The 9th International Workshop on Boolean Functions and their Applications (BFA)

September 9–13, 2024, Dubrovnik, Croatia

Quantum Codes from Classical Codes

Markus Grassl

International Centre for Theory of Quantum Technologies
University of Gdansk

markus.grassl@ug.edu.pl

www.codetables.de

12 September 2024

European Funds Smart Growth · Republic of Poland · FNP Foundation for Polish Science · European Union European Regional Development Fund

Overview

- qubits and qudits
- quantum codes (QECC)
  - CSS codes
  - stabilizer codes
- entanglement assisted quantum codes (EAQECC)
  - general code constructions
  - varying the hull dimension
  - propagation rules
- summary & outlook

Quantum Information

Quantum-bit (qubit)

basis states:

$$\text{“0”} \mathrel{\hat{=}} |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{C}^2, \qquad \text{“1”} \mathrel{\hat{=}} |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{C}^2$$

general state:

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

measurement (read-out):

result “0” with probability $|\alpha|^2$

result “1” with probability $|\beta|^2$

Quantum Information

Quantum register

basis states:

$$|b_1\rangle \otimes \ldots \otimes |b_n\rangle =: |b_1 \ldots b_n\rangle = |\boldsymbol{b}\rangle \qquad \text{where } b_i \in \{0,1\}$$

general state:

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

$\longrightarrow$ normalized vector in $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$

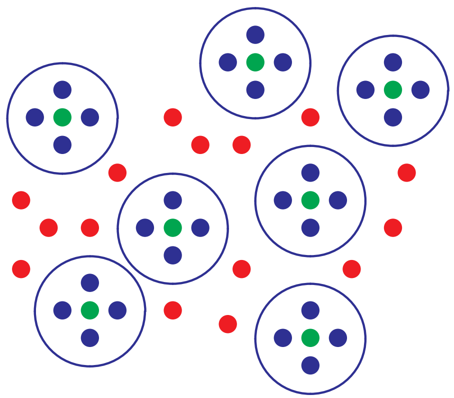
Qudits

generalization to $(\mathbb{C}^q)^{\otimes n}$: basis states $|\boldsymbol{b}\rangle$ labelled by vectors $\boldsymbol{b} \in \mathbb{F}_q^n$
$\Longrightarrow$ group algebra $\mathbb{C}[\mathbb{F}_q^n]$

The Basic Idea of QECC

Classical Codes

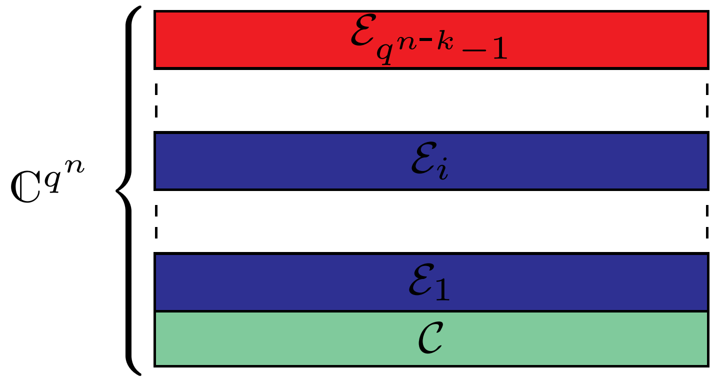
Partition of the set of all words of length n over an alphabet of size q.



- codewords
- errors of bounded weight
- other errors

Quantum Codes

Orthogonal decomposition of the vector space $\mathcal{H}^{\otimes n}$, where $\mathcal{H} \cong \mathbb{C}^q$.



$$\mathcal{H}^{\otimes n} = \mathcal{C} \oplus \mathcal{E}_1 \oplus \ldots \oplus \mathcal{E}_{q^{n-k}-1}$$

encoding: $|\boldsymbol{x}\rangle \mapsto U_{\text{enc}}(|\boldsymbol{x}\rangle \otimes |0\rangle)$

Quantum Errors

Bit-flip error:

- Interchanges $|0\rangle$ and $|1\rangle$. Corresponds to "classical" bit error.
- Given by NOT gate $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Phase-flip error:

- Inverts the relative phase of $|0\rangle$ and $|1\rangle$. Has no classical analogue!
- Given by the matrix $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Combination:

- Combining bit-flip and phase-flip gives $Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = XZ$.

Error Basis

Pauli Matrices

$$\sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- vector space basis of all 2×2 matrices
- unitary matrices which generate a *finite* group

Error Basis for many Qubits/Qudits

$\mathcal{E}$ error basis for subsystem of dimension d with $I \in \mathcal{E}$

$\Longrightarrow \mathcal{E}^{\otimes n}$ error basis with elements

$$E := E_1 \otimes \ldots \otimes E_n, \quad E_i \in \mathcal{E}$$

weight of E: number of factors $E_i \neq I$

Quantum Depolarizing Channel

- analogue of the binary symmetric channel (BSC) and uniform symmetric channel (USC)
- either transmits a quantum state faithfully or replaces it with a completely random (maximally mixed) state

$$\rho \mapsto (1-p)\rho + p\mathbb{1} = (1-p)\rho + \frac{p}{d^2}\sum_{E\in\mathcal{E}} E\rho E^\dagger,$$

  where $\mathcal{E}$ is (nice) unitary error basis

- after *discretisation*, each error operator E different from identity is equally likely

other quantum channels:
dephasing channel, amplitude damping channel, asymmetric channels

warning: A quantum channel implies a discrete channel, not the other way round.

Quantum Error-Correcting Codes (QECC)

- **subspace** $\mathcal{C}$ of a complex vector space $\mathcal{H} \cong \mathbb{C}^N$
  usually: $\mathcal{H} \cong \mathbb{C}^q \otimes \mathbb{C}^q \otimes \ldots \otimes \mathbb{C}^q =: (\mathbb{C}^q)^{\otimes n}$ "n qudits"

- **errors:** described by linear transformations acting non-trivially on some of the subsystems (local errors)

- **notation:** $\boxed{\mathcal{C} = ((n, K, d))_q}$ or $\boxed{\mathcal{C} = [\![n, k, d]\!]_q}$
  K-dimensional or q^k-dimensional subspace $\mathcal{C}$ of $(\mathbb{C}^q)^{\otimes n} \cong \mathbb{C}^{q^n}$

- **minimum distance** d:
  - detection of all errors acting nontrivially on $d-1$ subsystems
  - correction of all errors acting on $\lfloor (d-1)/2 \rfloor$ subsystems
  - correction of all erasures affecting up to $d-1$ subsystems
    [Grassl, Beth, & Pellizzari, *Codes for the Quantum Erasure Channel*, PRA **56**, pp. 33–38 (1997)]

Bit-flips and Phase-flips

Let $C \leq \mathbb{F}_2^n$ be a linear code. Then the image of the state

$$\frac{1}{\sqrt{|C|}} \sum_{\boldsymbol{c} \in C} |\boldsymbol{c}\rangle$$

under first a phase-flip $\boldsymbol{z} \in \mathbb{F}_2^n$ and then a bit-flip $\boldsymbol{x} \in \mathbb{F}_2^n$ is given by

$$\frac{1}{\sqrt{|C|}} \sum_{\boldsymbol{c} \in C} (-1)^{\boldsymbol{z} \cdot \boldsymbol{c}} |\boldsymbol{c} + \boldsymbol{x}\rangle.$$

Hadamard transform $H \otimes \ldots \otimes H$ maps this to

$$\frac{(-1)^{\boldsymbol{x} \cdot \boldsymbol{z}}}{\sqrt{|C^\perp|}} \sum_{\boldsymbol{b} \in C^\perp} (-1)^{\boldsymbol{x} \cdot \boldsymbol{b}} |\boldsymbol{b} + \boldsymbol{z}\rangle$$

CSS Codes

Introduced by R. Calderbank, P. Shor, and A. Steane
[Calderbank & Shor PRA, **54**, 1098–1105, 1996]
[Steane, PRL **77**, 793–797, 1996]

Construction: Let $C_1 = [n, k_1, d_1]_q$ and $C_2 = [n, k_2, d_2]_q$ be classical linear codes with $C_2^\perp \le C_1$. Let $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_K\}$ be representatives for the cosets $C_1/C_2^\perp$. Define quantum states

$$|\boldsymbol{x}_i + C_2^\perp\rangle := \frac{1}{\sqrt{|C_2^\perp|}} \sum_{\boldsymbol{y} \in C_2^\perp} |\boldsymbol{x}_i + \boldsymbol{y}\rangle$$

Theorem: Then the vector space $\mathcal{C}$ spanned by these states is a quantum code with parameters $[\![n, k_1 + k_2 - n, d]\!]_q$ where

$$d \ge \min\left\{\operatorname{wgt}(C_1 \setminus C_2^\perp), \operatorname{wgt}(C_2 \setminus C_1^\perp)\right\} \ge \min(d_1, d_2).$$

($d = \min(d_1, d_2)$ when $C_2^\perp = C_1$)

CSS Codes — how they work

Basis states:

$$|\boldsymbol{x}_i + C_2^\perp\rangle = \frac{1}{\sqrt{|C_2^\perp|}} \sum_{\boldsymbol{y}\in C_2^\perp} |\boldsymbol{x}_i + \boldsymbol{y}\rangle$$

Suppose a bit-flip error $\boldsymbol{b}$ happens to $|\boldsymbol{x}_i + C_2^\perp\rangle$:

$$\frac{1}{\sqrt{|C_2^\perp|}} \sum_{\boldsymbol{y}\in C_2^\perp} |\boldsymbol{x}_i + \boldsymbol{y} + \boldsymbol{b}\rangle$$

Now, we introduce an ancilla register initialized in $|0\rangle$ and compute the syndrome.

CSS Codes — how they work

Let H_1 be the parity check matrix of C_1, *i. e.*, $\boldsymbol{x}H_1^t = 0$ for all $\boldsymbol{x} \in C_1$.

$$\frac{1}{\sqrt{|C_2^\perp|}} \sum_{\boldsymbol{y} \in C_2^\perp} |\boldsymbol{x}_i + \boldsymbol{y} + \boldsymbol{b}\rangle |(\boldsymbol{x}_i + \boldsymbol{y} + \boldsymbol{b})H_1^t\rangle = \frac{1}{\sqrt{|C_2^\perp|}} \sum_{\boldsymbol{y} \in C_2^\perp} |\boldsymbol{x}_i + \boldsymbol{y} + \boldsymbol{b}\rangle |\boldsymbol{b}H_1^t\rangle$$

measure the ancilla to obtain $\boldsymbol{s} = \boldsymbol{b}H_1^t$

use this to correct the error by a conditional operation which flips the bits in $\boldsymbol{b}$

Phase-flips: Suppose we have the state

$$\frac{1}{\sqrt{|C_2^\perp|}} \sum_{\boldsymbol{y} \in C_2^\perp} (-1)^{(\boldsymbol{x}_i + \boldsymbol{y}) \cdot \boldsymbol{z}} |\boldsymbol{x}_i + \boldsymbol{y}\rangle$$

$H^{\otimes n}$ yields a superposition over a coset of C_2 which has a bit-flip.

Correct it as before (with a parity check matrix for C_2).

independent correction of bit-/phase flips $\Longrightarrow$ correction of combinations

Quantum Stabilizer Codes

[Gottesman, PRA **54** (1996); Calderbank, Rains, Shor, & Sloane, IEEE-TIT **44** (1998)]

Basic Idea

Decomposition of the complex vector space into eigenspaces of operators.

Error Basis for Qudits

[A. Ashikhmin & E. Knill, Nonbinary quantum stabilizer codes, IEEE-TIT **47** (2001)]

$$\mathcal{E} = \{X^\alpha Z^\beta : \alpha, \beta \in \mathbb{F}_q\},$$

where (you may think of $\mathbb{C}^q \cong \mathbb{C}[\mathbb{F}_q]$)

$$X^\alpha = \sum_{x\in\mathbb{F}_q} |x+\alpha\rangle\langle x| \qquad \text{for } \alpha \in \mathbb{F}_q$$

$$\text{and} \quad Z^\beta = \sum_{z\in\mathbb{F}_q} \omega^{\mathrm{Tr}(\beta z)}|z\rangle\langle z| \quad \text{for } \beta \in \mathbb{F}_q \ (\omega = \omega_p = \exp(2\pi i/p))$$

Stabilizer Codes

common eigenspace of an Abelian subgroup $\mathcal{S}$ of the group $\mathcal{G}_n$ with elements

$$\omega^\gamma(X^{\alpha_1}Z^{\beta_1})\otimes(X^{\alpha_2}Z^{\beta_2})\otimes\ldots\otimes(X^{\alpha_n}Z^{\beta_n}) =: \omega^\gamma X^{\boldsymbol{\alpha}}Z^{\boldsymbol{\beta}},$$

where $\boldsymbol{\alpha},\boldsymbol{\beta}\in\mathbb{F}_q^n$, $\gamma\in\mathbb{F}_p$

quotient group:

$$\overline{\mathcal{G}}_n := \mathcal{G}_n/\langle\omega I\rangle \cong (\mathbb{F}_q\times\mathbb{F}_q)^n \cong \mathbb{F}_q^n\times\mathbb{F}_q^n \quad \textit{as additive spaces}$$

$\mathcal{S}$ Abelian subgroup

$\iff (\boldsymbol{\alpha},\boldsymbol{\beta})\star(\boldsymbol{\alpha}',\boldsymbol{\beta}')=0$ for all $\omega^\gamma(X^{\boldsymbol{\alpha}}Z^{\boldsymbol{\beta}})$, $\omega^{\gamma'}(X^{\boldsymbol{\alpha}'}Z^{\boldsymbol{\beta}'})\in\mathcal{S}$,

where $\star$ is a symplectic inner product on $\mathbb{F}_q^n\times\mathbb{F}_q^n$

Stabilizer codes correspond to trace symplectic self-orthogonal codes over $\mathbb{F}_q^n\times\mathbb{F}_q^n$

Trace Symplectic Self-Orthogonal Codes

most general:

additive codes $C \subset \mathbb{F}_q^n \times \mathbb{F}_q^n$ that are self-orthogonal with respect to

$$(\boldsymbol{v}, \boldsymbol{w}) \star (\boldsymbol{v}', \boldsymbol{w}') := \operatorname{Tr}(\boldsymbol{v} \cdot \boldsymbol{w}' - \boldsymbol{v}' \cdot \boldsymbol{w}) = \operatorname{Tr}\Big(\sum_{i=1}^{n} v_i w_i' - v_i' w_i\Big) \tag{1}$$

special cases:

for $\mathbb{F}_q$-linear codes $C \subset \mathbb{F}_q^n \times \mathbb{F}_q^n$, (1) reduces to the symplectic inner product

$$(\boldsymbol{v}, \boldsymbol{w}) \star (\boldsymbol{v}', \boldsymbol{w}') := \boldsymbol{v} \cdot \boldsymbol{w}' - \boldsymbol{v}' \cdot \boldsymbol{w} = \sum_{i=1}^{n} v_i w_i' - v_i' w_i$$

for $\mathbb{F}_{q^2}$-linear codes $C \subset \mathbb{F}_{q^2}^n$ (1) reduces to the Hermitian inner product

$$\boldsymbol{x} \star \boldsymbol{y} := \sum_{i=1}^{n} x_i^q y_i \qquad \text{(identifying } \mathbb{F}_q \times \mathbb{F}_q \text{ and } \mathbb{F}_{q^2}\text{)}$$

Quantum Codes from Classical Codes

Hermitian self-orthogonal code

linear code $C = [n, k, d']_{q^2} \leq \mathbb{F}_{q^2}^n$ that is self-orthogonal with respect to the Hermitian inner product

$$\boldsymbol{x} \star \boldsymbol{y} := \sum_{i=1}^{n} x_i^q y_i,$$

i. e., $C \leq C^\star = \{\boldsymbol{x} \in \mathbb{F}_{q^2}^n \mid \forall \boldsymbol{y} \in C \colon \boldsymbol{x} \star \boldsymbol{y} = 0\}$

Theorem: (Hermitian construction)

Let $C = [n, k, d']_{q^2}$ be a Hermitian self-orthogonal code and let

$$d := \min\{\mathrm{wgt}(\boldsymbol{c}) \colon \boldsymbol{c} \in C^\star \setminus C\} \geq d_{\mathsf{min}}(C^\star).$$

Then there exists a quantum code $\mathcal{C} = [\![n, n-2k, d]\!]_q$. $\mathcal{C}$ is *pure* iff $d = d_{\mathsf{min}}(C^\star)$.

[Ketkar et al., *Nonbinary stabilizer codes over finite fields*, IEEE-TIT **52**, pp. 4892–4914 (2006)]

A Connection to Boolean Functions

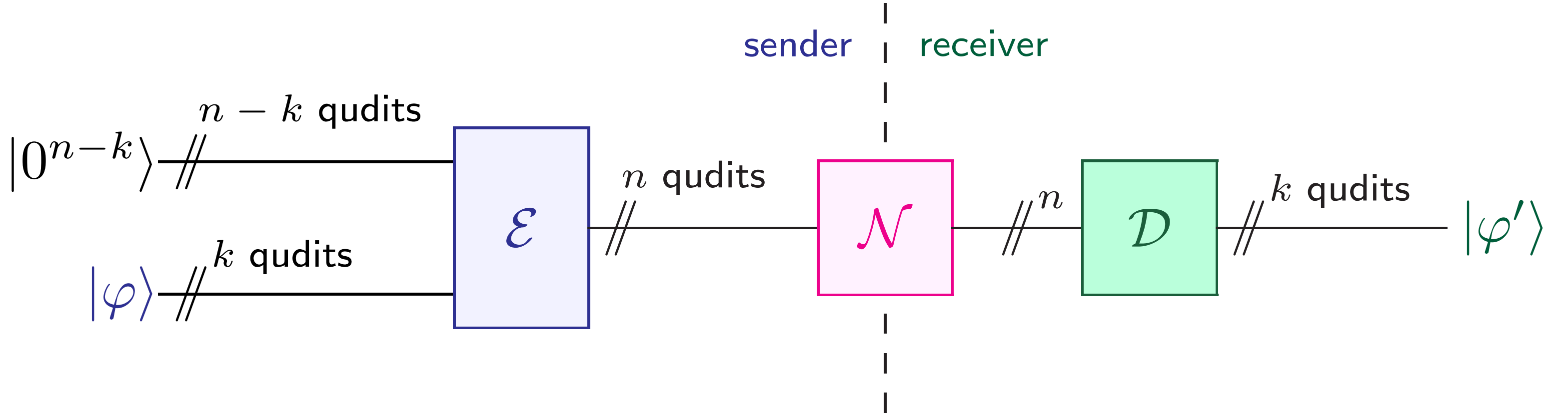
[Aggarwal & Calderbank, IEEE Trans. Inf. Theory, **54**, 1700–1707 (2008)]

- $f(x_1,\ldots,x_n) = \sum_{i=0}^{2^n-1} y_i x_1^{c_1}\cdots x_n^{c_n}$ a Boolean function
- $P_1,\ldots,P_n$ distinct, mutually commuting orthogonal projection operators on $\mathbb{C}^{2^n}$ of rank 2^{n-1}
- $P_f = f(P_1,\ldots,P_n) = \bigvee_{i=0}^{2^n-1} y_i P_1^{c_1}\cdots P_n^{c_n}$
  is a projection operator, where $P\vee P' := P+P'-PP'$ and $P^0 := I-P$
- $\operatorname{rank}(P_f) = |\{(x_1,\ldots,x_n)\in\mathbb{F}_2^n\colon f(x_1,\ldots,x_n)=1\}| = \operatorname{wgt}(f) = K$
- conditions on the *complementary set* of f

$$\mathsf{Cset}_f = \Big\{\boldsymbol{a}\colon \sum_{\boldsymbol{x}\in\mathbb{F}_2^n} f(\boldsymbol{x})f(\boldsymbol{x}+\boldsymbol{a}) = 0\Big\}$$

imply that P_f projects onto a QECC $((n,K,d))_2$

Quantum Error-Correcting Code (QECC)



Scheme of a communication protocol using a QECC $[\![n, k, d]\!]_q$

quantum Singleton bound: $\boxed{2d \leq n + 2 - k}$

[E. Rains, Nonbinary Quantum Codes, IEEE-TIT **45**, pp. 1827–1832 (1999)]

open question:

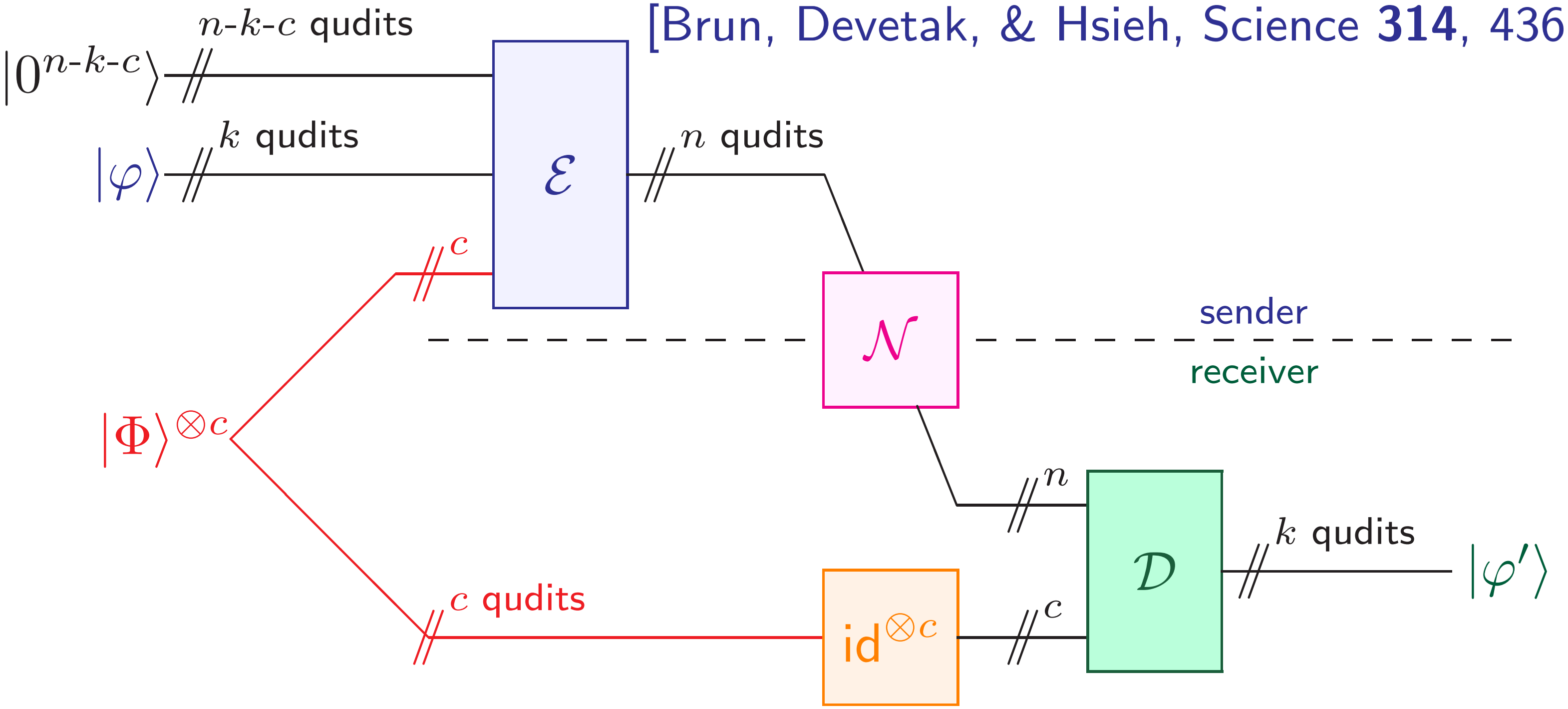
For which n, k do quantum MDS codes exist?

QMDS conjecture:

$n \leq q^2 + 1$ for $d > 2$ ($n \leq q^2 + 2$ in some cases)

Entanglement-Assisted QECC

[Brun, Devetak, & Hsieh, Science **314**, 436 (2006)]



Communication scheme using an entanglement-assisted QECC $\mathcal{C} = [\![n, k, d; c]\!]_q$

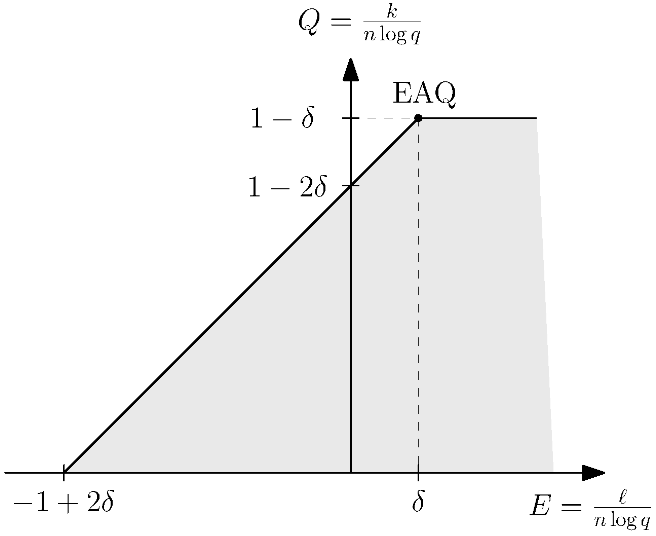
similar to a QECC of length $n + c$

$\Longrightarrow$ **conjectured bound:** $\boxed{2d \leq n + c + 2 - k}$

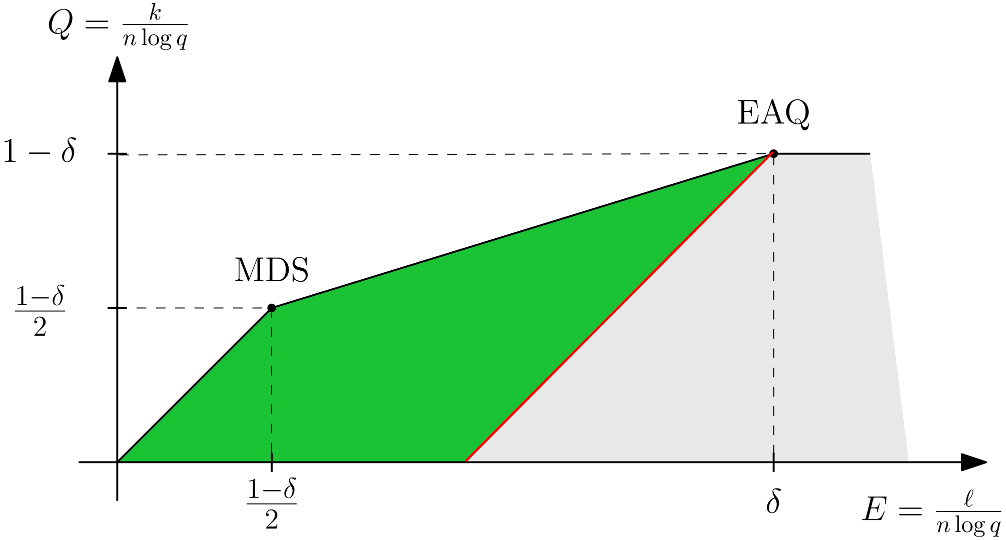
[Brun, Devetak, & Hsieh, arXiv:quant-ph/0608027]

Singleton-type Bounds

[Grassl, Huber, Winter, IEEE-TIT **68**, pp. 3942–3950 (2022)]



$(a) \quad \delta = \frac{d-1}{n} < \frac{1}{2}$



$(c) \quad \delta > \frac{1}{2}$

$\mathcal{C} = [\![n, k, d; c]\!]_q$:

(a) $\quad d < n/2 + 1 : \quad k \le \min\{n + c + 2 - 2d, n - d + 1\}$

(c) $\quad d \ge n/2 + 1 : \quad k \le c,$

$$k \le \frac{n-d+1}{3d-3-n}\big(c + (2d - 2 - n)\big),$$

$$k \le n - d + 1$$

Constructing Entanglement-Assisted QECC

Hermitian hull: $\mathrm{Hull}(C) = C \cap C^\star$

C is Hermitian self-orthogonal $\iff \mathrm{Hull}(C) = C$

Theorem: (Hermitian construction)
Let $C = [n, k, d']_{q^2}$ be a linear code with $c = k - \dim \mathrm{Hull}(C)$ and let

$$d := \min\{\mathrm{wgt}(\boldsymbol{c})\colon \boldsymbol{c} \in C^\star \setminus \mathrm{Hull}(C)\} \geq d_{\textsf{min}}(C^\star).$$

Then there exists an entanglement-assisted quantum code $\mathcal{C} = [\![n, n-2k+c, d; c]\!]_q$.

[Galindo et al., *Entanglement-assisted quantum error-correcting codes over arbitrary finite fields*, Quantum Inform. Proc., (2019)]

Proof idea: Lengthen the code C by c positions to make it self-orthogonal.
Additional positions correspond to c maximally entangled states.

LCD Codes

C is a linear complementary dual (LCD) code $\Longleftrightarrow \mathrm{Hull}(C) = C \cap C^\perp = \{\mathbf{0}\}$

Theorem [Carlet et al., IEEE-TIT **64** pp. 3010–3017 (2018)]
For $q > 2$, any linear code over $\mathbb{F}_{q^2}$ is monomially equivalent to a Hermitian LCD code.

Corollary
Given a linear code $C = [n, k, d]_{q^2}$, there exists an EAQECC $\mathcal{C} = [\![n, k, d; n-k]\!]_q$.

This is the point EAQ in the previous diagram.

but:
EAQECC from LCD codes require the maximal amount $c = n - k$ of entanglement.

Decreasing the Hull Dimension

[Luo, Ezerman, Grassl, Ling, arXiv:2207.05647]

Lemma

$$\dim \mathrm{Hull}(C) = k - \mathrm{rank}(GG^\star) \text{ and } c = \mathrm{rank}(GG^\star)$$

where G is a generator matrix of C and $G^\star$ its conjugate transpose

Theorem

For $C = [n, k, d]_{q^2}$ with $q > 2$ and $\dim \mathrm{Hull}(C) = \ell$, there exist equivalent codes C' with $\dim \mathrm{Hull}(C') = \ell'$ for each $\ell' \in \{0, 1, \ldots, \ell\}$.

Proof idea: Decompose C into the hull and its complement. Multiply the information set of the hull by some a_i with $a_i^{q+1} \neq 1$ to reduce the dimension of the hull.

Propagation Rule

Hermitian construction of a pure EAQECC $[\![n, k, d; c]\!]_q$ with $q > 2$ and $\dim \mathrm{Hull}(C) = \ell$ implies codes $[\![n, k + i, d; c + i]\!]_q$ for $i \in \{1, \ldots, \ell\}$.

Increasing the Hull Dimension

Theorem

The maximal dimension of the Hermitian hull is $\ell_{\text{max}} = \dim C - c_{\text{min}}$, where

$$c_{\text{min}} = \min\left\{\operatorname{rank}\left(G \operatorname{diag}(b_1, \ldots, b_n)\, G^\star\right) : b_i \in \mathbb{F}_q^*\right\}.$$

Theorem [E. Rains, IEEE-TIT **45**, pp. 1827–1832 (1999)]

A code $C = [n, k, d]_{q^2}$ is equivalent to a Hermitian self-orthogonal code iff the puncture code

$$P(C) = \left(C \star C\right)^\perp = \{(c_1\tilde{c}_1^q, \ldots, c_n\tilde{c}_n^q) : \boldsymbol{c}, \tilde{\boldsymbol{c}} \in C\}^\perp$$

contains a word $\boldsymbol{b} \in \mathbb{F}_q^n$ of weight n.

Open problem:

How to efficiently compute c_{min} and find $\boldsymbol{b}$?

More Propagation Rules

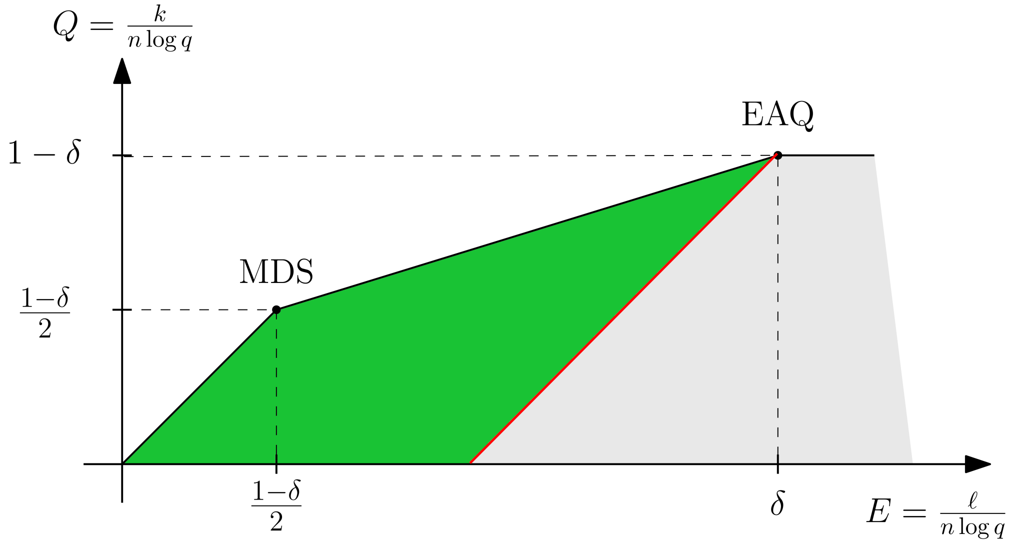
non-trivial propagation rules from [Luo, Ezerman, Grassl, Ling, arXiv:2207.05647]

(6) increasing the dimension of a pure quantum code with $q > 2$ by using extra entanglement, provided that $c \leq n - k - 2$:
$[\![n, k, d; c]\!]_q \longrightarrow [\![n, k+1, d; c+1]\!]_q$

(7) reducing the length by using extra entanglement, provided that $c \leq n - k - 2$:
$[\![n, k, d; c]\!]_q \longrightarrow [\![n-1, k, d; c+1]\!]_q$

(8) shortening a pure quantum code:
$[\![n, k, d; c]\!]_q \longrightarrow [\![n-1, k+1, d-1; c]\!]_q$

Singleton-type Bounds [arXiv:2207.05647]



$(c) \quad \delta > \frac{1}{2}$

Theorem

EAQECC $[\![n, k, d; c]\!]_q$ from the Hermitian or CSS-like construction obey the bound

$$k \leq \min\{n + c + 2 - 2d, n - d + 1\}$$

using classical MDS codes and teleportation, we achieve the point MDS

[M. Grassl, Phys. Rev. A **103** (2021)]

Summary & Outlook

- trace-symplectic self-orthogonal codes yield QECC
- any code $[n, k, d]_{q^2}$ can be used to construct EAQECC
- random codes have a small (Hermitian) hull, i.e., require a lot of entanglement
- goal: find codes with a large Hermitian hull, i.e., requiring little entanglement
- propagation rules allow to utilise more entanglement
  arXiv:2207.05647
- initial online tables for qubits and qutrits at
  `http://eaqecc.codetables.de`
- find new constructions beating the bound $k \leq n + c + 2 - 2d$ for $d > n/2$

Thank you!

Danke! Merci!

Hvala!

Acknowledgment

The 'International Centre for Theory of Quantum Technologies' project (contracts no. 2018/MAB/5 & 2018/MAB/5/AS-1) is carried out within the International Research Agendas Programme of the Foundation for Polish Science co-financed by the European Union from the funds of the Smart Growth Operational Programme, axis IV: Increasing the research potential (Measure 4.3).

This work is partially carried out under IRA Programme, project no. FENG.02.01-IP.05-0006/23, financed by the FENG program 2021-2027, Priority FENG.02, Measure FENG.02.01, with the support of the FNP.

European Funds Smart Growth

Republic of Poland

FNP Foundation for Polish Science

European Union European Regional Development Fund

Uniwersytet Gdański

References

- V. Aggarwal, R. Calderbank. Boolean Functions, Projection Operators, and Quantum Error Correcting Codes. IEEE Transactions on Information Theory, vol. 54, no. 4, 2008, 1700–1707. 10.1109/TIT.2008.917720

- S. E. Anderson, E. Camps-Moreno, H. H. López, G. L. Matthews, D. Ruano, I. Soprunov. Relative Hulls and Quantum Codes, IEEE Transactions on Information Theory, vol. 70, no. 5, 2004, 3190–3201. 10.1109/TIT.2024.3373550

- T. Brun, I. Devetak, M.-H. Hsieh. Correcting quantum errors with entanglement, Science 314, 436 (2006). Science, vol. 314, no. 5798, 2006, 436–439. 10.1126/science.1131563

- R. Calderbank, E. Rains, P. Shor, N. Sloane. Quantum Error Correction Via Codes over $\mathrm{GF}(4)$. IEEE Transactions on Information Theory, vol. 44, no. 4, 1998, 1369–1387. 10.1109/18.681315 quant-ph/9608006.

- R. Calderbank, P. Shor. Good quantum error-correcting codes exist. Physical Review A, vol. 54, no. 2, 1996, 1098–1105. 10.1103/PhysRevA.54.1098 quant-ph/9512032.

- C. Carlet, S. Mesnager, C. Tang, Y. Qi, 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, 2018, 3010–3017. 10.1109/TIT.2018.2789347

References

- C. Galindo, F. Hernando, R. Matsumoto, D. Ruano. Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. Quantum Information Processing, vol. 18, no. 4, 2019, 116. 10.1007/s11128-019-2234-5
- D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. Physical Review A, vol. 54, no. 3, 1996, 1862–1868. 10.1103/PhysRevA.54.1862 quant-ph/9604038.
- M. Grassl, T. Beth, T. Pellizzari. Codes for the Quantum Erasure Channel. Physical Review A, 56(1);33–38, 1997. DOI: 10.1103/PhysRevA.56.33. arXiv:quant-ph/9610042
- M. Grassl. Algebraic quantum codes: linking quantum mechanics and discrete mathematics. International Journal of Computer Mathematics: Computer Systems Theory, vol. 6, no. 4, 2021, 243–250. 10.1080/23799927.2020.1850530, arXiv:2011.06996 [cs.IT]
- M. Grassl. Entanglement-assisted quantum communication beating the quantum Singleton bound. Physical Review A, vol. 103, no. 2, 2021, L020601. 10.1103/PhysRevA.103.L020601 (open access)
- M. Grassl, F. Huber, A. Winter. Entropic proofs of Singleton bounds for quantum error-correcting codes. IEEE Transactions on Information Theory, vol. 68, no. 6, June 2022, 3942–3950. 10.1109/TIT.2022.3149291, arXiv:2010.07902 [quant-ph]

References

- A. Ketkar, A. Klappenecker, S. Kumar and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. IEEE Transactions on Information Theory, vol. 52, no. 11, 2006, 4892–4914. 10.1109/TIT.2006.883612, arXiv:0508070 [quant-ph]
- E. Knill, R. Laflamme. A theory of quantum error-correcting codes. Physical Review A, vol. 55, no. 2, 1997, 900–911. 10.1103/PhysRevA.55.900 quant-ph/9604034.
- D. A. Lidar, T. A. Brun (Eds.). Quantum Error Correction. Cambridge University Press, 2013. ISBN 978-0-52189-787-7.
- G. Luo, M. F. Ezerman, M. Grassl, S. Ling. How much entanglement does a quantum code need? arXiv:2207.05647 [quant-ph]

  Constructing quantum error-correcting codes that require a variable amount of entanglement. Quantum Information Processing, vol. 23, article 4, 2024. 10.1007/s11128-023-04211-x
- E. M. Rains. Nonbinary quantum codes. IEEE Transactions on Information Theory, vol. 45, no. 6, 1999, 1827–1832. 10.1109/18.782103, quant-ph/9703048
- P. Shor. Scheme for reducing decoherence in quantum computer memory. Physical Review A, vol. 52, no. 4, 1995, 2493–2496. 10.1103/PhysRevA.52.R2493
- A. Steane. Error correcting codes in quantum theory. Physical Review Letters, vol. 77, no. 5, 1996, 793–797. 10.1103/PhysRevLett.77.793