Algebraic Combinatorics and Applications
Universität Bayreuth
Thurnau, April 11-18, 2010

Quantum MDS Codes of Distance Three

Markus Grassl

Centre for Quantum Technologies
National University of Singapore

Markus.Grassl@nus.edu.sg
www.codetables.de

Overview

- A brief introduction to quantum codes
- Symplectic codes
- The puncture code of Rains
- Quantum MDS codes
- Constructing QMDS codes of distance three
- An open conjecture

Overview

- A brief introduction to quantum codes
- Symplectic codes
- The puncture code of Rains
- Quantum MDS codes
- Constructing QMDS codes of distance three
- An open conjecture
  - solved by Aart Blokhuis during Thursday's lunch break

Quantum Information

Quantum-bit (qubit)

basis states:

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

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:

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

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

Quantum Error-Correcting Codes

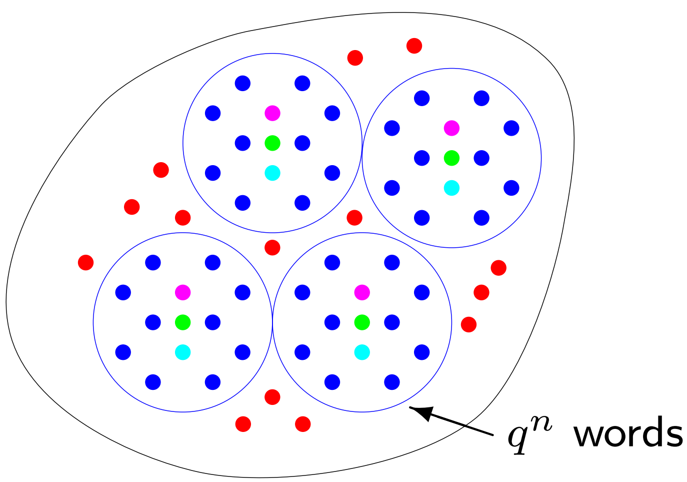
- **subspace** $\mathcal{C}$ of a complex vector space $\mathcal{H} \cong \mathbb{C}^N$
  usually: $\mathcal{H} \cong \mathbb{C}^m \otimes \mathbb{C}^m \otimes \ldots \otimes \mathbb{C}^m =: (\mathbb{C}^m)^{\otimes n}$ "n qudits"
- **errors:** described by linear transformations acting on
  - some of the subsystems (local errors)
  - many subsystems in the same way (correlated errors)
- **notation:** $\mathcal{C} = [\![n, k, d]\!]_q$
  q^k-dimensional subspace $\mathcal{C}$ of $(\mathbb{C}^q)^{\otimes n}$
- **minimum distance** d:
  - detection of errors acting on $d-1$ subsystems
  - correction of errors acting on $\lfloor (d-1)/2 \rfloor$ subsystems
  - correction of erasures acting on $d-1$ known subsystems

Basic Ideas

partitioning of all words

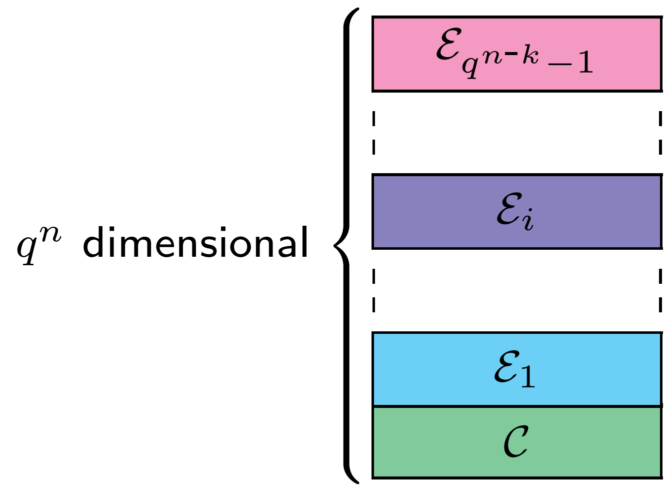
– combinatorics

– (linear) algebra



- codewords
- bounded weight errors
- other errors

orthogonal decomposition



$$(\mathbb{C}^d)^{\otimes n} = \mathcal{H}_{\mathcal{C}} \oplus \mathcal{H}_{\mathcal{E}_1} \oplus \ldots \oplus \mathcal{H}_{\mathcal{E}_i} \oplus \ldots$$

Quantum Error-Correcting Codes

quantum error-correction is "linear"

If the errors A and B can be corrected,
then all errors $\lambda A + \mu B$ $(\lambda, \mu \in \mathbb{C})$ can be corrected.

$\Longrightarrow$ consider only a vector space basis of the errors

Error Basis for Qudits

[A. Ashikhmin & E. Knill, Nonbinary quantum stabilizer codes, IEEE-IT **47**, pp. 3065–3072 (2001)]

$$\mathcal{E} = \{X_\alpha Z_\beta \colon \alpha, \beta \in \mathbb{F}_q\},$$

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

$$X_\alpha := \sum_{x \in \mathbb{F}_q} |x+\alpha\rangle\langle x| \quad \text{for } \alpha \in \mathbb{F}_q$$

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

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 codes over $\mathbb{F}_q^n \times \mathbb{F}_q^n$.

Symplectic Codes

most general:

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

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

in this talk:

$\mathbb{F}_q$-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

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

Symplectic Codes & Stabilizer Codes

Theorem: (Ashikhmin & Knill)
Let C be a symplectic code over $\mathbb{F}_q \times \mathbb{F}_q$ of size q^{n-k} and let
$d := \min\{\mathrm{wgt}(\boldsymbol{c})\colon \boldsymbol{c} \in C^\star \setminus C\}$.
Then there is a stabilizer code $\mathcal{C} = [\![n,k,d]\!]_q$.

Special cases:

- $C = C_1^\perp \times C_2^\perp$ with linear codes C_1, C_2 over $\mathbb{F}_q$, $C_2^\perp \subset C_1$
  Calderbank-Shor-Steane (CSS) codes
- $C = C_1 \times C_1$ with a weakly self-dual (Euclidean) linear code $C_1 \subset C_1^\perp$ over $\mathbb{F}_q$
- $C = \{(\boldsymbol{v},\boldsymbol{w})\colon \boldsymbol{v} + \gamma\boldsymbol{w} \in C_1\}$ where C_1 is a Hermitian self-orthogonal linear code over $\mathbb{F}_{q^2}$ (with some particular $\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$)

Quantum Singleton Bound

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

general bound on the minimum distance of $\mathcal{C} = [\![n,k,d]\!]_q$:

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

Quantum MDS codes:

quantum codes with equality in (1)

Minimum distance of a stabilizer code:

$$\mathrm{d}_{\min}(\mathcal{C}) := \min\{\mathrm{wgt}(\boldsymbol{c})\colon \boldsymbol{c} \in C^\star \setminus C\} \ge \mathrm{d}_{\min}(C^\star), \tag{2}$$

where C is the symplectic code corresponding to $\mathcal{C}$

Note: for QMDS codes we get equality in (2)

Shortening Quantum Codes

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

- shortening of classical codes: $C = [n, k, d] \to C_s = [n-1, k-1, d]$
- for stabilizer codes:
  shortening $C^\star \to C_s^\star \Longrightarrow$ puncturing $C \to C_p \Longrightarrow C_p \not\subset (C_p)^\star = C_s^\star$

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

Basic idea:

$$\sum_{i=1}^{n}(v_i w_i' - v_i' w_i) \quad \neq 0 \quad \text{for some } (\boldsymbol{v}, \boldsymbol{w}), (\boldsymbol{v}', \boldsymbol{w}') \in C$$

Shortening Quantum Codes

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

- shortening of classical codes: $C = [n, k, d] \to C_s = [n-1, k-1, d]$
- for stabilizer codes:
  shortening $C^\star \to C_s^\star \implies$ puncturing $C \to C_p \implies C_p \not\subseteq (C_p)^\star = C_s^\star$

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

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

$$\sum_{i=1}^{n} (v_i w_i' - v_i' w_i)\alpha_i = 0 \qquad \text{for all } (\boldsymbol{v}, \boldsymbol{w}), (\boldsymbol{v}', \boldsymbol{w}') \in C$$

Shortening Quantum Codes

puncture code of an $\mathbb{F}_q$-linear code C over $\mathbb{F}_q \times \mathbb{F}_q$:

$$P(C) := \left\langle \{\boldsymbol{c}, \boldsymbol{c}'\} \colon \boldsymbol{c}, \boldsymbol{c}' \in C \right\rangle^{\perp} \subseteq \mathbb{F}_q^n$$

with the vector valued bilinear form

$$\{(\boldsymbol{v}, \boldsymbol{w}), (\boldsymbol{v}', \boldsymbol{w})\} := (v_i w_i' - v_i' w_i)_{i=1}^n \in \mathbb{F}_q^n$$

$\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in P(C)$

$$\iff \sum_{i=1}^n (v_i w_i' - v_i' w_i)\alpha_i = 0 \quad \text{for all } (\boldsymbol{v}, \boldsymbol{w}), (\boldsymbol{v}', \boldsymbol{w}') \in C$$

$\Longrightarrow$ symplectic code $\widetilde{C} := \{(\boldsymbol{v}, (\alpha_i w_i)_{i=1}^n) \colon (\boldsymbol{v}, \boldsymbol{w}) \in C\}$

Shortening Quantum Codes

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

- delete the positions with $\alpha_i = 0$
- $\tilde{C}_p$ is still a symplectic code

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

Theorem: (Rains)
Let C be a code over $\mathbb{F}_q^n \times \mathbb{F}_q^n$ with $C^\star = (n, q^{n+k}, d)$.
If $\boldsymbol{\alpha} \in P(C)$ with $\operatorname{wgt}(\boldsymbol{\alpha}) = r$, then there is a stabilizer code
$\mathcal{C} = [\![r, \tilde{k} \ge r - (n-k), \tilde{d} \ge d]\!]_q$.
In particular:

$$\mathcal{C} = [\![n, k, d]\!]_q \stackrel{\boldsymbol{\alpha}}{\to} \tilde{\mathcal{C}} = [\![r, \tilde{k} \ge r - (n-k), \tilde{d} \ge d]\!]_q$$

The Easy Case: CSS-like Construction

[Rötteler, Grassl, and Beth, ISIT 2004]

- start with a cyclic (constacyclic) MDS code C_1 over $\mathbb{F}_q$ of length $q+1$
- in general, $C_1^\perp \not\subset C_1$
- compute $P(C)$ for $C = C_1^\perp \times C_1^\perp$:

$$P(C) = \left\langle (c_i d_i)_{i=1}^n : \boldsymbol{c}, \boldsymbol{d} \in C_1^\perp \right\rangle^\perp$$

- α^i, α^j roots of the generator polynomial of C_1
  $\Longrightarrow$ α^{i+j} is a root of the generator polynomial of $P(C)$
- $P(C)$ is also a cyclic (constacyclic) MDS code which contains words of "all" weights

Quantum MDS codes $\mathcal{C} = [\![n, n-2d+2, d]\!]_q$ exist for all $3 \le n \le q+1$ and $1 \le d \le n/2+1$.

The Harder Case: Hermitian-like Construction

- 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
- $$P(C) = \Big\langle (c_i d_i^q)_{i=1}^n : \boldsymbol{c}, \boldsymbol{d} \in C \Big\rangle^\perp \cap \mathbb{F}_q^n$$
  $$= \Big\langle (c_i d_i^q + c_i^q d_i)_{i=1}^n : \boldsymbol{c}, \boldsymbol{d} \in C \Big\rangle^\perp$$
- C is the dual of a code whose generator polynomial has roots α^i, α^j
  $\Longrightarrow \alpha^{i+qj}$ is a root of the generator polynomial of $P(C)$
- $P(C)$ is also a cyclic (constacyclic) code, but in general no MDS code
- known so far [Beth, Grassl, Rötteler], [Klappenecker et al.]
  - QMDS codes exist for some $n > q+1$ and $d \le q+1$, including q^2-1, q^2, q^2+1
  - some other QMDS codes, e. g., derived from Reed-Muller codes

QMDS of Distance Three

q^2-ary simplex code $C = [q^2+1, 2, q^2]_{q^2}$ generated by

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 1 & \omega & \omega^2 & \dots & \omega^{q^2-2} \end{pmatrix} = \begin{pmatrix} \boldsymbol{g}_0 \\ \boldsymbol{g}_1 \end{pmatrix},$$

where ω is a primitive element of $GF(q^2)$

Considered as $\mathbb{F}_q$-linear code generated by

$$\{\boldsymbol{g}_0, \boldsymbol{g}_0' = \alpha\boldsymbol{g}_0, \boldsymbol{g}_1, \boldsymbol{g}_1' = \alpha\boldsymbol{g}_1\}$$

where $\alpha \in GF(q^2) \setminus GF(q)$

The Dual of the Puncture Code

$$\begin{aligned} P(C)^\perp &= \left\langle \boldsymbol{g}_0^{q+1}, \boldsymbol{g}_0 \circ \boldsymbol{g_1}^q + \boldsymbol{g}_0^q \circ \boldsymbol{g}_1, \boldsymbol{g}_0 \circ \alpha^q \boldsymbol{g}_1^q + \boldsymbol{g}_0^q \circ \alpha \boldsymbol{g}_1, \boldsymbol{g}_1^{q+1} \right\rangle \\ &= \left\langle \boldsymbol{f}_0, \quad \boldsymbol{f}_1, \quad \boldsymbol{f}_2, \quad \boldsymbol{f}_3 \right\rangle, \end{aligned}$$

using $\boldsymbol{v} \circ \boldsymbol{w} = (v_1 w_1, v_2 w_2, \ldots, v_n w_n)$ and $\boldsymbol{v}^m = (v_1^m, v_2^m, \ldots, v_n^m)$

We have

$$\begin{aligned} f_0 &= z^{q+1} \\ f_1 &= x^q z + x z^q &&= \mathrm{homogen}_z(x + x^q) &&= \mathrm{homogen}_z(\mathrm{tr}(x)) \\ f_2 &= \alpha^q x^q z + \alpha x z^q &&= \mathrm{homogen}_z(\alpha x + \alpha^q x^q) &&= \mathrm{homogen}_z(\mathrm{tr}(\alpha x)) \\ f_3 &= x^{q+1} \end{aligned}$$

Choosing $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $-\alpha^2 = \beta_1 \alpha + 1$ for some $\beta_1 \in \mathbb{F}_q$ yields

$$f_1^2 + \beta_1 f_1 f_2 + f_2^2 = (4 - \beta_1^2) f_0 f_3.$$

Ovoid Code

Lemma: The dual of the puncture code is an ovoid code, i. e.

$$P(C)^{\perp} = [q^2+1, 4, q^2-q]_q.$$

(see, e. g., Example TF3 in [Calderbank & Kantor, 1986])

This code is a two-weight code with weights $q^2 - q$ and q^2.

$$A_i = \begin{cases} 1 & \text{for } i = 0, \\ (q^3+q)(q-1) & \text{for } i = q^2 - q, \\ (q^2+1)(q-1) & \text{for } i = q^2, \\ 0 & \text{else.} \end{cases}$$

The Dual of the Ovoid Code

Problem: We need the non-zero weights of the puncture code $P(C)$.

The homogenized weight enumerator of $P(C)^\perp$ is

$$W_{P(C)^\perp} = X^{q^2+1} + (q^3+q)(q-1)X^{q+1}Y^{q^2-q} + (q^2+1)(q-1)XY^{q^2}$$

MacWilliams transformation yields

$$\begin{aligned} W_{P(C)}(X,Y) &= q^{-4}\, W_{P(C)^\perp}(X+(q-1)Y, X-Y) \\ &= \sum_{i=0}^{q^2+1} B_i X^{q^2+1-i} Y^i \end{aligned}$$

Conjecture: For $q > 2$, the code $P(C)$ contains words of all weights $w = 4, \ldots, q^2+1$, i.e., $B_i > 0$.

Confirmed for the first 50 prime powers as well as for small weights.

Geometric Proof

THANKS to Aart Blokhuis

Main idea: Show that we can find a linear combination of exactly w points of the ovoid that is zero, corresponding to a word of weight w in the dual code.

- Choose 5 points $Q_0, \ldots, Q_4$ of the ovoid $\mathcal{O}$ in a plane $\mathcal{P}$ (for $q \geq 4$).
- Choose 2 points P_1 and P_2 of the ovoid outside of the plane.
- Any point in the plane can be expressed as linear combination of exactly 4 points Q_i.
- Choose $m = w - 4$ other points and consider their sum S.
  - If $S \in \mathcal{P}$, use exactly 4 other points Q_i to get zero.
  - Otherwise, consider the intersection of $\mathcal{P}$ with the line through S and P_1 (or P_2 if $S = P_1$). Use exactly 3 other points Q_i to get zero.

Conclusions

Theorem:
Quantum MDS codes $[\![n, n-4, 3]\!]_q$ exist for all $4 \le n \le q^2 + 1$ and prime powers $q > 2$.

Extends Ruihu Li & Zongben Xu, On $[\![n, n-4, 3]\!]_q$ Quantum MDS Codes for odd prime power q, arXiv:0906.2509 using different methods.

Further research:

- Find quantum MDS codes of of length $n > q + 1$ and $d > 3$.
- For which q, n, d do QMDS codes $[\![n, n-2d+2, d]\!]_q$ exist?
- Characterize $P(C)$ for classes of codes.
- Develop general methods to determine the non-zero coefficients of the weight distribution.

References

[1] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Transactions on Information Theory* **47**, pp. 3065–3072 (2001), http://arXiv.org/abs/quant-ph/0005008

[2] M. Grassl, Th. Beth, and M. Rötteler, "On Optimal Quantum Codes," *International Journal of Quantum Information* **2**, pp. 55–64 (2004), http://arXiv.org/abs/quant-ph/0312164

[3] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Transactions on Information Theory* **52**, pp. 4892–4914 (2006), http://arXiv.org/abs/quant-ph/0508070

[4] R. Li and Z. Xu, "On $[\![n, n-4, 3]\!]_q$ Quantum MDS Codes for odd prime power q," http://arXiv.org/abs/0906.2509

[5] E. Rains, "Nonbinary Quantum Codes," *IEEE Transactions on Information Theory* **45**, pp. 1827–1832 (1999), http://arXiv.org/abs/quant-ph/9703048

[6] M. Rötteler, M. Grassl, and Th. Beth, "On Quantum MDS Codes," Proceedings 2004 IEEE International Symposium on Information Theory (ISIT 2004), p. 356.