(D, G_2) = C_{\mathcal{L}}(D, G_1 \cap G_2)$ .

## Sketch of the Proof

( $\Rightarrow$ ) Let  $c \in C_{\mathcal{L}}(D, G_1) \cap C_{\mathcal{L}}(D, G_2)$ , 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  $g_1 = g_2$  and, consequently,  $c \in C_{\mathcal{L}}(D, G_1 \cap G_2)$

( $\Leftarrow$ ) This is a straightforward consequence of Munuera and Pellikaan's Proposition

# Algebraic Geometry Codes

## Definition of $C_{\mathcal{L}}(D, G)^{\perp}$

The Euclidean dual of the (AG) code  $C_{\mathcal{L}}(D, G)$  is given by  $C_{\mathcal{L}}(D, G)^{\perp} = C_{\mathcal{L}}(D, G^{\perp})$ , where  $G^{\perp} = D - G + (\eta)$ , and  $\eta$  is a Weil differential such that  $\nu_{P_i}(\eta) = -1$  and  $\eta_{P_i}(1) = 1$  for all  $i = 1, \dots, n$ .

# Algebraic Geometry Codes

## Definition of $C_{\mathcal{L}}(D, G)^{\perp}$

The Euclidean dual of the (AG) code  $C_{\mathcal{L}}(D, G)$  is given by  $C_{\mathcal{L}}(D, G)^{\perp} = C_{\mathcal{L}}(D, G^{\perp})$ , where  $G^{\perp} = D - G + (\eta)$ , and  $\eta$  is a Weil differential such that  $\nu_{P_i}(\eta) = -1$  and  $\eta_{P_i}(1) = 1$  for all  $i = 1, \dots, n$ .

- ▶  $C_{\mathcal{L}}(D, G)^{\perp}$  is a linear  $[n, k', d']_q$  with parameters

$$k' = n + g - 1 - \deg(G) \text{ and } d' \geq \deg(G) - (2g - 2).$$

# Content

Motivations

Algebraic Geometry Codes

**New QUENTA codes**

Asymptotically Good QUENTA codes

# Euclidean Construction Method

## Proposition<sup>11</sup>

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 QUENTA code with parameters  $[[n, k_1 + k_2 - n + c, d; c]]_q$ , where  $d \geq \min\{d_1, d_2\}$ , and

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

is the number of required maximally entangled states.

---

<sup>11</sup>Galindo, C., Hernando, F., Matsumoto, R., Ruano, D.: Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. Quantum Information Processing 18(116), 1–18 (2019)

# Euclidean Construction Method

## Proposition<sup>11</sup>

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 QUENTA code with parameters  $[[n, k_1 + k_2 - n + c, d; c]]_q$ , where  $d \geq \min\{d_1, d_2\}$ , and

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

is the number of required maximally entangled states.

An QUENTA code is

- ▶ MDS if  $d = (n - k + c)/2 + 1$
- ▶ Maximal entanglement if  $c = n - k$

---

<sup>11</sup>Galindo, C., Hernando, F., Matsumoto, R., Ruano, D.: Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. Quantum Information Processing 18(116), 1–18 (2019)



# QUENTA codes derived from AG codes

## Main Theorem

Let  $F/\mathbb{F}_q$  be an algebraic function field. If  $\deg(G_1^\perp \cap G_2) < 0$ , then there is an QUENTA code with parameters  $[[n, \deg(G_2) - g + 1, d; c]]_q$ , where  $d \geq n - \max\{\deg(G_1), \deg(G_2)\}$  and  $c = n + g - 1 - \deg(G_1)$ .

# QUENTA codes derived from AG codes

## Main Theorem

Let  $F/\mathbb{F}_q$  be an algebraic function field. If  $\deg(G_1^\perp \cap G_2) < 0$ , then there is an QUENTA code with parameters  $[[n, \deg(G_2) - g + 1, d; c]]_q$ , where  $d \geq n - \max\{\deg(G_1), \deg(G_2)\}$  and  $c = n + g - 1 - \deg(G_1)$ .

## Sketch of the Proof

We have the following:

- ▶  $C_{\mathcal{L}}(D, G_i)$  has parameters  $[n, \deg(G_i) - g + 1, d_i \geq n - \deg(G_i)]_q$
- ▶ The dimension of the Euclidean dual of  $C_{\mathcal{L}}(D, G_1)$  is  $n + g - 1 - \deg(G_1)$
- ▶ Since  $\deg(G_1^\perp \cup G_2) < 0$ , then  $\dim(C_1^\perp \cap C_2) = 0$  and  $c = n - \deg(G_i) + g - 1$

# QUENTA codes derived from Hermitian AG Codes

## Theorem (Explicit Example 1)

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

# QUENTA codes derived from Hermitian AG Codes

## Theorem (Explicit Example 1)

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

Some examples of parameters:

$[[7, 3, 3; 3]]_4$ ,  $[[26, 12, 10; 8]]_9$ , and  $[[63, 40, 18; 13]]_{16}$

# QUENTA codes derived from Hermitian AG Codes

## Sketch of the Proof

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

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

- ▶ It has  $1 + q^3$  rational points and genus  $q(q-1)/2$
- ▶  $G_1 = a_1P_0 + a_2P_\infty$ , and  $G_2 = b_1P_0 + b_2P_\infty$
- ▶ As a Weil differential, consider  $\eta = \frac{1}{x^{q^2-x}}dx$ , which has divisor  $(\eta) = -D - P_0 + (q^3 + 2g - 2)P_\infty$

# QUENTA codes derived from Hermitian AG Codes

## Sketch of the Proof

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

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

- ▶ It has  $1 + q^3$  rational points and genus  $q(q-1)/2$
- ▶  $G_1 = a_1P_0 + a_2P_\infty$ , and  $G_2 = b_1P_0 + b_2P_\infty$
- ▶ As a Weil differential, consider  $\eta = \frac{1}{x^{q^2-x}}dx$ , which has divisor  $(\eta) = -D - P_0 + (q^3 + 2g - 2)P_\infty$
- ▶ Since  $a_1 > \min\{b_2, q^3 + q(q-1) - 3 - a_2\}$ , we have that  $C_{\mathcal{L}}(D, G_1)$  and  $C_{\mathcal{L}}(D, G_2)$  are LCD
- ▶ Thus,  $c = n - k_1 = q^3 - 1 - a_1 - a_2 + q(q-1)/2 - 1$  and the result follows

# QUENTA codes derived from Elliptic AG Codes

## Theorem (Explicit Example 2)

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  $[[n, b_1 + b_2, n - a_1 - a_2; n - a_1 - a_2]]_q$ .

# QUENTA codes derived from Elliptic AG Codes

## Theorem (Explicit Example 2)

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  $[[n, b_1 + b_2, n - a_1 - a_2; n - a_1 - a_2]]_q$ .

For  $a_1 = b_1$  and  $a_2 = b_2$ , the QUENTA code created is **almost MDS** and **maximal entanglement**



# QUENTA codes derived from Elliptic AG Codes

## Theorem (Explicit Example 2)

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  $[[n, b_1 + b_2, n - a_1 - a_2; n - a_1 - a_2]]_q$ .

For  $a_1 = b_1$  and  $a_2 = b_2$ , the QUENTA code created is **almost MDS** and **maximal entanglement**

Some examples of parameters:

$[[7, 4, 3; 3]]_4$ ,  $[[12, 7, 5; 5]]_8$ , and  $[[39, 25, 14; 14]]_{32}$

# QUENTA codes derived from Elliptic AG Codes

## Sketch of the Proof

- ▶  $F/\mathbb{F}_q$  be the elliptic function field with  $e$  rational points and genus  $g = 1$  defined by the equation

$$y^2 + y = x^3 + bx + c,$$

- ▶ Assume that  $G_1 = a_1P_0 + a_2P_\infty$  and  $G_2 = b_1P_0 + b_2P_\infty$
- ▶ Let  $\eta = \frac{dx}{\prod_{\alpha_j \in S}(x + \alpha_j)}$ , then  $(\eta) = (e - 1)P_\infty - P_{\alpha_0} - D$

# QUENTA codes derived from Elliptic AG Codes

## Sketch of the Proof

- ▶  $F/\mathbb{F}_q$  be the elliptic function field with  $e$  rational points and genus  $g = 1$  defined by the equation

$$y^2 + y = x^3 + bx + c,$$

- ▶ Assume that  $G_1 = a_1P_0 + a_2P_\infty$  and  $G_2 = b_1P_0 + b_2P_\infty$
- ▶ Let  $\eta = \frac{dx}{\prod_{\alpha_i \in S}(x + \alpha_i)}$ , then  $(\eta) = (e - 1)P_\infty - P_{\alpha_0} - D$
- ▶ From  $a_1 > \min\{b_2, n - a_1\}$ , we have that  $C_{\mathcal{L}}(D, G_1)$  and  $C_{\mathcal{L}}(D, G_2)$  are LCD
- ▶ Thus,  $c = n - k_1 = n - a_1 - a_2$  and the result follows

# Content

Motivations

Algebraic Geometry Codes

New QUENTA codes

Asymptotically Good QUENTA codes

# Preliminary

## Definition

Let  $q$  be a prime power. A family of indexed linear codes  $C_i$ , with parameters  $[n_i, k_i, d_i]_q$ , such that  $n_i \rightarrow \infty$  as  $i \rightarrow \infty$ , is called asymptotically good if  $\delta = \lim_{i \rightarrow \infty} d_i/n_i > 0$  and  $R = \lim_{i \rightarrow \infty} k_i/n_i > 0$

# Asymptotically Good QUINTA Codes

## Theorem

Let  $q \geq 3$  be a power of a prime and  $A(q) = \limsup_{g \rightarrow \infty} \frac{N_q(g)}{g}$ . Then there exists a family of asymptotically good maximal entanglement QUINTA codes with parameters  $[[n_t, k_t, d_t; c_t]]_q$ , such that

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

and

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

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

# Asymptotically Good QUENTA Codes

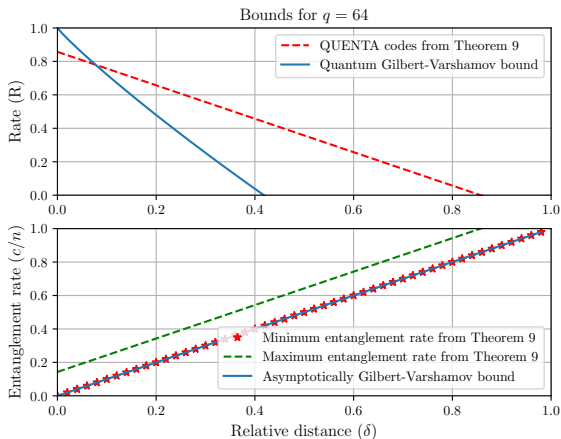
## Sketch of the Proof

- ▶ From Carlet, *et al.*<sup>12</sup>, there is a asymptotically good family of LCD codes
- ▶ Using such family and the result presented, there is a family of asymptotically good QUENTA code
- ▶ Since the classical codes are LCD, the family of QUENTA codes is also maximal entanglement

---

<sup>12</sup>Carlet, C., Mesnager, S., Tang, C., Qi, Y., Pellikaan, R.: Linear codes over  $F_q$  are equivalent to LCD codes for  $q > 3$ . *IEEE Transactions on Information Theory* 64(4), 3010–3017 (2018)

# Comparison between asymptotically QUENTA codes and quantum GV bound<sup>13</sup>



<sup>13</sup>Galindo, C., Hernando, F., Matsumoto, R., Ruano, D.: Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. Quantum Information Processing 18(116), 1–18 (2019)



Thanks for your attention!

Any questions?

# Communication scheme using an QUENTA code

