Quantum BCH and Reed-Solomon Entanglement-Assisted Codes

Francisco R. F. Pereira
Joint work with Ruud Pellikaan

TU/e, the Netherlands

40th WIC SITB, Belgium
May 28, 2019

Content

Classical and Quantum Information

- **Classical information**
  often represented by a finite alphabet, e.g., bits 0 and 1

- **Quantum-bit (qubit)**
  basis states:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{C}^2 \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{C}^2$$

  general pure state

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad \text{where } \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

  measurement (read-out):

  "0" with probability $|\alpha|^2$ "1" with probability $|\beta|^2$

Classical and Quantum Information

- **Bit strings**
  larger set of messages represented by bit strings of length n, i.e., $\mathbf{x} \in \{0,1\}^n$

- **Quantum register**
  basis states:

$$|b_1\rangle \otimes \cdots \otimes |b_n\rangle = |b_1 \ldots b_n\rangle = |\mathbf{b}\rangle \quad \text{where } b_i \in \{0,1\}$$

  general pure state:

$$|\psi\rangle = \sum_{\mathbf{x}\in\{0,1\}^n} c_{\mathbf{x}} |\mathbf{x}\rangle \quad \text{where} \quad \sum_{\mathbf{x}\in\{0,1\}^n} |c_{\mathbf{x}}|^2 = 1$$

Classical and Quantum Information

- **Bit strings**
  larger set of messages represented by bit strings of length n, i.e., $\mathbf{x} \in \{0,1\}^n$

- **Quantum register**
  basis states:

$$|b_1\rangle \otimes \cdots \otimes |b_n\rangle = |b_1 \ldots b_n\rangle = |\mathbf{b}\rangle \quad \text{where } b_i \in \{0,1\}$$

  general pure state:

$$|\psi\rangle = \sum_{\mathbf{x}\in\{0,1\}^n} c_{\mathbf{x}} |\mathbf{x}\rangle \quad \text{where} \quad \sum_{\mathbf{x}\in\{0,1\}^n} |c_{\mathbf{x}}|^2 = 1$$

  For example, $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Error Basis

- **Pauli Matrices**

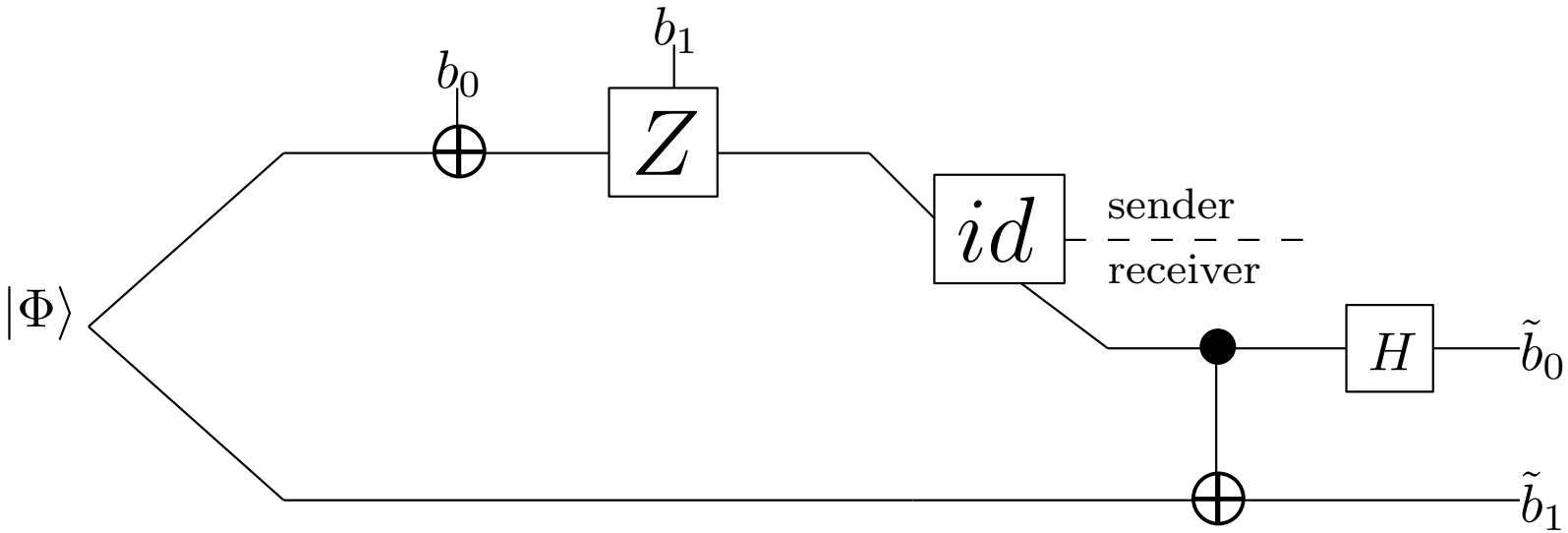
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

vector space basis of all 2×2 matrices

Content

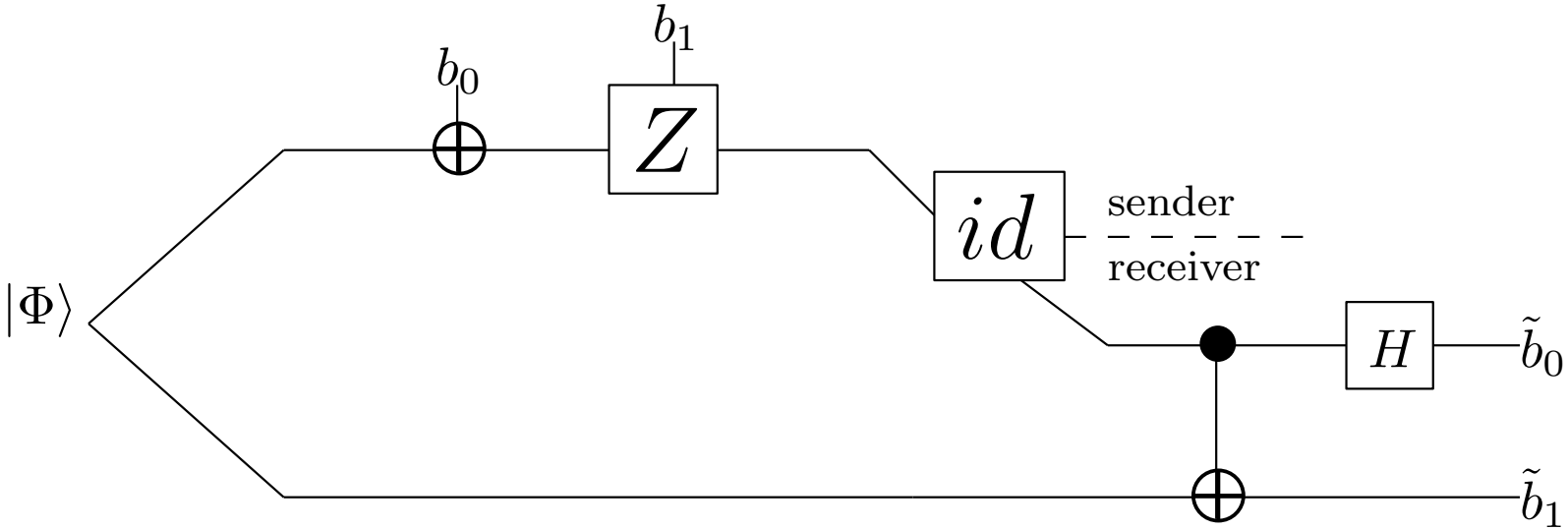
Super Dense Coding

How does it work?



Super Dense Coding

How does it work?



- Two classical bits with one use of a quantum channel
- Proposed by Bennett and Weisner in 1992

Content

Attempt of Repetition Code

- Good candidate for Bit-flip channels

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad \rightarrow \quad |\psi_{enc}\rangle = \alpha\,|000\rangle + \beta\,|111\rangle$$

Attempt of Repetition Code

- Good candidate for Bit-flip channels

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad \rightarrow \quad |\psi_{enc}\rangle = \alpha\,|000\rangle + \beta\,|111\rangle$$

- Possibles 1-qubit error in our setting

$$\begin{matrix} |000\rangle \\ |111\rangle \end{matrix} \xrightarrow{I\otimes I\otimes I} \begin{matrix} |000\rangle \\ |111\rangle \end{matrix}$$

Attempt of Repetition Code

- Good candidate for Bit-flip channels

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad \rightarrow \quad |\psi_{enc}\rangle = \alpha\,|000\rangle + \beta\,|111\rangle$$

- Possibles 1-qubit error in our setting

$$\begin{array}{ccc} |000\rangle & \xrightarrow{I\otimes I\otimes I} & |000\rangle \\ |111\rangle & & |111\rangle \end{array}$$

$$\begin{array}{ccc} |000\rangle & \xrightarrow{X\otimes I\otimes I} & |100\rangle \\ |111\rangle & & |011\rangle \end{array}$$

Attempt of Repetition Code

- Good candidate for Bit-flip channels

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad \rightarrow \quad |\psi_{enc}\rangle = \alpha\,|000\rangle + \beta\,|111\rangle$$

- Possibles 1-qubit error in our setting

$$\begin{array}{ccc} |000\rangle & \xrightarrow{I\otimes I\otimes I} & |000\rangle \\ |111\rangle & & |111\rangle \end{array}$$

$$\begin{array}{ccc} |000\rangle & \xrightarrow{X\otimes I\otimes I} & |100\rangle \\ |111\rangle & & |011\rangle \end{array}$$

$$\begin{array}{ccc} |000\rangle & \xrightarrow{I\otimes X\otimes I} & |010\rangle \\ |111\rangle & & |101\rangle \end{array}$$

Attempt of Repetition Code

- Good candidate for Bit-flip channels

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad \rightarrow \quad |\psi_{enc}\rangle = \alpha\,|000\rangle + \beta\,|111\rangle$$

- Possibles 1-qubit error in our setting

$$\begin{array}{lll} |000\rangle & \xrightarrow{I\otimes I\otimes I} & |000\rangle \\ |111\rangle & & |111\rangle \end{array}$$

$$\begin{array}{lll} |000\rangle & \xrightarrow{X\otimes I\otimes I} & |100\rangle \\ |111\rangle & & |011\rangle \end{array}$$

$$\begin{array}{lll} |000\rangle & \xrightarrow{I\otimes X\otimes I} & |010\rangle \\ |111\rangle & & |101\rangle \end{array}$$

$$\begin{array}{lll} |000\rangle & \xrightarrow{I\otimes I\otimes X} & |001\rangle \\ |111\rangle & & |110\rangle \end{array}$$

Content

Entanglement-Assisted Quantum Error Correcting Code

- The first QUENTA code was proposed by Bowen[1]
- The stabilizer formalism for qubits QUENTA code was done by Brun *et al.*[2]
- This class of codes can violate the quantum Hamming bound[3]

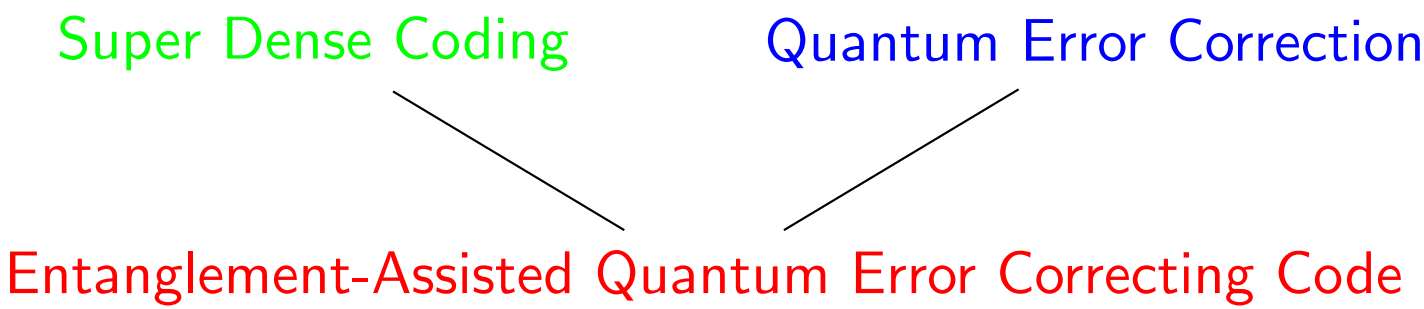
[1] Bowen, G.: Entanglement required in achieving entanglement-assisted channel capacities. Physical Review A 66, 052313–1-052313–8 (2006)

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

[3] 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 Code

- The first QUENTA code was proposed by Bowen[1]
- The stabilizer formalism for qubits QUENTA code was done by Brun *et al.*[2]
- This class of codes can violate the quantum Hamming bound[3]

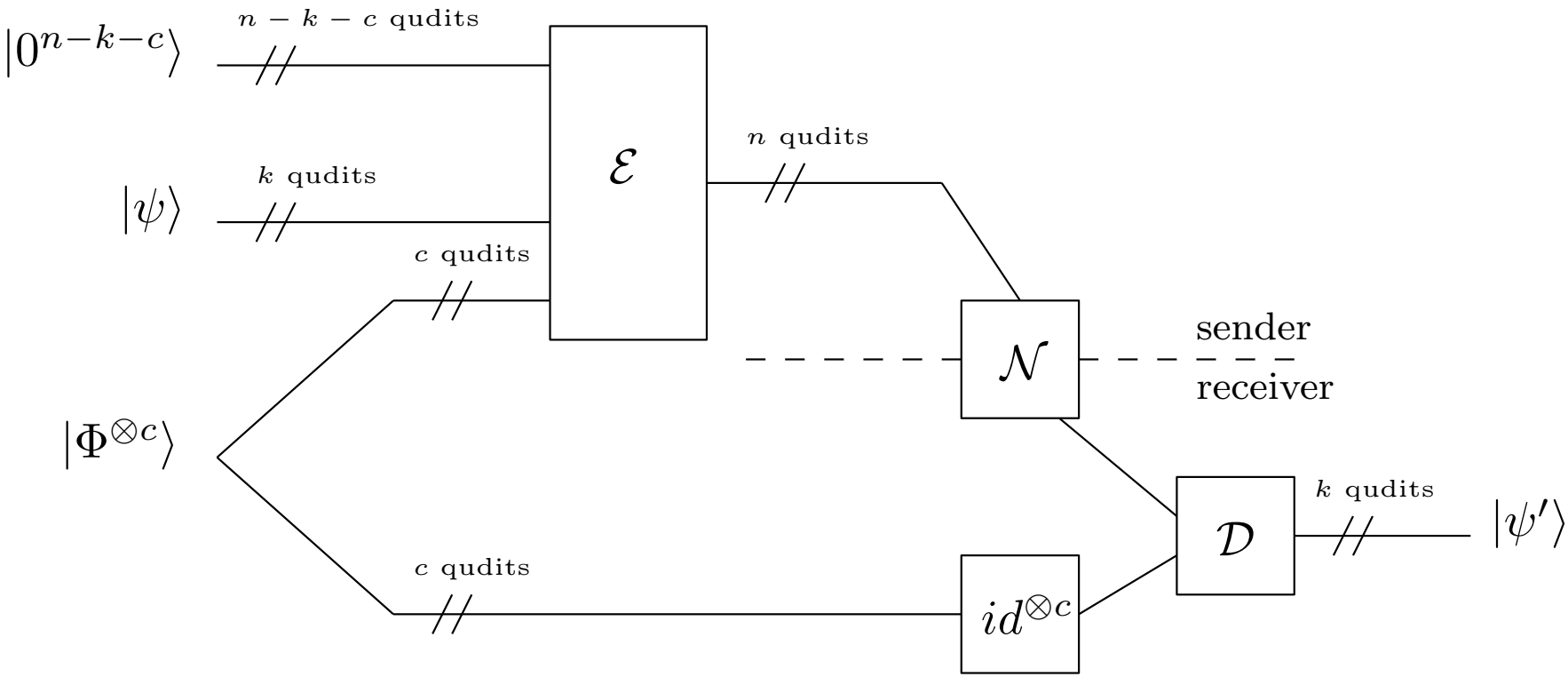


[1] Bowen, G.: Entanglement required in achieving entanglement-assisted channel capacities. Physical Review A 66, 052313–1-052313–8 (2006)

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

[3] 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)

QUENTA Code Scheme



Euclidean Construction Method

Proposition

Let C_1 and C_2 be two linear codes with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ and parity check matrices H_1 and H_2, respectively. Then there is an QUENTA code with parameters $[[n, k_1 + k_2 - n + c, d \geq \min\{d_1, d_2\}; c]]_q$ that requires

$$c = \text{rank}(H_1 H_2^T)$$

Euclidean Construction Method

Proposition

Let C_1 and C_2 be two linear codes with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ and parity check matrices H_1 and H_2, respectively. Then there is an QUENTA code with parameters $[[n, k_1 + k_2 - n + c, d \geq \min\{d_1, d_2\}; c]]_q$ that requires

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

maximally entangled states.

Euclidean Construction Method

Proposition

Let C_1 and C_2 be two linear codes with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ and parity check matrices H_1 and H_2, respectively. Then there is an QUENTA code with parameters $[[n, k_1 + k_2 - n + c, d \geq \min\{d_1, d_2\}; c]]_q$ that requires

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

maximally entangled states.

A entanglement-assisted quantum code is

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

Content

Content

Notation

- Let $q \neq 2$ be a prime power and $\mathbb{F}_q$ be a finite field
- n denotes the code length, with $\gcd(n, q) = 1$, and $m = \mathrm{ord}_n(q)$
- $Z(C)$ denotes the defining set of a cyclic code C
- Lastly, $g(x)$ is the generator polynomial of C

BCH Codes

Definition

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

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

where $m_i(x)$ is the minimal polynomial of α^i over $\mathbb{F}_q$. In particular, $Z(C) = \{b, b+1, \ldots, b+\delta-2\}$.

If $n = q^m - 1$ then the BCH code is called *primitive*, and if $b = 1$ it is called *narrow sense*.

BCH Codes

Definition

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

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

where $m_i(x)$ is the minimal polynomial of α^i over $\mathbb{F}_q$. In particular, $Z(C) = \{b, b+1, \ldots, b+\delta-2\}$.
If $n = q^m - 1$ then the BCH code is called *primitive*, and if $b = 1$ it is called *narrow sense*.

It is possible to show that the dimension is equal to $n - |Z(C)|$ and the minimal distance of C is at least δ

Euclidian Dual BCH Codes

Proposition

Let C be a BCH code of length n and defining set $Z(C)$. Then the defining set of $C^{\perp}$ is given by

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

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

Reed-Solomon Codes

Definition

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

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

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

Reed-Solomon Codes

Definition

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

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

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

Defining set: $Z(RS_k(n, b)) = \{b, b + 1, \ldots, b + n - k - 1\}$

Euclidean Dual Reed-Solomon Codes

Proposition

Let $RS_k(n, b)$ be a Reed-Solomon code. Then its Euclidian dual can be described as

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

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

Content

The General Cyclic Case

Lemma

Let C_1 and C_2 be two cyclic codes with defining set $Z(C_1)$ and $Z(C_2)$, respectively. Then

$$Z(C_1 \cap C_2) = Z(C_1) \cup Z(C_2).$$

The General Cyclic Case

Lemma

Let C_1 and C_2 be two cyclic codes with defining set $Z(C_1)$ and $Z(C_2)$, respectively. Then

$$Z(C_1 \cap C_2) = Z(C_1) \cup Z(C_2).$$

Theorem

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

The General Cyclic Case

Corollary

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

Quantum Reed-Solomon Entanglement-Assisted Codes

Theorem

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

1. For $k_1 - b_1 \geq b_2$, there is an QUENTA code with parameters

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

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

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

Quantum Reed-Solomon Entanglement-Assisted Codes

Corollary

Let $C = RS_k(n, b)$ be a Reed-Solomon codes over $\mathbb{F}_q$ with $0 \leq b \leq (k+1)/2$. Then there is an MDS QUENTA code with parameters $[[n, 2b-1, n-k+1; n+2b-2k-1]]_q$. In particular, for $b = (k+1)/2$, there is a maximal entanglement MDS QUENTA code.

Quantum BCH Entanglement-Assisted Codes

Theorem

Let C_1 and C_2 be two BCH codes over $\mathbb{F}_q$ with $Z(C_i) = \{b_i, \ldots, b_i + \delta - 2\}$, for $i = 1, 2$, with $b_1 + b_2 = n + 2 - \delta$. If the parameters are given by $[n, k_1, \delta]_q$ and $[n, k_2, \delta]_q$ for C_1 and C_2, respectively, then there is an QUENTA code with parameters $[[n, k_1 + k_2 - n + c, \delta; c]]_q$, with $c = n - \max\{k_1, k_2\}$.

Thanks for your attention!

Any questions?