ERATO *Conference on*
QUANTUM INFORMATION SCIENCE 2003

September 4–6, 2003
Niijima-kaikan
Kyoto, Japan

On Optimal Quantum Codes

Markus Grassl,
Thomas Beth, and Martin Rötteler

Arbeitsgruppe *Quantum Computing*
Institut für Algorithmen und Kognitive Systeme
Universität Karlsruhe
Germany

IQC Institute *for* Quantum Computing
University of Waterloo
Canada

Overview

- active quantum error-correcting codes (QECCs)
- bounds on QECCs
- non-binary QECCs
- quantum MDS codes
- shortening quantum codes
- summary & outlook

Quantum Error-Correcting Codes (QECCs)

- notation: $\mathcal{C} = [\![n, k, d]\!]_q$
- input: quantum state $|\psi\rangle_{\text{in}} \in \mathcal{H}^{\otimes k}$, $\dim \mathcal{H} = q$
- encoding: quantum state $|\underline{\psi}\rangle_{\text{enc}} \in \mathcal{H}^{\otimes n}$
- minimum distance d:

$\Longrightarrow$ correction of up to $t = \lfloor (d-1)/2 \rfloor$ errors, i. e.,
arbitrary quantum operations on an arbitrary set of $\leq t$ subsystems

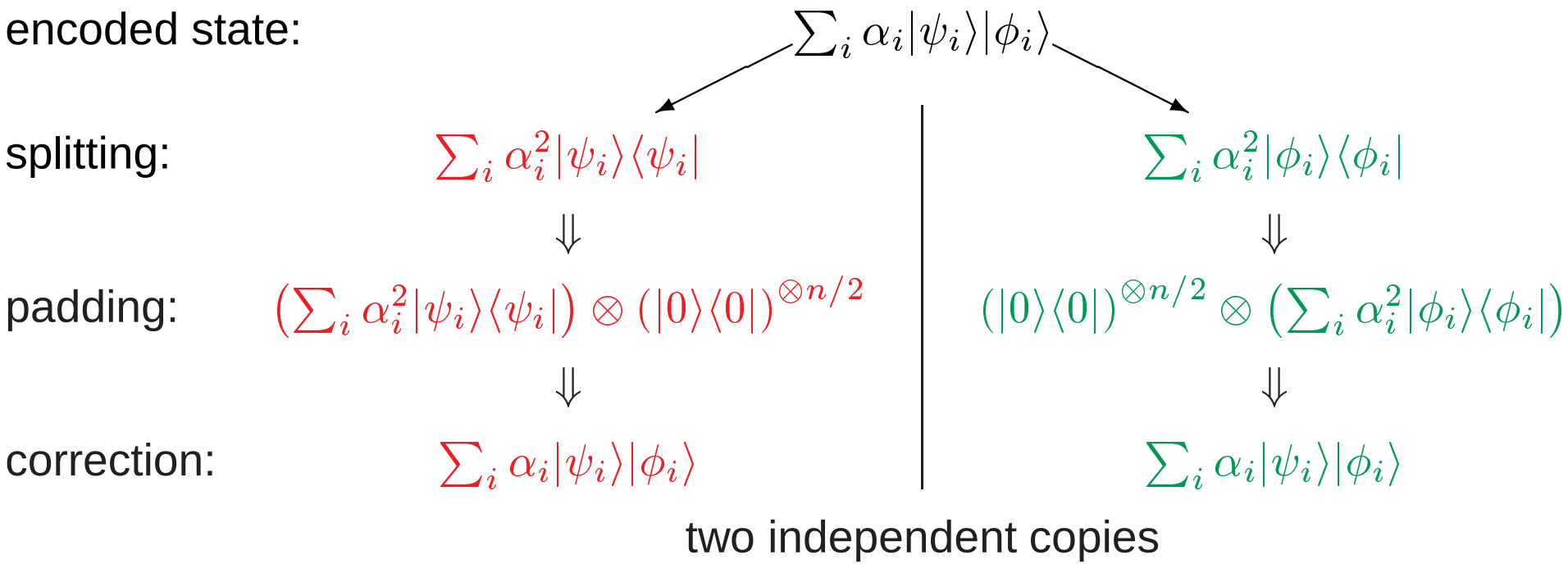
$\Longrightarrow$ correction of up to $d-1$ erasures, i. e.,
arbitrary quantum operations on a known set of $\leq d-1$ subsystems

Central Problem:

relations between the parameters n, k, and d (for finite n, k and for $n \to \infty$)

No-Cloning Bound

Assumption: $\mathcal{C} = [\![n, 1, n/2 + 1]\!]$ exists



$\Longrightarrow$ no-cloning bound: $d - 1 < n/2$

Quantum Singleton Bound

(E. Rains, Nonbinary Quantum Codes, quant-ph/9703048)

Let $\mathcal{C} = [\![n, k, d]\!]_q$ be a quantum error-correcting code. Then

$$k + 2d \leq n + 2. \tag{1}$$

If equality holds in (1) then $\mathcal{C}$ is pure and $\mathcal{C}$ is a **quantum MDS code**.

- bound is valid for arbitrary $q := \dim \mathcal{H}$
- for QECCs over qubits ($q = 2$), the bound is almost never achieved
- QECCs $[\![5, 1, 3]\!]_p$ exist for all primes p [Chau], [Rains]
- QECCs $[\![6, 2, 3]\!]_p$ and $[\![7, 3, 3]\!]_p$ exist for all primes $p \geq 3$ [Feng]
- MDS codes exist *for sufficiently large primes* p [Werner/Schlingemann]

Bounds on Qubit-QECCs

$n\backslash k$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
3	2	1	1	1											
4	2	2	2	1	1										
5	3	3	2	1	1	1									
6	4	3	2	2	2	1	1								
7	3	3	2	2	2	1	1	1							
8	4	3	3	3	2	2	2	1	1						
9	4	3	3	3	2	2	2	1	1	1					
10	4	4	4	3	3	2	2	2	2	1	1				
11	5	5	4	3	3	3	2	2	2	1	1	1			
12	6	5	4	4	4	3	3	2	2	2	2	1	1		
13	5	5	4	4	4	3–4	3	3	2	2	2	1	1	1	
14	6	5	5	4–5	4	4	4	3	3	2	2	2	2	1	1

Non-Binary Quantum Codes

General Theory:

- Knill [1996], Klappenecker & Rötteler [2000]: Clifford codes
- Rains [1997], Hamada [2002]: codes for prime dimension
- Ashikhmin & Knill [2000]: codes for prime power dimension (CSS construction, $GF(q)$-linear codes, additive codes)

Specific Constructions:

- Aharonov & Ben-Or [1996]: polynomial codes with $k = 1$
- Chau [1997]: QECCs $[\![9, 1, 3]\!]_d$ and $[\![5, 1, 3]\!]_d$ for arbitrary d
- Bierbrauer [1998]: $GF(q)$-linear codes

Classical MDS Codes

Singleton Bound: $d \leq n - k + 1$ for all codes $C = [n, k, d]$

Some Constructions:

- Reed-Solomon (RS) codes of length $q - 1$ over $GF(q)$ and $1 \leq k \leq q - 1$
- extended RS codes of length q over $GF(q)$ and $1 \leq k \leq q$

Properties:

- the dual code is also an MDS code
- shortening of $C = [n, n - d + 1, d]$ yields $C^s = [n - 1, n - d, d]$
- puncturing of $C = [n, n - d + 1, d]$ yields $C^p = [n - 1, n - d + 1, d - 1]$
- $C = [n, n - d + 1, d]$ contains words of Hamming weight 0, $d, d + 1, \ldots n$

Quantum MDS Codes of Length q

(cf. also D. P. Chi, Workshop on Quantum Computation & Quantum Information, Seoul, 2001)

extended RS code $C^{(q,\mu)} = [q, \mu+1, q-\mu]$ over $GF(q)$ generated by

$$G^{(q,\mu)} := \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ \alpha^0 & \alpha^1 & \alpha^2 & \dots & \alpha^{q-2} & 0 \\ \alpha^0 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(q-2)} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha^0 & \alpha^\mu & \alpha^{2\mu} & \dots & \alpha^{\mu(q-2)} & 0 \end{pmatrix}$$

for $0 \leq \mu \leq q/2$:
$C^{(q,\mu)}$ is contained in its dual, i. e., $C^{(q,\mu)} \subseteq (C^{(q,\mu)})^\perp = [q, q-\mu-1, \mu+2]$

$\Longrightarrow$ CSS construction yields

$$\mathcal{C}^{(q,\mu)} = [\![q, q-2\mu-2, \mu+2]\!]_q$$

Quantum MDS Codes of Length q^2

Hermitian inner product on $GF(q^2)^n$:

$$\boldsymbol{v} * \boldsymbol{w} := \sum_{i=1}^{n} v_i \overline{w_i} = \sum_{i=1}^{n} v_i w_i^q \tag{2}$$

extended RS code $C^{(q^2,\mu)} = [q^2, \mu+1, q^2-\mu]$ over $GF(q^2)$

for $0 \leq \mu \leq q-2$:
$C^{(q^2,\mu)}$ is contained in its dual with respect to (2), i. e.,

$$C^{(q^2,\mu)} = [q^2, \mu+1, q^2-\mu] \subseteq (C^{(q^2,\mu)})^* = [q^2, q^2-\mu-1, \mu+2]$$

$\Longrightarrow$ stabilizer construction yields

$$\mathcal{C}^{(q^2,\mu)} = [\![q^2, q^2-2\mu-2, \mu+2]\!]_q$$

Shortening Quantum Codes (I)

(E. Rains, Nonbinary Quantum Codes, quant-ph/9703048)

Stabilizer Codes:

symplectic inner product on $GF(q)^n \times GF(q)^n$:

$$(\boldsymbol{v}, \boldsymbol{w}) \star (\boldsymbol{v}', \boldsymbol{w}') := \mathrm{Tr}(\boldsymbol{v} \cdot \boldsymbol{w}' - \boldsymbol{v}' \cdot \boldsymbol{w}) = \mathrm{Tr}(\sum_{i=1}^{n} v_i w_i' - v_i' w_i) \qquad (3)$$

classical code C with $C \subseteq C^\star$, in particular

$$\mathrm{Tr}(\boldsymbol{v} \cdot \boldsymbol{w}' - \boldsymbol{v}' \cdot \boldsymbol{w}) = 0 \qquad \text{for all } (\boldsymbol{v}, \boldsymbol{w}), (\boldsymbol{v}', \boldsymbol{w}') \in C$$

Basic Idea: find $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, some $\alpha_i = 0$, with

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

Shortening Quantum Codes (II)

vector valued bilinear form:

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

puncture code of a $GF(q)$-linear code C over $GF(q) \times GF(q)$:

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

$\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in P(C)$ with $\operatorname{wgt} \boldsymbol{\alpha} = r$
$\Longrightarrow$ code $\tilde{C}$ of length $\tilde{n} = r$ with $\tilde{C} \subseteq \tilde{C}^{\star}$

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

The Puncture Code

1. for $\mathcal{C}^{(q,\mu)} = [\![q, q-2\mu-2, \mu+2]\!]_q$:

   $P(C) = [q, q-2\mu-1, 2\mu+2]$ is an MDS code

   $\Longrightarrow$ $P(C)$ contains words of weight $r = 2\mu+2, \ldots, q$

   $\Longrightarrow$ quantum MDS codes

   $$\mathcal{C} = [\![n, n-2d+2, d]\!]_q \qquad \text{for } 2 \leq n \leq q,\ 1 \leq d \leq n/2+1$$

2. for $\mathcal{C}^{(q,\mu)} = [\![q^2, q^2-2\mu-2, \mu+2]\!]_q$:

   no closed formula for $P(C)$, but

   explicit computation of $P(C)$ shows that $P(C)$ contains words of many different weights

   $\Longrightarrow$ quantum MDS codes

   $$\mathcal{C} = [\![n, n-2d+2, d]\!]_q \qquad \text{for } \textit{some } 2 \leq n \leq q^2,\ 1 \leq d \leq n/2+1,\ d \leq q$$

Results (I)

q	codes of length q^2	$P(C)$	weights in $P(C)$
2	$[\![4,2,2]\!]_2$	$[4,3,2]_2$	$2,4$
3	$[\![9,7,2]\!]_3$	$[9,8,2]_3$	2–9
	$[\![9,5,3]\!]_3$	$[9,5,4]_3$	4–9
4	$[\![16,14,2]\!]_4$	$[16,15,2]_4$	2–16
	$[\![16,12,3]\!]_4$	$[16,12,4]_4$	4–16
	$[\![16,10,4]\!]_4$	$[16,17,8]_4$	$8,10,12,14,16$
5	$[\![25,23,2]\!]_5$	$[25,24,2]_5$	2–25
	$[\![25,21,3]\!]_5$	$[25,21,4]_5$	4–25
	$[\![25,19,4]\!]_5$	$[25,16,6]_5$	$6,8$–25
	$[\![25,17,5]\!]_5$	$[25,9,12]_5$	12–25

Results (II)

q	codes of length q^2	$P(C)$	weights in $P(C)^a$
7	$[\![49, 47, 2]\!]_7$	$[49, 48, 2]_7$	2–49
	$[\![49, 45, 3]\!]_7$	$[49, 45, 4]_7$	4–49
	$[\![49, 43, 4]\!]_7$	$[49, 40, 6]_7$	6–49
	$[\![49, 41, 5]\!]_7$	$[49, 33, 8]_7$	8, 12–19, 25–49
	$[\![49, 39, 6]\!]_7$	$[49, 24, 16]_7$	16, 18–49
	$[\![49, 37, 7]\!]_7$	$[49, 13, 24]_7$	24, 25, 28, 30–49

[a] For the last three codes in the table, the weights listed are obtained by random sampling since the complete weight distribution is not known. It is likely that even more shortenings are possible.

Summary & Outlook

Main Result:

two new families of quantum MDS codes for qudits:

- quantum MDS codes of length $n \leq q$ for all possible parameters
- quantum MDS codes of length $n \leq q^2$ with $d \leq q$ for *some* n

Outlook:

- general structure of $P(C)$
- codes of length $\tilde{n}$ when there are no words in $P(C)$ of weight $\tilde{n}$
- codes of length $n > q^2$ for qudits of dimension q
  (constructions for $n = q^2 + 1$ already found)