Carleton Finite Fields eSeminar
Carleton University

Algebraic Quantum Codes: New challenges for classical coding theory?

Markus Grassl

International Centre for Theory of Quantum Technologies
University Gdansk

markus.grassl@ug.edu.pl
www.codetables.de

17 March 2021 

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

Overview

- a (qu)bit of quantum mechanics
- general quantum error-correcting codes (QECC)
- quantum Singleton bound
- quantum codes from classical codes
- degenerate/impure codes
- quantum MDS codes
- open problems

Classical & Quantum Information

Classical information

often represented by a finite alphabet, e. g., bits 0 and 1

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 pure quantum state:

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

measurement (read-out):

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

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

Classical & Quantum Information

Bit strings

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

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 pure quantum state:

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

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

Classical & Quantum Information

Larger alphabet

messages represented as vectors over a finite field, i. e., $\boldsymbol{x} \in \mathbb{F}_q^n$

Qudit register

basis states:

$$|b_1\rangle \otimes \ldots \otimes |b_n\rangle =: |b_1 \ldots b_n\rangle = |\boldsymbol{b}\rangle \qquad \text{where } b_i \in \mathbb{F}_q$$

general pure quantum state:

$$|\psi\rangle = \sum_{\boldsymbol{x} \in \mathbb{F}_q^n} c_{\boldsymbol{x}} |\boldsymbol{x}\rangle \qquad \text{where } \sum_{\boldsymbol{x} \in \mathbb{F}_q^n} |c_{\boldsymbol{x}}|^2 = 1$$

$\longrightarrow$ normalised vector in $(\mathbb{C}^q)^{\otimes n} \cong \mathbb{C}^{q^n} \cong \mathbb{C}[\mathbb{F}_q^n]$

(isomorphic as vector spaces)

Quantum Operations

Unitary Operations

invertible linear transformations on the space $\mathbb{C}^{q^n}$ preserving the norm and hence total probability

Local Operations

operations on $\mathbb{C}^q \otimes \mathbb{C}^q \otimes \ldots \otimes \mathbb{C}^q$ acting nontrivially only on some of the tensor factors

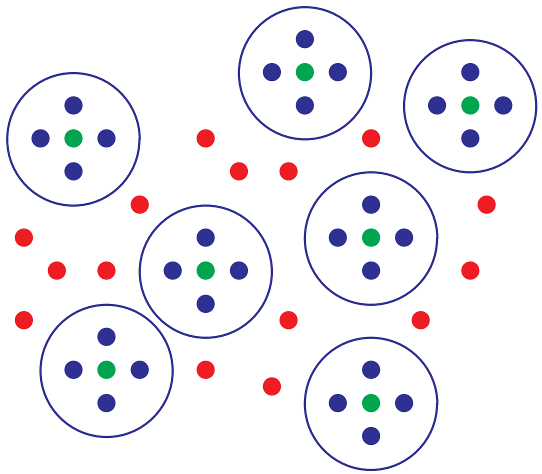
(von Neumann) Measurements

- set of orthogonal projections Π_i, $\Pi_i\Pi_j = \delta_{ij}\Pi_i$, summing to identity
- projection Π_i is selected randomly "by Nature"
- result ("output") is the classical index i
- re-normalized post-measurement state is supported on the image of Π_i
- probability p_i for result i is given by the squared norm of the projection

The Basic Idea of QECC

Classical codes

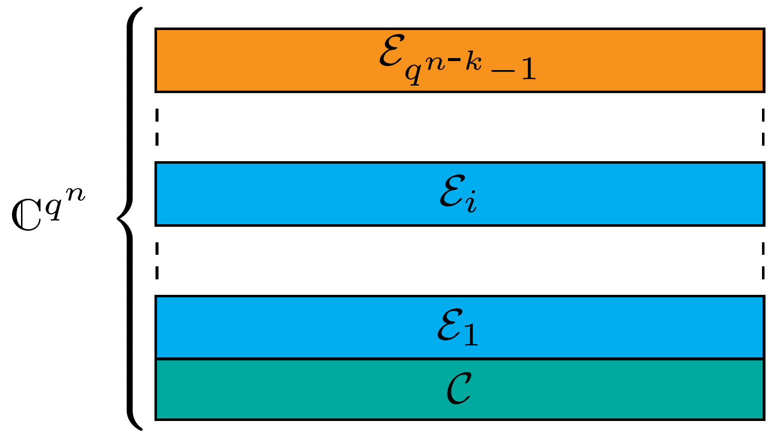
partition of the set of all words of length n over an alphabet of size q



- codewords
- errors of bounded weight
- other errors

Quantum codes

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

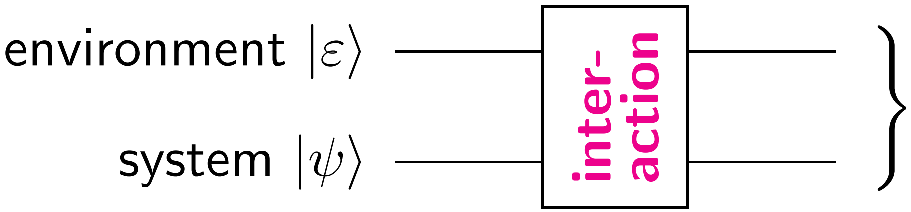


$$\mathcal{H}^{\otimes n} = \mathcal{C} \oplus \mathcal{E}_1 \oplus \ldots \oplus \mathcal{E}_{q^{n-k}-1}$$

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

Interaction System/Environment

"Closed" System



$$= U_{\mathsf{env/sys}}\big(|\varepsilon\rangle|\psi\rangle\big)$$

"Channel"

$$\mathsf{Q}\colon \rho_{\mathsf{in}} := |\psi\rangle\langle\psi| \longmapsto \rho_{\mathsf{out}} := \mathsf{Q}(|\psi\rangle\langle\psi|) := \sum_i E_i \rho_{\mathsf{in}} E_i^\dagger$$

with Kraus operators (error operators) E_i

Local/low correlated errors

- product channel $\mathsf{Q}^{\otimes n}$ where Q is "close" to identity
- Q can be expressed (approximated) with error operators $\tilde{E}_i$ such that each $\tilde{E}_i$ acts on few subsystems, e. g. quantum gates

Knill-Laflamme Conditions

[Knill & Laflamme, Physical Review A **55**, 900–911 (1997)]

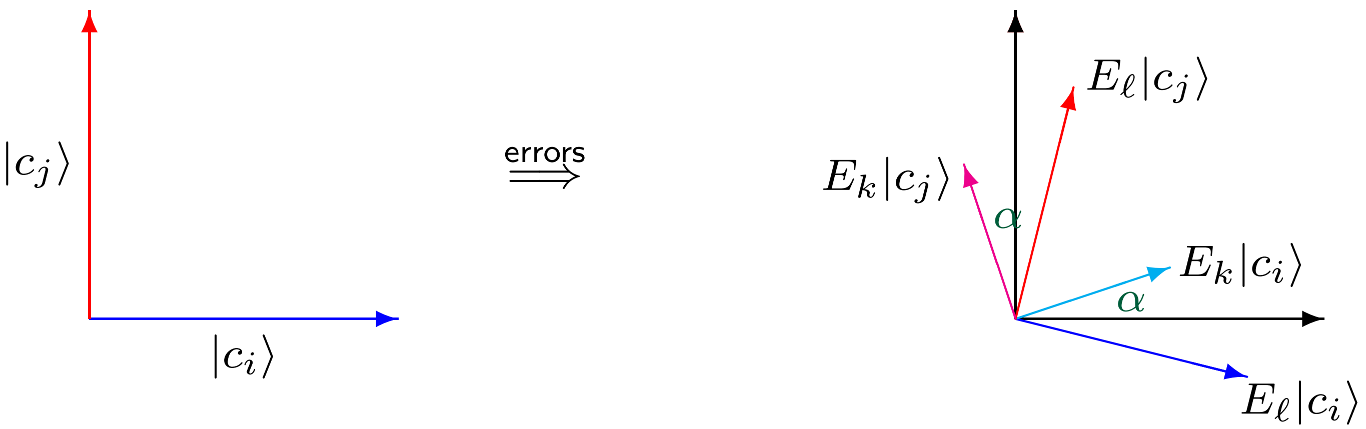
A subspace $\mathcal{C}$ of $\mathcal{H}$ with orthonormal basis $\{|c_1\rangle, \ldots, |c_K\rangle\}$ is an error-correcting code for the error operators $\mathcal{E} = \{E_1, E_2, \ldots\}$, if there exists constants $\alpha_{k,l} \in \mathbb{C}$ such that for all $|c_i\rangle$, $|c_j\rangle$ and for all $E_k, E_l \in \mathcal{E}$:

$$\langle c_i | E_k^\dagger E_l | c_j \rangle = \delta_{i,j} \alpha_{k,l}$$

interpretation:

(i) orthogonal states remain orthogonal under errors

(ii) errors "rotate" all basis states the same way



Linearity of the Knill-Laflamme Conditions

Assume that $\mathcal{C}$ can correct the errors $\mathcal{E} = \{E_1, E_2, \ldots\}$.

New error-operators:

$$A := \sum_k \lambda_k E_k \quad \text{and} \quad B := \sum_l \mu_l E_l$$

$$\begin{aligned}\langle c_i|A^\dagger B|c_j\rangle &= \sum_{k,l} \overline{\lambda_k}\mu_l \langle c_i|E_k^\dagger E_l|c_j\rangle \\ &= \sum_{k,l} \overline{\lambda_k}\mu_l \delta_{i,j}\alpha_{k,l} \\ &= \delta_{i,j} \cdot \alpha'(A,B)\end{aligned}$$

It is sufficient to correct error operators that form a basis of the linear vector space spanned by the operators $\mathcal{E}$.

$\Longrightarrow$ only a finite set of errors ("discretisation")

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 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)
  - many subsystems in the same way (correlated 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)]

Quantum Singleton Bound

classical Singleton bound for $C = (n, K, d)_q$:

$$d \le n - \log_q K + 1$$

quantum Singleton bound for QECC $\mathcal{C} = ((n, K, d))_q$:

$$2d \le n - \log_q K + 2 \tag{1}$$

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

Quantum MDS (QMDS) codes:

quantum codes $\mathcal{C} = ((n, q^{n+2-2d}, d))_q$ with equality in (1)

QMDS Conjecture

QMDS Conjecture:

The length of any QMDS code $\mathcal{C} = ((n, K, d))_q$ with $d \geq 3$ is bounded by $n \leq q^2 + 1$, with the exception of $[\![q^2+2, q^2-4, 4]\!]_q$ for $q = 2^m$, when $n \leq q^2 + 2$.

related results:

[F. Huber & M. Grassl, Quantum, vol. 4, June 2020, 284]

Theorem:

The weight enumerator of any QMDS code equals the weight enumerator of a corresponding classical MDS code.

Theorem:

The length of a QMDS code $\mathcal{C} = ((n, K, d))_q$ with $d \geq 3$ is at most $n \leq q^2 + d - 2$.

Quantum Stabilizer Codes

[Gottesman, PRA **54** (1996); Calderbank, Rains, Shor, & Sloane, IEEE-IT **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-IT **47** (2001)]

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

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

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

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

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:

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

$\mathcal{S}$ 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 symplectic self-orthogonal codes over $\mathbb{F}_q^n \times \mathbb{F}_q^n$.

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

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

special cases:

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

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

$\mathbb{F}_{q^2}$-linear Hermitian codes $C \subset \mathbb{F}_{q^2}^n$ that are self-orthogonal with respect to

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

Quantum Codes from Classical Codes

Hermitian self-orthogonal code

linear code $C = [n, k, d']_{q^2} \le \mathbb{F}_{q^2}^n$ 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., $C \le C^\star = \{\boldsymbol{x} \in \mathbb{F}_{q^2}^n \mid \forall \boldsymbol{y} \in C \colon \boldsymbol{x} \star \boldsymbol{y} = 0\}$

Theorem: (Hermitian construction)

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

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

Then there exists a quantum code $\mathcal{C} = [\![n, n-2k, d]\!]_q$.

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

Impure/Degenerate Codes (I)

recall:

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 $\mathcal{C} = [\![n, n-2k, d]\!]_q$.

Definition: A quantum code is "impure" or "degenerate", when $d > d_{\mathsf{min}}(C^\star)$.

- elements in the classical code C correspond to stabiliser *operators* that act trivially on the complex vectors in the quantum code
  $\Longrightarrow$ we do not have to correct those "errors"
- the stabiliser operators take the role of check equations
  $\Longrightarrow$ a lower weight reduces the complexity of syndrome computation (LDPC)
- ingredients for other types of quantum codes
  (hybrid codes, entanglement-assisted QECC)

Impure/Degenerate Codes (II)

"Coset codes"

Given a self-orthogonal code $C \le C^\star$, we consider the cosets of C in $C^\star$:

$$\{C + \boldsymbol{x}_0, C + \boldsymbol{x}_{\boldsymbol{1}}, \ldots\} \qquad \text{with } \boldsymbol{x}_i \in C^\star$$

information is stored in the codes, i.e., $i \mapsto \boldsymbol{x}_i + C$

- we want the distance between the cosets to be large
- in particular, the covering radius of C should be large

Open Problem:

Construct degenerate quantum codes $[\![n, k, d]\!]_q$ with d larger than (known) pure/non-degenerate codes.

Example: $[\![25, 1, 9]\!]_2$ (upper bound $d \le 10$, $d_{\text{pure}} \ge 8$)

Stabilizer QMDS Codes

quantum Singleton bound for QECC $\mathcal{C} = [\![n, k, d]\!]_q$:

$$2d \leq n - k + 2 \qquad (2)$$

Quantum MDS (QMDS) codes:

quantum codes $\mathcal{C} = [\![n, n + 2 - 2d, d]\!]_q$ with equality in (2)

Hermitian construction

classical MDS code $C \leq C^\star = [n, n - k', d^\star]_{q^2}$ yields $\mathcal{C} = [\![n, n - 2k', d]\!]_q$ with

$$\left.\begin{array}{ll} \text{MDS:} & d \geq d^\star = k' + 1 \\ \text{and by (2):} & d \leq k' + 1 \end{array}\right\} \Longrightarrow \mathcal{C} \text{ is QMDS with } d = k' + 1$$

as $d = d^*$, a QMDS code is "pure" (holds for all QMDS codes)

Propagation Rules

The existence of a quantum code $\mathcal{C} = ((n, K, d))_q$ or $\mathcal{C} = [\![n, k, d]\!]_q$ implies the existence of

- $\mathcal{C}' = ((n, K', d))_q$ with $1 < K' \leq K$ (subcode)
- $\mathcal{C}' = ((n-1, K, d-1))_q$ for $d > 1$ (puncturing)
- $\mathcal{C}' = ((n-1, qK, d-1))_q$ when $\mathcal{C}$ is pure
  $\mathcal{C}' = [\![n-1, k+1, d-1]\!]_q$ when $\mathcal{C}$ is pure (stabilizer shortening)

only the last rule preserves the QMDS property

$\Longrightarrow$ putative QMDS families with $n + k$ constant

[F. Huber & M. Grassl, Quantum, vol. 4, June 2020, 284]

$$[\![6,0,4]\!]_2 \to [\![5,1,3]\!]_2 \to [\![4,2,2]\!]_2 \to [\![3,3,1]\!]_2$$

$$[\![9,3,4]\!]_3 \to [\![8,4,3]\!]_3 \to [\![7,5,2]\!]_3 \to [\![6,6,1]\!]_3$$

Shortening Stabilizer Codes

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

- shortening of classical codes: $C = [n, k, d]_{q^2} \to C_s = [n-1, k-1, d]_{q^2}$
- for stabilizer codes:
  shortening $C^\star \to C_s^\star \Longrightarrow$ puncturing $C \to C_p \Longrightarrow C_p \not\leq (C_p)^\star = C_s^\star$
  existence of $\mathcal{C} = [\![n, k, d]\!]_q$ does not necessarily imply the
  existence of $\mathcal{C} = [\![n-1, k-1, d]\!]_q$

General problem:
How to turn a non-self-orthogonal code into a self-orthogonal one?

Basic idea:

$$\sum_{i=1}^{n} x_i^q y_i \quad \neq 0 \qquad \text{for some } \boldsymbol{x}, \boldsymbol{y} \in C = [n, k, d']_{q^2}$$

Shortening Stabilizer Codes

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

- shortening of classical codes: $C = [n, k, d]_{q^2} \to C_s = [n-1, k-1, d]_{q^2}$
- for stabilizer codes:
  shortening $C^\star \to C_s^\star \implies$ puncturing $C \to C_p \implies C_p \not\leq (C_p)^\star = C_s^\star$
  existence of $\mathcal{C} = [\![n, k, d]\!]_q$ does not necessarily imply the
  existence of $\mathcal{C} = [\![n-1, k-1, d]\!]_q$

General problem:

How to turn a non-self-orthogonal code into a self-orthogonal one?

Basic idea: find $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_q^n$ such that

$$\sum_{i=1}^{n} x_i^q y_i \alpha_i = 0 \qquad \text{for all } \boldsymbol{x}, \boldsymbol{y} \in C = [n, k, d']_{q^2}$$

Puncture Code $P(C)$

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

puncture code of a linear code C over $\mathbb{F}_{q^2}$:

$$P(C) := \left\langle (x_1^q y_1, x_2^q y_2 \ldots, x_n^q y_n) \colon \boldsymbol{x}, \boldsymbol{y} \in C \right\rangle^\perp \cap \mathbb{F}_q^n$$

$$\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in P(C) \Longrightarrow \sum_{i=1}^n (x_i^q y_i)\alpha_i = 0 \quad \text{for all } \boldsymbol{x}, \boldsymbol{y} \in C$$

$$\text{choose } \boldsymbol{\beta} \in \mathbb{F}_{q^2}^n \text{ with } {\beta_i}^{q+1} = \alpha_i \Longrightarrow \sum_{i=1}^n (\beta_i x_i)^q (\beta_i) y_i = 0 \quad \text{for all } \boldsymbol{x}, \boldsymbol{y} \in C$$

$\Longrightarrow$ Hermitian self-orthogonal code

$$\widetilde{C} := \{(\beta_1 x_1, \beta_2 x_2, \ldots, \beta_n x_n) \colon \boldsymbol{x} \in C\} \le \widetilde{C}^\star$$

Shortening Quantum Codes

$\boldsymbol{\alpha} \in P(C)$ with $\mathrm{wgt}(\boldsymbol{\alpha}) = r$:

- delete the positions with $\alpha_i = 0$, resulting in $\widetilde{C}_p$
- $\widetilde{C}_p$ is still a Hermitian self-orthogonal code

$\Longrightarrow$ code $\widetilde{C}_p$ of length $\tilde{n} = r$ with $\widetilde{C}_p \leq \widetilde{C}_p^\star$

Theorem:
Let C be a linear code over $\mathbb{F}_{q^2}$ with $C^\star = [n,k,d]_{q^2}$.
If $\boldsymbol{\alpha} \in P(C)$ with $\mathrm{wgt}(\boldsymbol{\alpha}) = r$, then there exists a stabilizer code $\mathcal{C} = [\![r, \tilde{k} \geq r - 2k, \tilde{d} \geq d]\!]_q$.
In particular:

$$\mathcal{C} = [\![n,k,d]\!]_q \xrightarrow{\boldsymbol{\alpha}} \widetilde{\mathcal{C}} = [\![r, \tilde{k} \geq r-(n-k), \tilde{d} \geq d]\!]_q$$

[Grassl, Beth, & Rötteler, *On Optimal Quantum Codes*, Int. J. Quantum Information **2**, pp. 55–64 (2004)]

The Easy Case: QMDS Codes with $n \le q+1$

[Rötteler, Grassl, and Beth, *On Quantum MDS Codes*, ISIT 2004, p. 356]

- start with a cyclic (constacyclic) MDS code C_1 over $\mathbb{F}_q$ of length $q+1$
- lift the code to $\mathbb{F}_{q^2}$, i. e., $C = C_1 \otimes \mathbb{F}_{q^2}$; but in general, $C \not\leq C^\star$
- however, $P(C)$ is also a cyclic (constacyclic) MDS code which contains words of "all" weights

Theorem:
Quantum MDS codes $\mathcal{C} = [\![n, n-2d+2, d]\!]_q$ exist for all $2 \le n \le q+1$ and $1 \le d \le n/2+1$.

The Harder Case: $q+1 < n \leq q^2+1$

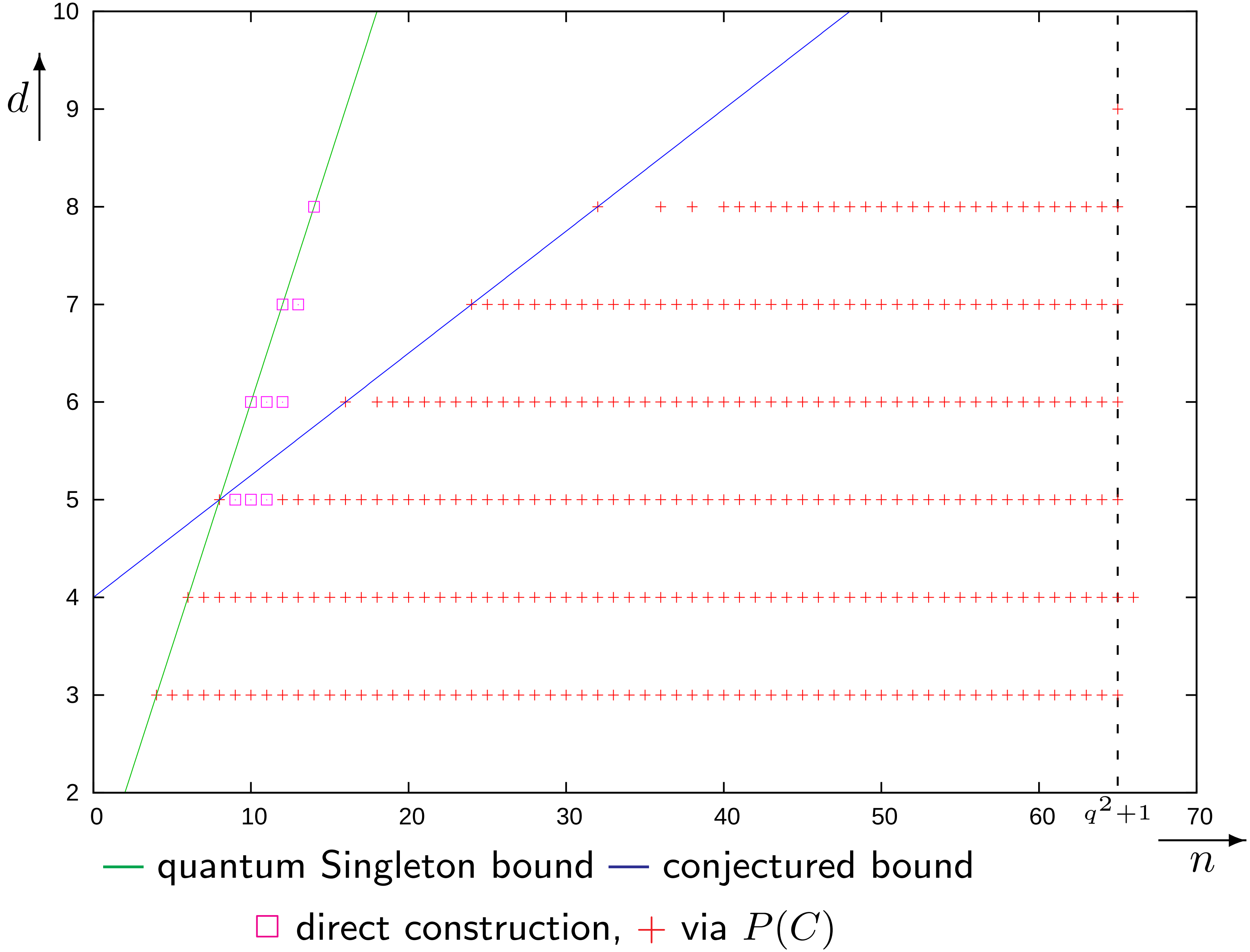
[Grassl & Rötteler, *Quantum MDS Codes over Small Fields*, ISIT 2015, pp. 1104–1108]

- start with a cyclic (constacyclic) MDS code C over $\mathbb{F}_{q^2}$ of length q^2+1
- in general, C is not a Hermitian self-orthogonal code
- $$P(C) = \left\langle (x_i^q y_i)_{i=1}^n : \boldsymbol{x}, \boldsymbol{y} \in C \right\rangle^\perp \cap \mathbb{F}_q^n = \left\langle (x_i y_i^q + x_i^q y_i)_{i=1}^n : \boldsymbol{x}, \boldsymbol{y} \in C \right\rangle^\perp$$
- $P(C)$ is also a cyclic (constacyclic) code, but in general no MDS code
  $\Longrightarrow$ analyse/sample which weights occur in $P(C)$

Open Problem:

Find efficient ways to determine which weights occur in a code.

Computational Results: QMDS Codes for $q = 8$



Special Cases

[Grassl & Rötteler, *Quantum MDS Codes over Small Fields*, ISIT 2015, pp. 1104–1108]

Theorem:
Our construction yields QMDS codes $\mathcal{C} = [\![q^2+1, q^2+3-2d, d]\!]_q$ for all $1 \le d \le q+1$ when q is odd, or when q is even and d is odd.

Remark:
Our construction does not yield a QMDS code $[\![17, 11, 4]\!]_4$, but QMDS codes $[\![4^m+1, 4^m+3-2^{m+1}, 2^m]\!]_{2^m}$ for (at least) $m = 3, 4, 5, 6, 7$.

Theorem:
For $q = 2^m$, there exist QMDS codes $\mathcal{C} = [\![4^m+2, 4^m-4, 4]\!]_{2^m}$.

Proof: (main idea, see [Grassl & Rötteler arXiv:1502.05267 [quant-ph]])
Use the triple-extended Reed-Solomon code and show that $P(C)$ contains a word of weight q^2+2.

Generalized Reed-Solomon Codes

[S. Ball, *Some constructions of quantum MDS codes*, DCC, 2021]

Theorem:

There exists a QMDS code $\mathcal{C} = [\![q^2+1, q^2+1-2d, d]\!]_q$ for all $d \le q+1$ where $d \neq q$.

Proof: Construct a generalized RS code $C = [q^2+1, d-1]_q$ that is contained in its Hermitian dual.

Theorem:

If $k \geq q+1$ then a k-dimensional generalised Reed-Solomon code over $\mathbb{F}_{q^2}$ is not contained in its Hermitian dual.

$\Longrightarrow$ no QMDS codes of distance $d > q+1$

Open Problem:

Construct QMDS codes $\mathcal{C} = [\![q^2+1, q^2+1-2q, q]\!]_q$ for q even.

(The case q odd is covered by [Grassl & Rötteler, ISIT 2015].)

Sporadic QMDS Codes with $d \geq q+2$

QMDS codes from Hermitian self/dual codes:

$[\![n,k,d]\!]_q$	reference
$[\![10,0,6]\!]_3$	Glynn's code
$[\![10,0,6]\!]_4$	Grassl & Rötteler
$[\![14,0,8]\!]_5$	Ball, doubly circulant
$[\![18,0,10]\!]_5$	Ball, doubly circulant
$[\![18,0,10]\!]_7$	Ball, doubly circulant

plus the implied QMDS families

Open Problem:

Construct non-GRS MDS codes that are Hermitian self-orthogonal.

More Open Problems

- Can we find more QMDS codes with $d > q+1$ or even some families?
- Assume that a QMDS code $[\![n,k,d]\!]_q$ exists.
  Can we find QMDS codes $[\![n',k',d']\!]_q$ for all admissible $n' \le n$, $k' \le k$?
- So far, whenever a QMDS codes exists, we can construct one using a Hermitian self-orthogonal MDS code.
  Are there QMDS codes based on non-linear MDS codes (additive or even non-additive) which can not be obtained from linear codes?
- Are there QMDS codes that are not related to classical MDS codes?
- Investigate QMDS codes when q is not a power of a prime.
- Prove/disprove or refine the QMDS conjecture.

Thank you!
Danke! Merci!
Dziekuje!

Acknowledgment

The ‘International Centre for Theory of Quantum Technologies’ project (contract no. 2018/MAB/5) 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).

European Funds Smart Growth

Republic of Poland

FNP Foundation for Polish Science

European Union European Regional Development Fund

UNIWERSYTET GDAŃSKI

References

- S. Ball. Some constructions of quantum MDS codes. Designs, Codes and Cryptography, 2021. DOI: 10.1007/s10623-021-00846-y arXiv:1907.04391
- R. Calderbank, E. Rains, P. Shor, N. Sloane. Quantum Error Correction Via Codes over $\mathrm{GF}(4)$. IEEE Transactions on Information Theory, 44(4):1369–1387, 1998. quant-ph/9608006.
- R. Calderbank, P. Shor. Good quantum error-correcting codes exist. Physical Review A, 54(2):1098–1105, 1996. quant-ph/9512032.
- D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. Physical Review A, 54(3):1862–1868, 1996. 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. Algorithmic aspects of quantum error-correcting codes. in: R. K. Brylinski G. Chen (Eds.). Mathematics of Quantum Computation. Chapman & Hall/CRC, 2002, pp. 223-252. ISBN 978-1-58488-282-4.
- M. Grassl, M. Rötteler. Quantum MDS Codes over Small Fields. Proceedings ISIT 2015, pp. 1104–1108, 2015. arXiv:1502.05267 [quant-ph]

References

- M. Grassl. Algebraic Quantum Codes: Linking Quantum Mechanics and Discrete Mathematics. International Journal of Computer Mathematics: Computer Systems Theory, 2020. DOI: 10.1080/23799927.2020.1850530 arXiv:2011.06996
- F. Huber, M. Grassl. Quantum Codes of Maximal Distance and Highly Entangled Subspaces. Quantum, 4:284, 2019. DOI: 10.22331/q-2020-06-18-284
- A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli. Nonbinary Stabilizer Codes Over Finite Fields. IEEE Transactions on Information Theory, 52(11):4892–4914, 2006. quant-ph/0508070.
- E. Knill, R. Laflamme. A theory of quantum error-correcting codes. Physical Review A, 55(2):900–911, 1997. quant-ph/9604034.
- D. A. Lidar, T. A. Brun (Eds.). Quantum Error Correction. Cambridge University Press, 2013. ISBN 978-0-52189-787-7.
- P. Shor. Scheme for reducing decoherence in quantum computer memory. Physical Review A, 52(4):2493–2496, 1995. DOI: 10.1103/PhysRevA.52.R2493
- A. Steane. Error correcting codes in quantum theory. Physical Review Letters, 77(5):793–797, 1996. DOI: 10.1103/PhysRevLett.77.793