Second International Conference on Quantum Error Correction University of Southern California, Los Angeles, USA

December 5–9, 2011

Quantum Error-Correcting Codes by Concatenation

Markus Grassl

joint work with Bei Zeng



National University of Singapore

Centre for Quantum Technologies National University of Singapore Singapore

Why Bei isn't here



Jonathan, November 24, 2011

Overview

- Shor's nine-qubit code revisited
- The code $\llbracket 25, 1, 9 \rrbracket$
- Concatenated graph codes
- Generalized concatenated quantum codes
- Codes for the Amplitude Damping (AD) channel
- Conclusions

Shor's Nine-Qubit Code Revisited

Bit-flip code: $|0\rangle \mapsto |000\rangle$, $|1\rangle \mapsto |111\rangle$.Phase-flip code: $|0\rangle \mapsto |+++\rangle$, $|1\rangle \mapsto |---\rangle$.

Effect of single-qubit errors on the bit-flip code:

- $\bullet~X\mbox{-errors}$ change the basis states, but can be corrected
- Z-errors at any of the three positions:

- \implies Bit-flip code & error correction convert the channel into a phase-error channel
- \implies Concatenation of bit-flip code and phase-flip code yields $\llbracket 9, 1, 3 \rrbracket$

The Code $\llbracket 25, 1, 9 \rrbracket$

- The best single-error correcting code is $\mathcal{C}_0 = \llbracket 5, 1, 3 \rrbracket$
- Re-encoding each of the 5 qubits with C_0 yields $C = \llbracket 5^2, 1, 3^2 \rrbracket = \llbracket 25, 1, 9 \rrbracket$
- The code ${\mathcal C}$ is a subspace of five copies of $[\![5,1,3]\!]$
- The stabilizer of C is generated by five copies of the stabilizer of C_0 and an encoded version of the stabilizer of C_0
- The code \mathcal{C} is degenerate
- *m*-fold self-concatenation of $[\![n, 1, d]\!]$ yields $[\![n^m, 1, d^m]\!]$

Level-decoding of $\llbracket 25, 1, 9 \rrbracket$

The code corrects up to t = 4 errors (t < d/2)

different error patterns:



- errror correction on both levels: corrects a), but fails for b)
- error detection on lowest level, error correction on higer level: corrects b), but fails for a)
- \implies optimal decoding must pass information between the levels

Overview

- Shor's nine-qubit code revisited
- The code $\llbracket 25, 1, 9 \rrbracket$
- ⇒ Concatenated graph codes
 [Beigi, Chuang, Grassl, Shor & Zeng, Graph Concatenation for QECC,
 JMP 52 (2011), arXiv:0910.4129]
 - Generalized concatenated quantum codes
 - Codes for the Amplitude Damping (AD) channel
 - Conclusions

Canonical Basis of a Stabilizer Code

- fix logical operators \overline{X}_i and \overline{Z}_ℓ
- the stabilizer ${\mathcal S}$ and the logical operators \overline{Z}_ℓ mutually commute
- the logical state $|\overline{00\ldots0}\rangle$ is a stabilizer state
- define the (logical) basis states as

$$|\overline{i_1 i_2 \dots i_k}\rangle = \overline{X}_1^{i_1} \cdots \overline{X}_k^{i_k} |\overline{00 \dots 0}\rangle$$

in terms of a classical code over a finite field:

- the logical state $|\overline{00\dots 0}\rangle$ corresponds to a self-dual code \mathcal{C}_0
- the basis states $|\overline{i_1 i_2 \dots i_k}\rangle$ correspond to *cosets* of \mathcal{C}_0
- $\bullet\,$ for a stabilizer code, the union of the cosets is an additive code \mathcal{C}^*

Graphical Quantum Codes

[D. Schlingemann & R. F. Werner: QECC associated with graphs, PRA **65** (2002), quant-ph/0012111] [Grassl, Klappenecker & Rötteler: Graphs, Quadratic Forms, & QECC, ISIT 2002, quant-ph/0703112]

Basic idea

- a classical symplectic self-dual code defines a single quantum state $C_0 = [\![n,0,d]\!]_q$
- the standard form of the stabilizer matrix is (I|A)
- $\bullet\,$ the generators have exactly one tensor factor X
- self-duality implies that A is symmetric
- A can be considered as adjacency matrix of a graph with n vertices
- logical X-operators give rise to more quantum states in the code $\mathcal{C} = [\![n,k,d']\!]_q$
- use additionally k input vectices

Graphical Representation of $\llbracket 6, 2, 3 \rrbracket_3$

,												、
(1	0	0	0	0	0	0	0	0	1	0	2
	0	1	0	0	0	0	0	0	1	2	2	2
	0	0	1	0	0	0	0	1	0	2	0	1
	0	0	0	1	0	0	1	2	2	0	0	0
	0	0	0	0	1	0	0	2	0	0	0	2
	0	0	0	0	0	1	2	2	1	0	2	0
-	0	0	0	0	0	0	1	0	1	1	0	0
	0	0	0	0	0	0	1	0	0	0	2	1 /
•												

stabilizer & logical X-operators



graphical representation

Encoder based on Graphical Representation

[M. Grassl, Variations on Encoding Circuits for Stabilizer Quantum Codes, LNCS 6639, pp. 142–158, 2011]



Encoder based on Graphical Representation



Concatenation of Graph Codes

[Beigi, Chuang, Grassl, Shor & Zeng, Graph Concatenation for QECC, JMP 52 (2011), arXiv:0910.4129]

 \bullet self-concatenation of $[\![5,1,3]\!]$



- measure the five auxillary nodes in X-bases
- *X*-measurement corresponds to sequence of local complementations
 ⇒ many different choices









General Concatenation Rule

(for qubit codes; see paper for qudit codes)

- Any edge connecting an input vertex with an auxiilary vertex is replaced by a set of edges connecting the input vertex with all neighbors of the auxillary vertex.
- Any edge between two auxiliary vertices A and B is replaced by a complete bipartite graph connecting any neighbor of A with all neighbors of B.



Overview

- Shor's nine-qubit code revisited
- The code $\llbracket 25, 1, 9 \rrbracket$
- Concatenated graph codes
- ⇒ Generalized concatenated quantum codes [Grassl, Shor, Smith, Smolin & Zeng, PRA 79 (2009), arXiv:0901.1319] [Grassl, Shor & Zeng, ISIT 2009, arXiv:0905.0428]
 - Codes for the Amplitude Damping (AD) channel
 - Conclusions

Stabilizer Codes

- stabilizer group $S = \langle S_1, \dots, S_{n-k} \rangle$ generated by n k mutually commuting tensor products of (generalized) Pauli matrices
- $C = \llbracket n, k, d \rrbracket$ is a common eigenspace of the S_i
- orthogonal decomposition of the vector space $\mathcal{H}^{\otimes n}$ into joint eigenspaces



- labelling of the spaces by the eigenvalues of the S_i
- errors that change the eigenvalues can be detected

Variations on $\llbracket 5, 1, 3 \rrbracket_2$

decomposition of $(\mathbb{C}^2)^{\otimes 5} = B^{(0)} = ((5, 2^5, 1))_2$ into 16 mutually orthogonal quantum codes $B_i^{(1)} = ((5, 2, 3))_2$

$$\langle ^{7}0 \rangle$$

$$\langle ^{7}1 \rangle$$

 $B_0^{(1)} B_1^{(1)} B_2^{(1)} B_3^{(1)} B_4^{(1)} B_5^{(1)} B_6^{(1)} B_7^{(1)} B_8^{(1)} B_9^{(1)} B_{10}^{(1)} B_{11}^{(1)} B_{12}^{(1)} B_{13}^{(1)} B_{14}^{(1)} B_{15}^{(1)}$ new basis: $\{|i; j\rangle : i = 0, \dots, 15; j = 0, 1\}$

Construction of $((15, 2^7, 3))_2$

- basis $\{|i; j\rangle : i = 0, \dots, 15; j = 0, 1\}$ of $B^{(0)} = ((5, 2^5, 1))_2$
 - states $|i;\mathbf{0}\rangle$ and $|i;\mathbf{1}\rangle$ are in the code $B_i^{(1)} = ((5,2,3))_2$
 - for $i \neq i'$, some states $|i;j\rangle$ and $|i';j'\rangle$ have distance < 3
- protect the quantum number i
- a classical code of distance three suffices for this purpose
- generalized concatenated QECC $(\!(3\times 5, 16\times 2^3, 3)\!)$ with basis

 $\{|i; j_1\rangle | i; j_2\rangle | i; j_2\rangle : i = 0, \dots, 15; \ j_1 = 0, 1; j_2 = 0, 1; j_3 = 0, 1\}$

• normalizer code is a generalized concatenated code with

- inner codes
$$\mathcal{B}^{(0)} = (5, 2^{10}, 1)_4$$
 and $\mathcal{B}^{(1)} = (5, 2^6, 3)_4$

– outer codes $\mathcal{A}_1=[3,1,3]_{16}$ and $\mathcal{A}_2=[3,3,1]_{2^6}$

Encoding of $((15, 2^7, 3))_2$

encoder for the nested codes $((5, 2, 3))_2 \le ((5, 2^5, 1))_2$



Encoding of
$$((15, 2^7, 3))_2$$

generalized concatenated encoder



A New Qubit Non-Stabilizer Code

[Grassl, Shor, Smith, Smolin & Zeng, PRA 79 (2009), arXiv:0901.1319]

- the classical outer code can be any code, not only linear codes
- from the Hamming code $[18, 16, 3]_{17}$ over GF(17) one can derive a code

 $\mathcal{A} = (18, \lceil 16^{18}/17^2 \rceil, 3)_{16} \qquad [\mathsf{Dumer, Handbook CT}]$

- the resulting GCQC has parameters $((90, 2^{81.825}, 3))_2$
- the quantum Hamming bound reads $K(1+3n) \leq 2^n$, here $K < 2^{81.918}$
- the best stabilizer code has parameters $[\![90,81,3]\!]_2$
- the linear programming bound yields $K < 2^{81.879}$
- our code encodes 0.825 qubits more than any stabilizer code and at most 0.054 qubits less than the best possible code

A New Qutrit Non-Stabilizer Code

[Grassl, Shor, Smith, Smolin & Zeng, PRA 79 (2009), arXiv:0901.1319]

- inner code $B^{(0)} = \bigoplus_{i=0}^{80} B_i^{(1)}$ with each $B^{(1)} = ((10, 3^6, 3))_3$
- from the Hamming code $[84, 82, 3]_{83}$ over GF(83) one can derive a code

 $\mathcal{A} = (84, \lceil 81^{84}/83^2 \rceil, 3)_{81}$ [Dumer, Handbook CT]

- the resulting GCQC has parameters $((840, 3^{831.955}, 3))_2$
- the quantum Hamming bound reads $K(1+8n) \leq 3^n$, here $K < 3^{831.979}$
- the best stabilizer code has parameters $[\![840, 831, 3]\!]_3$
- the linear programming bound yields $K < 3^{831.976}$
- our code encodes 0.955 qutrits more than any stabilizer code and at most 0.021 qutrits less than the best possible code
- first non-stabilizer qutrit code better than any stabilizer code

A New Stabilizer Code $[\![36, 26, 4]\!]_2$

[Grassl, Shor & Zeng, ISIT 2009, arXiv:0905.0428]

inner codes: chain of nested stabilizer codes

$$B^{(0)} = \llbracket 6, 6, \mathbf{1} \rrbracket_2 \supset B^{(1)} = \llbracket 6, 4, \mathbf{2} \rrbracket_2 \supset B^{(2)} = \llbracket 6, 0, \mathbf{4} \rrbracket_2.$$

classical outer codes

$$\mathcal{A}_1 = [6, 3, 4]_{2^{6-4}}, \qquad \mathcal{A}_2 = [6, 5, 2]_{2^{4-0}}, \qquad \mathcal{A}_3 = [6, 6, 1]_{2^6}$$

dimension

$$|\mathcal{A}_1| \times |\mathcal{A}_2| = (2^2)^3 (2^4)^5 = 2^6 2^{20} = 2^{26}$$

minimum distance

$$d \ge \min\{\mathbf{1} \times 4, \mathbf{2} \times 2, \mathbf{4} \times 1\} = 4$$

previously, only a code $[\![36, 26, 3]\!]_2$ was known [http://www.codetables.de]

Varying Inner Codes

[Dettmar et al., Modified Generalized Concatenated Codes ..., IEEE-IT 41:1499–1503 (1995)]

inner codes: chain of nested stabilizer codes

$$B_j^{(0)} = \llbracket n_j, n_j, 1 \rrbracket_2 \supset B_j^{(1)} = \llbracket n_j, n_j - 6, 3 \rrbracket_2$$

for $n_j \in \{7, \dots, 17\} \cup \{21\}$

classical outer codes

$$\mathcal{A}_1 = [65, 63, 3]_{2^6}, \qquad \mathcal{A}_2 = [65, 65, 1]_{2^{2n_j - 6}}$$

generalized concatenated quantum codes

$$\llbracket n, n-12, 3 \rrbracket_2$$
 with $n = \sum_{j=1}^{65} n_j \in \{455, \dots, 1361\} \cup \{1365\}$

direct and simple construction of quantum codes with different length

A New Distance-Three Qubit Code

[Grassl, Shor & Zeng, ISIT 2009, arXiv:0905.0428]

inner codes: chain of nested stabilizer codes

$$B^{(0)} = [\![8, 8, 1]\!]_2 \supset B^{(1)} = [\![8, 6, 2]\!]_2 \supset B^{(2)} = [\![8, 3, 3]\!]_2.$$

classical outer codes

$$\mathcal{A}_1 = (6, 164, 3)_{2^{8-6}}, \qquad \mathcal{A}_2 = [6, 5, 2]_{2^{6-3}}, \qquad \mathcal{A}_3 = [6, 6, 1]_{2^{8+3}}$$

dimension

$$|\mathcal{A}_1| \times |\mathcal{A}_2| \times \dim(B^{(2)})^6 = 164 \times (2^3)^5 \times 2^{3 \times 6} \approx 2^{40.358}$$

minimum distance

$$d \ge \min\{1 \times 3, 2 \times 2, 3 \times 1\} = 3$$

LP bound $K < 2^{40.791}$, hence the best stabilizer code is $[\![48, 40, 3]\!]_2$

Overview

- Shor's nine-qubit code revisited
- The code $\llbracket 25, 1, 9 \rrbracket$
- Concatenated graph codes
- Generalized concatenated quantum codes
- ⇒ Codes for the Amplitude Damping (AD) channel
 [Duan, Grassl, Ji & Zeng, Multi-Error-Correcting Amplitude Damping
 Codes, ISIT 2010, arXiv:1001.2356]
 - Conclusions

Amplitude Damping (AD) Channel

- with some probability, an excited quantums state $|1\rangle$ decays into the ground state $|0\rangle$, i.e., $|1\rangle \to |0\rangle$
- modeled by error operator $A_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$
- at low temperature, spontaneous excitation $|0\rangle \rightarrow |1\rangle$ is negligible

• from
$$\sum_{k} A_{k}^{\dagger} A_{k} = I$$
 we get $A_{0} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}$

• channel model

$$\mathcal{E}_{\mathsf{AD}}(\rho) = A_0 \rho A_0^{\dagger} + A_1 \rho A_1^{\dagger}$$

notes:

- The channel operators do not contain identitiy *I*.
- Similar to the classical \mathcal{Z} -channel, but also error A_0 .

Approximate Error Correction

(see [Leung, Nielsen, Chuang & Yamamoto, Physical Review A, 56(4):2567–2573, 1997])

Perfect error correction

Knill-Laflamme conditions for code with basis $|c_i\rangle$ and for error operators A_k :

$$\langle c_i | A_k^{\dagger} A_l | c_j \rangle = \delta_{ij} \alpha_{kl}, \quad \text{where } \alpha_{kl} \in \mathbb{C}$$

Approximate error correction

correction of errors up to some order t (t-code)

$$\langle c_i | A_k^{\dagger} A_l | c_j \rangle = \delta_{ij} \alpha_{kl} + O(\gamma^{t+1})$$
 where $\alpha_{kl} \in \mathbb{C}$

Example: code from [Leung et al.] with t = 1

$$|0\rangle_L = \frac{1}{\sqrt{2}} (|0000\rangle + |1111\rangle) \qquad |1\rangle_L = \frac{1}{\sqrt{2}} (|0011\rangle + |1100\rangle)$$

Amplitude Damping (AD) Channel

Relation to Pauli errors

$$\begin{aligned} A_0 &= \frac{1 + \sqrt{1 - \gamma}}{2}I + \frac{1 - \sqrt{1 - \gamma}}{2}Z\\ A_1 &= \frac{\sqrt{\gamma}}{2}\left(X + iY\right) \quad \text{and} \quad A_1^{\dagger} &= \frac{\sqrt{\gamma}}{2}\left(X - iY\right) \end{aligned}$$

- quantum error-correction is linear in the error operators
- A_1 and A_1^{\dagger} span the same space of operators as X and Y

 \implies codes for an asymmetric quantum channel can be used for the AD channel

but: We don't need to correct for A_1^{\dagger} .

Expansion of the Errors

Relation to Pauli errors

$$A_0 = \frac{1 + \sqrt{1 - \gamma}}{2}I + \frac{1 - \sqrt{1 - \gamma}}{2}Z$$
$$A_1 = \frac{\sqrt{\gamma}}{2}(X + iY) \quad \text{and} \quad A_1^{\dagger} = \frac{\sqrt{\gamma}}{2}(X - iY)$$

note: $1 - \sqrt{1 - \gamma} = \frac{1}{2}\sqrt{\gamma}^2 + \frac{1}{8}\sqrt{\gamma}^4 + \frac{1}{16}\sqrt{\gamma}^6 + \frac{5}{128}\sqrt{\gamma}^8 + O(\sqrt{\gamma}^{10})$

 \implies For a *t*-code, it is sufficient to independently correct t + 1 errors Z and 2t + 1 errors X.

Proposition [Gottesman, PhD thesis]

An [[n, k]] CSS code of X-distance 2t + 1 and Z-distance t + 1 is an [[n, k]] t-code.

Quantum Dual Rail Code

Lemma

Using the quantum dual-rail code Q_1 which encodes a single qubit into two qubits, given by

$$|0\rangle_L = |01\rangle, \quad |1\rangle_L = |10\rangle,$$

two uses of the AD channel simulate a quantum erasure channel.

Proof

For the basis states $|i
angle_L$ of \mathcal{Q}_1 we compute

$$(A_0 \otimes A_0)|i\rangle_L = \sqrt{1 - \gamma}|i\rangle_L$$
$$(A_0 \otimes A_1)|i\rangle_L = (A_1 \otimes A_0)|i\rangle_L = \sqrt{\gamma}|00\rangle$$
$$(A_1 \otimes A_1)|i\rangle_L = 0.$$
(1)

Hence for any state ρ of the code \mathcal{Q}_1 , we get

$$\mathcal{E}_{\mathsf{AD}}^{\otimes 2}(\rho) = (1 - \gamma)\rho + \gamma(|00\rangle\langle 00|).$$

Quantum Dual Rail Code

Theorem

If there exists an [[m, k, d]] quantum code Q_2 , then there is a [[2m, k]] t-code Q correcting t = d - 1 amplitude damping errors.

Proof

- \mathcal{Q} is the concatenation of \mathcal{Q}_2 with the quantum dual rail code \mathcal{Q}_1
- the effective channel for the outer code \mathcal{Q}_2 is

$$\mathcal{E}_{\mathsf{AD}}^{\otimes 2}(\rho) = (1 - \gamma)\rho + \gamma(|00\rangle\langle 00|)$$

• Q_2 corrects d-1 erasure errors

Length Comparison with CSS and Stabilizer Codes

CSS code					stab. code	concatenation
n	k	t	t+1	2t + 1	n'	2m
12–13	1	2	3	5	11	10
19–20	1	3	4	7	17	20
25–30	1	4	5	9	23–25	22
33–41	1	5	6	11	29	32
39–54	1	6	7	13	35–43	34
47–70	1	7	8	15	41–53	44–48
53–79	1	8	9	17	47–61	46–50
61–89	1	9	10	19	53–81	56
67–105	1	10	11	21	59–85	58

Length Comparison with CSS and Stabilizer Codes

CSS code					stab. code	concatenation
n	k	t	t+1	2t + 1	n'	2m
14–17	2	2	3	5	14	16
20–27	2	3	4	7	20–23	20
27–37	2	4	5	9	26–27	28
34–45	2	5	6	11	32–41	32
41–62	2	6	7	13	38–51	40–46
48–71	2	7	8	15	44–59	44–52
55–87	2	8	9	17	50–78	52–54
62–102	2	9	10	19	56–83	56–56
69–110	2	10	11	21	62–104	64–82

Distance Comparison with Stabilizer Codes

n	k	t	2t + 1	d	t'		n	k	t	2t + 1	d	t'
8	1	1	3	3	1		8	2	1	3	3	1
10	1	2	5	4	1		16	2	2	5	6	2
20	1	3	7	7	3		20	2	3	7	6–7	2–3
22	1	4	9	7–8	3		28	2	4	9	10	4
32	1	5	11	11	5		32	2	5	11	10–11	4–5
34	1	6	13	11–12	5		46	2	6	13	12–16	5–7
48	1	7	15	13–17	6–8		52	2	7	15	14–18	6–8
50	1	8	17	13–17	6–8		54	2	8	17	14–18	6–8
56	1	9	19	15–19	7–9		56	2	9	19	14–19	6–9
58	1	10	21	15–20	7–9	_	82	2	10	21	18–28	8–13

Distance Comparison with Stabilizer Codes

						- •						
n	k	t	2t + 1	d	t'		n	k	t	2t + 1	d	t'
16	5	1	3	4–5	1–2		16	6	1	3	4	1
22	5	2	5	6–7	2–3		24	6	2	5	6–7	2–3
28	5	3	7	7–9	3–4		28	6	3	7	6–8	2–3
36	5	4	9	8–11	3–5		36	6	4	9	8–11	3–5
42	5	5	11	9–13	4–6		48	6	5	11	10–15	4–7
50	5	6	13	11–16	5–7		58	6	6	13	12–19	5–9
60	5	7	15	13–19	6–9		64	6	7	15	14–21	6–10
78	5	8	17	15–25	7–12		84	6	8	17	17–27	8–13
86	5	9	19	18–28	8–13		92	6	9	19	18–29	8–14
98	5	10	21	19–32	9–15		104	6	10	21	19–33	9–16

Conclusions

- concatenation yields large codes from small components
- generalized concatenation for quantum codes allows the use of classical outer codes
- outer codes need not be linear
- construction of non-additive quantum codes with higher dimension than stabilizer codes
- simple construction of QECCs with varying length
- structured encoding circuits
- concatenation allows to transform channels