Entanglement-Assisted Quantum Codes from Algebraic Geometry Codes

Francisco Revson F. Pereira

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

TU/e, the Netherlands, and UFCG, Brazil

WCC 2019

April 5, 2019

Content

CSS Construction Method[1]

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 $d \geq \min\{d_1, d_2\}$.

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

CSS Construction Method[1]

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

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

CSS Construction Method[1]

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!

[1] 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[2]
- The stabilizer formalism for qubits QUENTA code was done by Brun *et al.*[3]
- It was shown that this class of codes can achieve the hashing bound[4] and violate the quantum Hamming bound[5]

---

[2] Bowen, G.: Entanglement required in achieving entanglement-assisted channel capacities. Physical Review A 66, 052313–1-052313–8 (2006)

[3] Brun, T., Devetak, I., Hsieh, M.H.: Correcting quantum errors with entanglement. Science 314(5798), 436–439 (2006)

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

[5] 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[6] [7] [8] [9]

[6] 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)

[7] 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)

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

[9] 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[6] [7] [8] [9]
- What about codes with lengths that are proportional to a higher power of the finite field?

---

[6] 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)

[7] 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)

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

[9] 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[6] [7] [8] [9]
- What about codes with lengths that are proportional to a higher power of the finite field? Algebraic Geometry Codes

[6] 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)

[7] 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)

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

[9] 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

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 $P_0, P_1, \ldots, P_n, P_\infty$ be pairwise distinct rational places of $F/\mathbb{F}_q$ and $D = P_1 + \cdots + P_n$

Some Notations

- Let $F/\mathbb{F}_q$ be an algebraic function field over $\mathbb{F}_q$ with genus g
- Let $P_0, P_1, \ldots, P_n, P_\infty$ be pairwise distinct rational places of $F/\mathbb{F}_q$ and $D = P_1 + \cdots + P_n$
- Let G, G_1, G_2 be divisors of $F/\mathbb{F}_q$ such that
  - $suppG \cap suppD = \varnothing$ and $suppG_i \cap suppD = \varnothing$, 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 $P_0, P_1, \ldots, P_n, P_\infty$ be pairwise distinct rational places of $F/\mathbb{F}_q$ and $D = P_1 + \cdots + P_n$
- Let G, G_1, G_2 be divisors of $F/\mathbb{F}_q$ such that
  - $suppG \cap suppD = \varnothing$ and $suppG_i \cap suppD = \varnothing$, 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

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

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

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

- $C_{\mathcal{L}}(D, G)$ 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[10]

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

[10] 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

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 η is a Weil differential such that $\nu_{P_i}(\eta) = -1$ and $\eta_{P_i}(1) = 1$ for all $i = 1, \ldots, n$.

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 η is a Weil differential such that $\nu_{P_i}(\eta) = -1$ and $\eta_{P_i}(1) = 1$ for all $i = 1, \ldots, n$.

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

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

Content

Euclidean Construction Method

Proposition[11]

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

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

is the number of required maximally entangled states.

[11] 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[11]

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

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

is the number of required maximally entangled states.

An QUENTA code is

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

[11] 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 with genus g. Assume that $C_1 = C_{\mathcal{L}}(D, G_1)$ and $C_2 = C_{\mathcal{L}}(D, G_2)$. If $\deg(G_1^{\perp} \cup G_2) < n$, then there is a QUENTA 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 $c = n + g - 1 - \deg(G_1) - \ell(G_1^{\perp} \cap G_2)$.

QUENTA codes derived from AG codes

Main Theorem

Let $F/\mathbb{F}_q$ be an algebraic function field with genus g. Assume that $C_1 = C_{\mathcal{L}}(D, G_1)$ and $C_2 = C_{\mathcal{L}}(D, G_2)$. If $\deg(G_1^{\perp} \cup G_2) < n$, then there is a QUENTA 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 $c = n + g - 1 - \deg(G_1) - \ell(G_1^{\perp} \cap G_2)$.

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 $\deg(G_1^{\perp} \cup G_2) < n$, then $\dim(C_1^{\perp} \cap C_2) = \ell(G_1^{\perp} \cap G_2)$

QUENTA codes derived from AG codes

Corollary

Let $F/\mathbb{F}_q$ be an algebraic function field. If $\deg(G_1^{\perp} \cup G_2) < n$ and $\deg(G_1^{\perp} \cap G_2) < 0$, 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 $c = n + g - 1 - \deg(G_1)$. In particular, if it is possible to have $G_1 = G_2 = G$, then the QUENTA code has parameters $[[n, \deg(G) - g + 1, n - \deg(G); n + g - 1 - \deg(G)]]_q$.

Content

QUENTA codes derived from Rational AG Codes

Theorem (Explicit Example 1)

Let q be a power of a prime. So, if a_1, a_2, b_1, b_2 are 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 is a QUENTA code with parameters

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

- If $b_2 < a_1 + 1$, then there is a QUENTA code with parameters

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

QUENTA codes derived from Rational AG Codes

Sketch of the Proof

- Let $\mathbb{F}_q(z)/\mathbb{F}_q$ be the rational function field
- Assume that $G_1 = a_1 P_0 + a_2 P_\infty$ and $G_2 = b_1 P_0 + b_2 P_\infty$
- Consider the Weil differential $\eta = \frac{1}{x^q - x} dx$, which has divisor $(\eta) = (q-2)P_\infty - P_0 - D$

QUENTA codes derived from Rational AG Codes

Sketch of the Proof

- Let $\mathbb{F}_q(z)/\mathbb{F}_q$ be the rational function field
- Assume that $G_1 = a_1 P_0 + a_2 P_\infty$ and $G_2 = b_1 P_0 + b_2 P_\infty$
- Consider the Weil differential $\eta = \frac{1}{x^q - x} dx$, which has divisor $(\eta) = (q-2)P_\infty - P_0 - D$
- Since that $b_2 \leq q - 2 - a_2$, then $\deg(G_1^\perp \cup G_2) = b_1 + q - 2 - a_2 < q - 1$
- By the hypothesis $b_1 \leq a_2$, we can use the main theorem and $G_1^\perp \cap G_2 = (-1 - a_1)P_0 + b_2 P_\infty$
- For $b_2 \geq a_1 + 1$ we have that $c = q - 1 - 1 - (a_1 + a_2) - (b_2 - a_1) = q - 2 - (a_2 + b_2)$

QUENTA codes derived from Rational AG Codes

Corollary

If $a_1 \leq a_2 \leq \lfloor \frac{q-2}{2} \rfloor$, then there is an MDS maximal entanglement QUENTA code with parameters $[[q-1, 2a_1+1, q-1-(a_1+a_2); q-2-2a_2]]_q$.

Content

QUENTA codes derived from Hermitian AG Codes

Theorem (Explicit Example 2)

Let q be a power of a prime and a_1, a_2, b_1, b_2 be positive integers such that $b_1 \leq a_1 - q(q-1)$, $b_2 \leq q^3 + q(q-1) - 2 - a_2$, 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 a QUENTA code with parameters

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

- If $b_2 < a_1 + 1$, then there exists a QUENTA code with parameters

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

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 $q(q-1)/2$
- $G_1 = a_1 P_0 + a_2 P_\infty$, and $G_2 = b_1 P_0 + b_2 P_\infty$
- 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 $q(q-1)/2$
- $G_1 = a_1 P_0 + a_2 P_\infty$, and $G_2 = b_1 P_0 + b_2 P_\infty$
- As a Weil differential, consider $\eta = \frac{1}{x^{q^2}-x} dx$, which has divisor $(\eta) = -D - P_0 + (q^3 + 2g - 2)P_\infty$
- $b_2 \leq q^3 + q(q-1) - 2 - a_2$ implies in $G_1^\perp \cup G_2 = b_1 P_0 + (q^3 + q(q-1) - 2 - a_2)P_\infty$
- From $b_1 \leq a_1 - q(q-1)$, we have that $\deg(G_1^\perp \cup G_2) < q^3 - q$ and we can use the main theorem
- Then the first case comes from $b_2 \geq a_1 + 1$, which implies that $\deg(G_1^\perp \cap G_2) \geq 0$ and $c = q^3 - 2 + q(q-1) - (a_2 + b_2)$

Content

QUENTA codes derived from Elliptic AG Codes

Theorem (Explicit Example 3)

Let $q = 2^m$, with $m \geq 1$ an integer, and $F/\mathbb{F}_q$ be the elliptic function field with e rational points. Let a_1, a_2, b_1, b_2 be positive integers such that $b_1 \leq a_1 - 2$, $b_2 \leq e - 1 - a_1$, 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 a QUENTA code with parameters

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

- If $b_2 < a_1 + 1$, then there exists a QUENTA code with parameters

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

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 $G_1 = a_1 P_0 + a_2 P_\infty$ and $G_2 = b_1 P_0 + b_2 P_\infty$
- Let $\eta = \frac{dx}{\prod_{\alpha_i \in S}(x+\alpha_i)}$, 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 $G_1 = a_1 P_0 + a_2 P_\infty$ and $G_2 = b_1 P_0 + b_2 P_\infty$
- Let $\eta = \frac{dx}{\prod_{\alpha_i \in S}(x+\alpha_i)}$, then $(\eta) = (e-1)P_\infty - P_{\alpha_0} - D$
- The fact that $b_2 \leq e - 1 - a_1$ implies in $G_1^\perp \cup G_2 = b_1 P_{q^3} + (e - 1 - a_1)P_\infty$
- By the hypothesis $b_1 \leq a_1 - 2$, we have that $\deg(G_1^\perp \cup G_2) < e - 2$, thus we can use main theorem
- Then the first case comes from $b_2 \geq a_1 + 1$, which implies that $\deg(G_1^\perp \cap G_2) \geq 0$ and $c = e - 1 - (a_2 + b_2)$

QUENTA codes derived from Rational AG Codes

Corollary

If there exists an elliptic curve with e rational places, then for $a_2 \leq a_1 \leq \lfloor \frac{e-2}{2} \rfloor$ there is an almost near MDS QUENTA code with parameters $[[e-2, a_1+a_2-2, e-2-(a_1+a_2); e-2-(a_1+a_2)]]_q$.

Content

Preliminary

Definition

Let q be a prime power and $\alpha_q = \sup\{R \in [0,1] : (\delta, R) \in U_q\}$, 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 $n_t \to \infty$ as $t \to \infty$ 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.

Preliminary

Proposition[12]

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

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

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

Asymptotically Good QUENTA Codes

Theorem

Let $q \geq 3$ be a power of a prime and $A(q)$ as before. 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

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

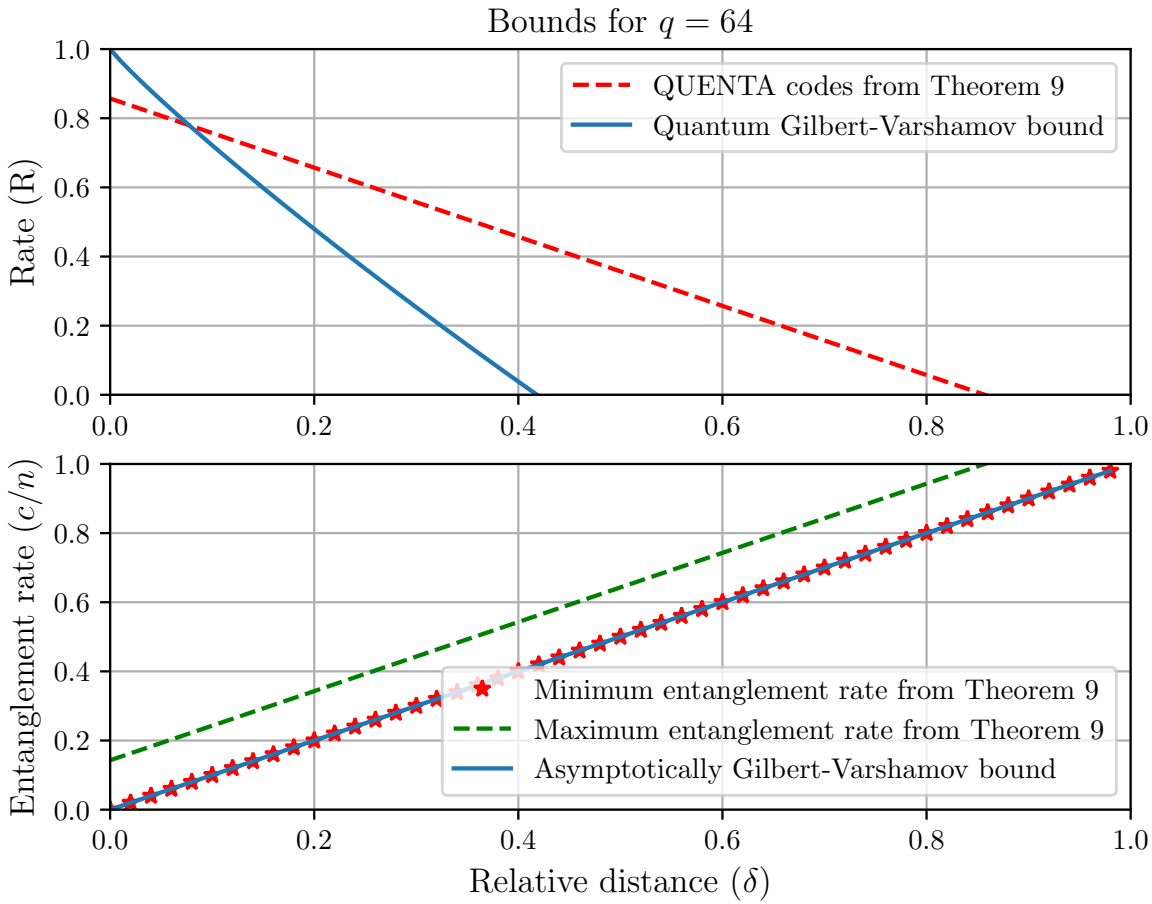
and

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

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

Comparison between asymptotically QUENTA codes and quantum GV bound[13]

Test



[13] 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