International Summer School on
Quantum Information
MPIPKS, Dresden, August 29 – September 30, 2005

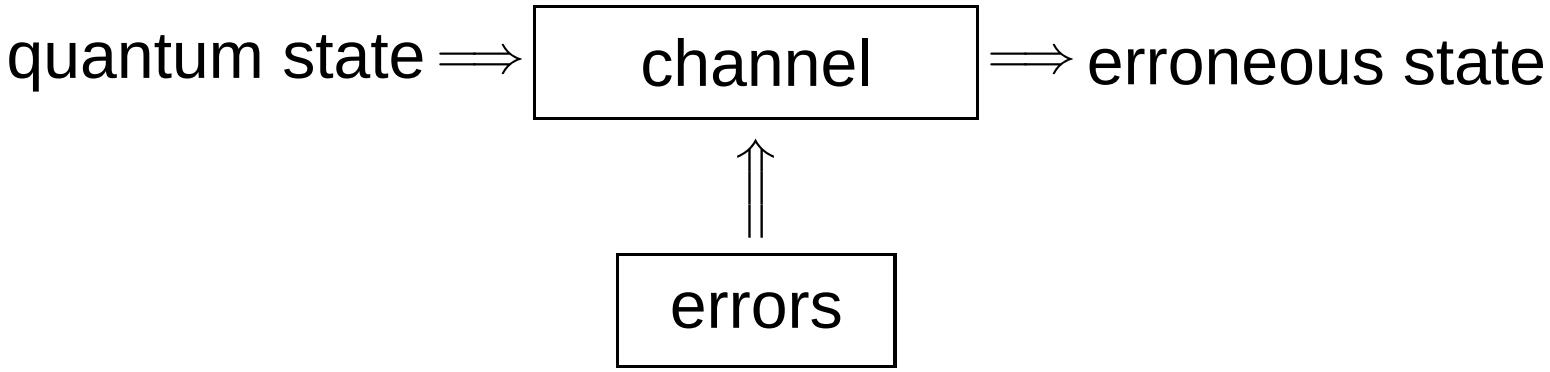
Quantum Algorithms &
Quantum Error Correction

Martin Rötteler & *Markus Grassl*

Arbeitsgruppe *Quantum Computing*, Prof. Beth
Institut für Algorithmen und Kognitive Systeme
Fakultät für Informatik, Universität Karlsruhe (TH)
Germany
http://iaks-www.ira.uka.de/QIV

QECCs: The Basic Problem

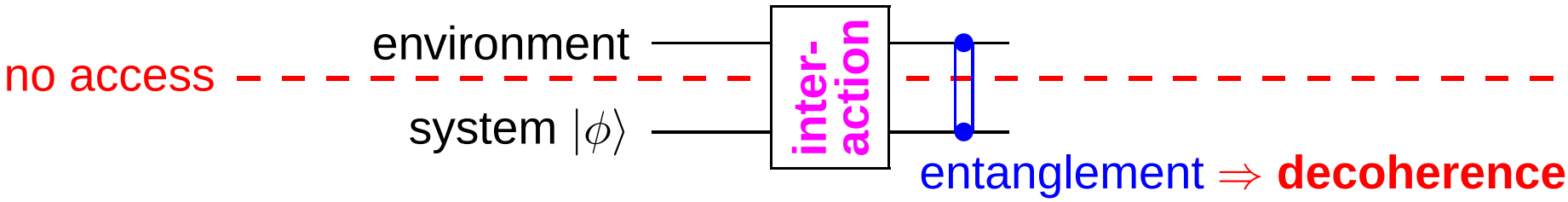
storage
transmission
} of quantum information



Errors are induced by, e. g., interaction with an environment, coupling to a bath, or also by imperfect operations.

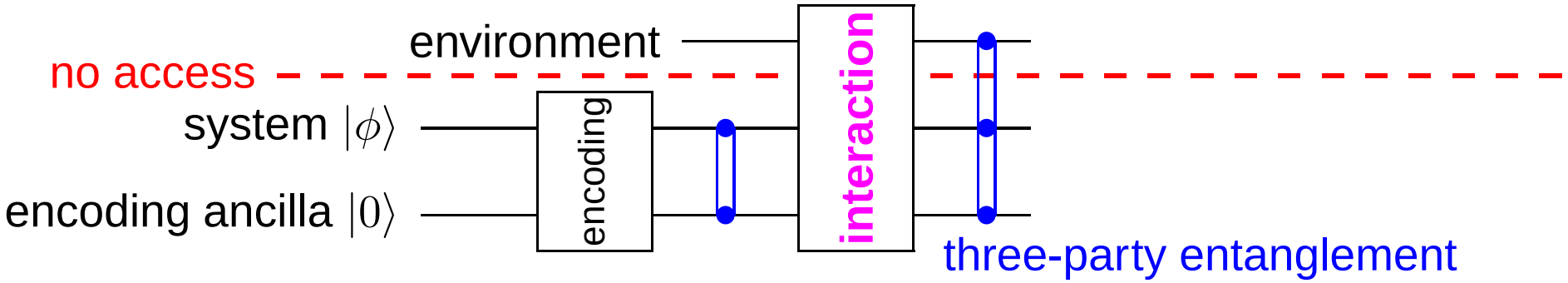
Quantum Error Correction

General scheme



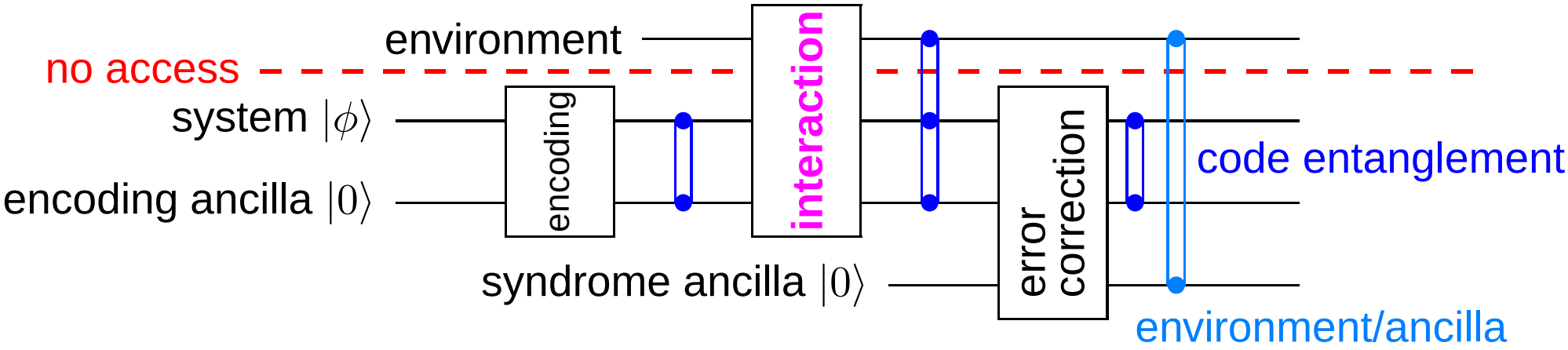
Quantum Error Correction

General scheme



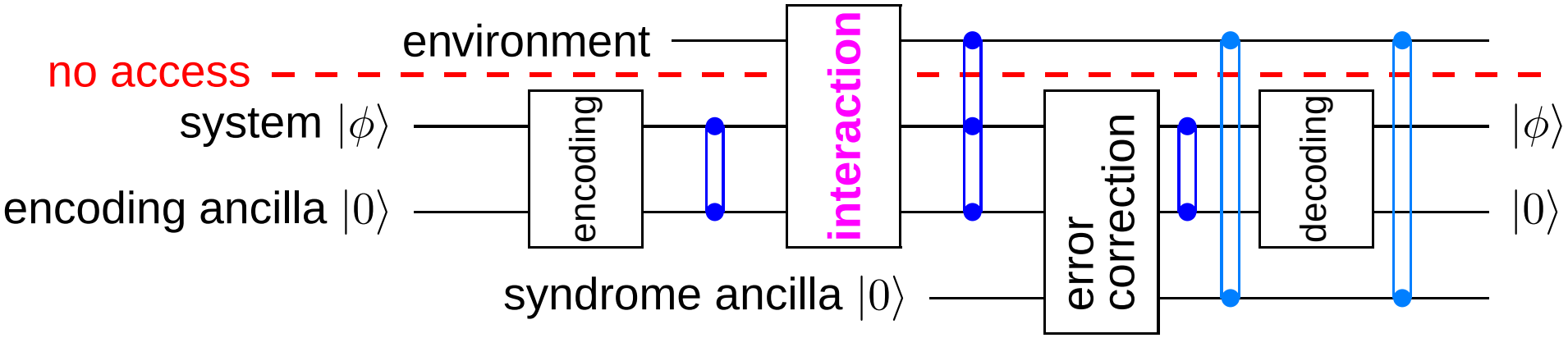
Quantum Error Correction

General scheme



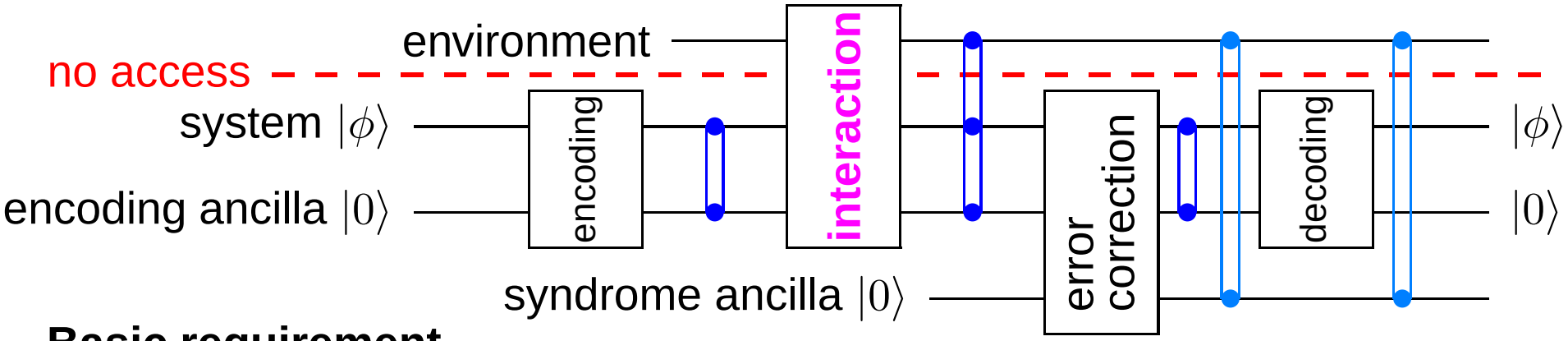
Quantum Error Correction

General scheme



Quantum Error Correction

General scheme



Basic requirement

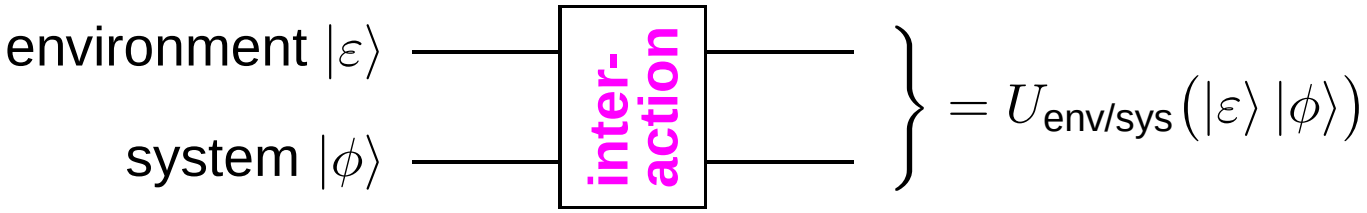
some knowledge about the interaction between system and environment

Common assumptions

- no initial entanglement between system and environment
- local or uncorrelated errors, i. e., only a few qubits are disturbed
  $\Longrightarrow$ CSS codes, stabilizer codes
- interaction with symmetry $\Longrightarrow$ decoherence free subspaces

Interaction System/Environment

“Closed” System



“Channel”

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

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 E_i acts on few subsystems, e. g. quantum gates

Computer Science Approach: *Discretize*

QECC Characterization

[Knill & Laflamme, PRA **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 $E_k, E_l \in \mathcal{E}$:

$$\langle c_i | E_k^\dagger E_l | c_j \rangle = \delta_{i,j} \alpha_{k,l}. \tag{1}$$

It is sufficient that (1) holds for a vector space basis of $\mathcal{E}$.

Linearity of 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.

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 $E_i \neq I$

Local Error Model

Code Parameters

$\mathcal{C} = [\![n, k, d]\!]$

n: number of subsystems used in total

k: number of (logical) subsystems encoded

d: “minimum distance”

- correct all errors acting on at most $(d-1)/2$ subsystems
- detect all errors acting on less than d subsystems
- correct all errors acting on less than d subsystems at *known* positions

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 $Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = XZ$.

Pauli and Hadamard matrices

"Pauli" matrices:

$$I,\ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ Y = XZ = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Hadamard matrix: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Important properties:

- $H^\dagger X H = Z$, "H changes bit-flips to phase-flips"
- $ZX = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -Y = -XZ$, "$X$ and Z anticommute"
- All errors either commute or anticommute!

Discretization of Quantum Errors

Consider errors $E = E_1 \otimes \ldots \otimes E_n, \quad E_i \in \{I, X, Y, Z\}$.

Pauli matrices:

$$I,\ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ Y = XZ = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

The weight of E is the number of $E_i \neq \mathbf{1}$. E. g., the weight of $I \otimes X \otimes Z \otimes Z \otimes I \otimes Y \otimes Z$ is 5.

Theorem: (later) If a code $\mathcal{C}$ corrects errors E of weight t or less, then $\mathcal{C}$ can correct arbitrary errors affecting $\leq t$ qubits.

Repetition Code

classical:

sender: repeats the information,

e. g. $0 \mapsto 000$, $1 \mapsto 111$

receiver: compares received bits and makes majority decision

quantum mechanical "solution":

sender: copies the information,

e. g. $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \mapsto |\psi\rangle\,|\psi\rangle\,|\psi\rangle$

receiver: compares and makes majority decision

but: unknown quantum states can neither be copied

nor can they be disturbance-free compared

The No-Cloning Theorem

Theorem: *Unknown* quantum states cannot be copied.

Proof: The copier would map $|0\rangle |\psi_{\text{in}}\rangle \mapsto |0\rangle |0\rangle$, $|1\rangle |\psi_{\text{in}}\rangle \mapsto |1\rangle |1\rangle$, and

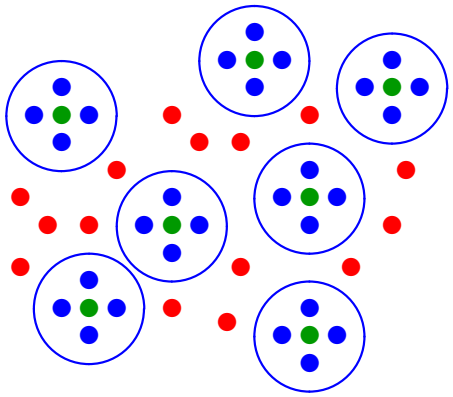
$$\begin{aligned}(\alpha |0\rangle + \beta |1\rangle) |\psi_{\text{in}}\rangle &\mapsto \alpha |0\rangle |0\rangle + \beta |1\rangle |1\rangle \\ &\neq (\alpha |0\rangle + \beta |1\rangle) \otimes (\alpha |0\rangle + \beta |1\rangle) \\ &= \alpha^2 |0\rangle |0\rangle + \beta^2 |1\rangle |1\rangle + \alpha\beta(|0\rangle |1\rangle + |1\rangle |0\rangle)\end{aligned}$$

Contradiction to the linearity of quantum mechanics!

The Basic Idea

Classical codes

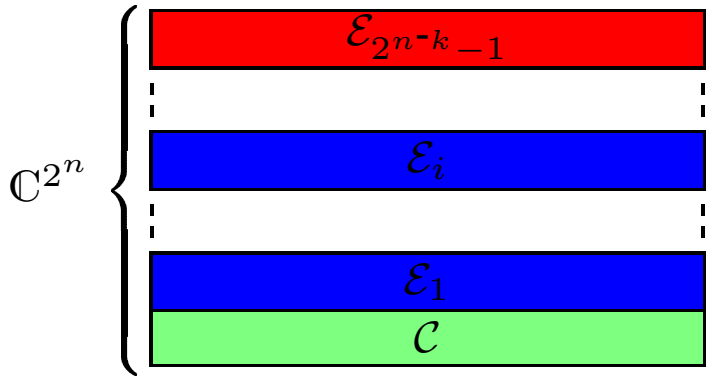
Partition of the set of all words of length n over an alphabet of size 2.



- codewords
- errors of bounded weight
- other errors

Quantum codes

Orthogonal decomposition of the vector space $\mathcal{H}^{\otimes n}$, where $\mathcal{H} \cong \mathbb{C}^2$.



$$\mathcal{H}^{\otimes n} = \mathcal{C} \oplus \mathcal{E}_1 \oplus \ldots \oplus \mathcal{E}_{2^{n-k}-1}$$

Encoding: $|\underline{x}\rangle \mapsto U_{enc}(|\underline{x}\rangle\,|0\rangle)$

Simple Quantum Error-Correcting Code

Repetition code: $|0\rangle \mapsto |000\rangle$, $|1\rangle \mapsto |111\rangle$

Encoding of one qubit:

$$\alpha\,|0\rangle + \beta\,|1\rangle \mapsto \alpha\,|000\rangle + \beta\,|111\rangle\,.$$

This defines a two-dimensional subspace $\mathcal{H}_{\mathcal{C}} \leq \mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2$

bit-flip	quantum state	subspace
no error	$\alpha\,\|000\rangle + \beta\,\|111\rangle$	$(\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1})\mathcal{H}_{\mathcal{C}}$
1^{st} position	$\alpha\,\|100\rangle + \beta\,\|011\rangle$	$(X \otimes \mathbb{1} \otimes \mathbb{1})\mathcal{H}_{\mathcal{C}}$
2^{nd} position	$\alpha\,\|010\rangle + \beta\,\|101\rangle$	$(\mathbb{1} \otimes X \otimes \mathbb{1})\mathcal{H}_{\mathcal{C}}$
3^{rd} position	$\alpha\,\|001\rangle + \beta\,\|110\rangle$	$(\mathbb{1} \otimes \mathbb{1} \otimes X)\mathcal{H}_{\mathcal{C}}$

Hence we have an orthogonal decomposition of $\mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2$

Simple Quantum Error-Correcting Code

Problem: What about phase-errors?

Phase-flip Z: $|0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto -|1\rangle$.

In the Hadamard basis $|+\rangle, |-\rangle$ given by

$$\begin{aligned} |+\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ |-\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

the phase-flip operates like the bit-flip $Z|+\rangle = |-\rangle$, $Z|-\rangle = |+\rangle$.

To correct phase errors we use repetition code and Hadamard basis:

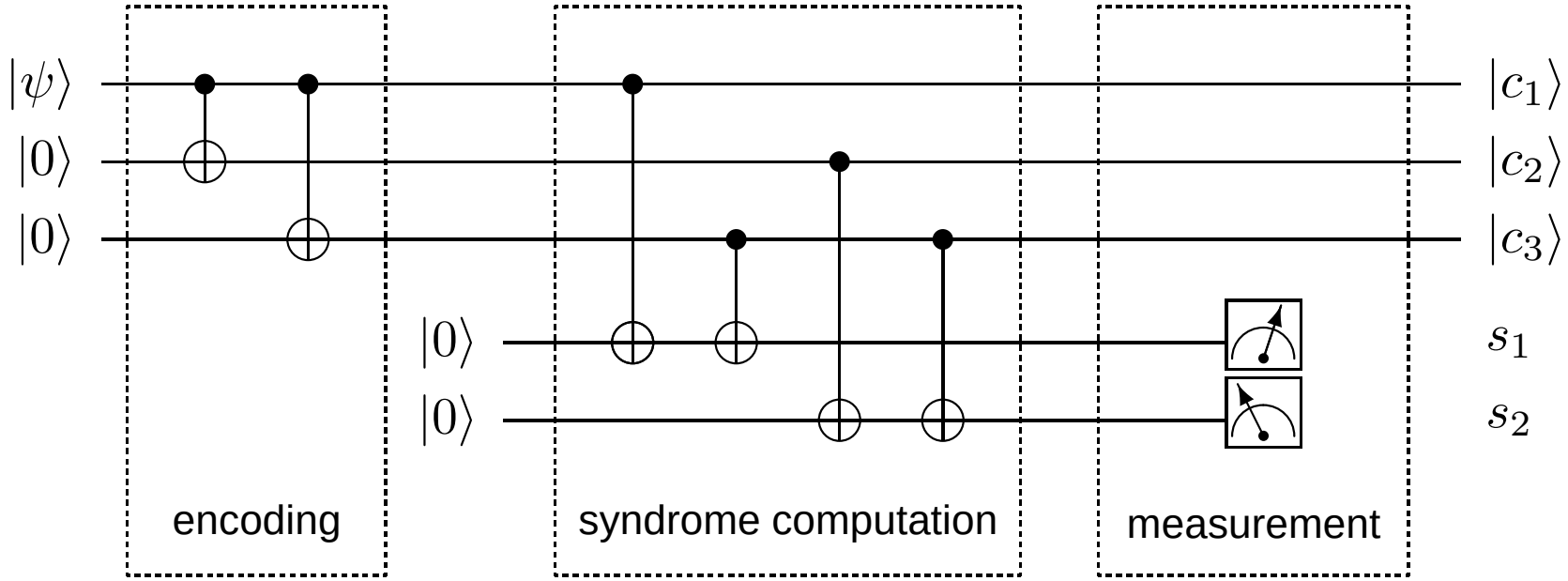
$$\begin{aligned} |0\rangle &\mapsto (H\otimes H\otimes H)\tfrac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = \tfrac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle) \\ |1\rangle &\mapsto (H\otimes H\otimes H)\tfrac{1}{\sqrt{2}}(|000\rangle - |111\rangle) = \tfrac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle) \end{aligned}$$

Simple Quantum Error-Correcting Code

phase-flip	quantum state	subspace
no error	$\frac{\alpha}{2}(\|000\rangle + \|011\rangle + \|101\rangle + \|110\rangle)$ $+\frac{\beta}{2}(\|001\rangle + \|010\rangle + \|100\rangle + \|111\rangle)$	$(\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1})\mathcal{H}_C$
1^{st} position	$\frac{\alpha}{2}(\|000\rangle + \|011\rangle - \|101\rangle - \|110\rangle)$ $+\frac{\beta}{2}(\|001\rangle + \|010\rangle - \|100\rangle - \|111\rangle)$	$(Z \otimes \mathbb{1} \otimes \mathbb{1})\mathcal{H}_C$
2^{nd} position	$\frac{\alpha}{2}(\|000\rangle - \|011\rangle + \|101\rangle - \|110\rangle)$ $+\frac{\beta}{2}(\|001\rangle - \|010\rangle + \|100\rangle - \|111\rangle)$	$(\mathbb{1} \otimes Z \otimes \mathbb{1})\mathcal{H}_C$
3^{rd} position	$\frac{\alpha}{2}(\|000\rangle - \|011\rangle - \|101\rangle + \|110\rangle)$ $-\frac{\beta}{2}(\|001\rangle + \|010\rangle + \|100\rangle - \|111\rangle)$	$(\mathbb{1} \otimes \mathbb{1} \otimes Z)\mathcal{H}_C$

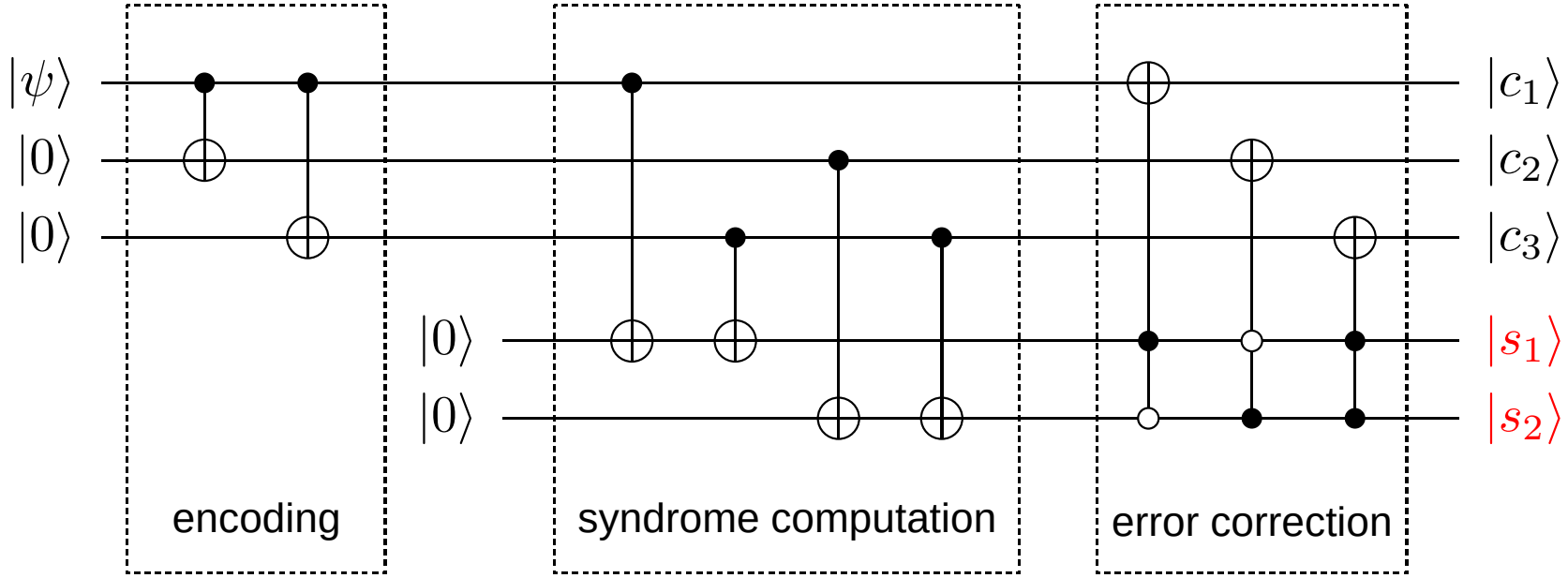
We again obtain an orthogonal decomposition of $\mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2$

Simple Quantum Error-Correcting Code



Error	$X \otimes I \otimes I$	gives	syndrome	$s_1 s_2 = 10$
Error	$I \otimes X \otimes I$	gives	syndrome	$s_1 s_2 = 01$
Error	$I \otimes I \otimes X$	gives	syndrome	$s_1 s_2 = 11$

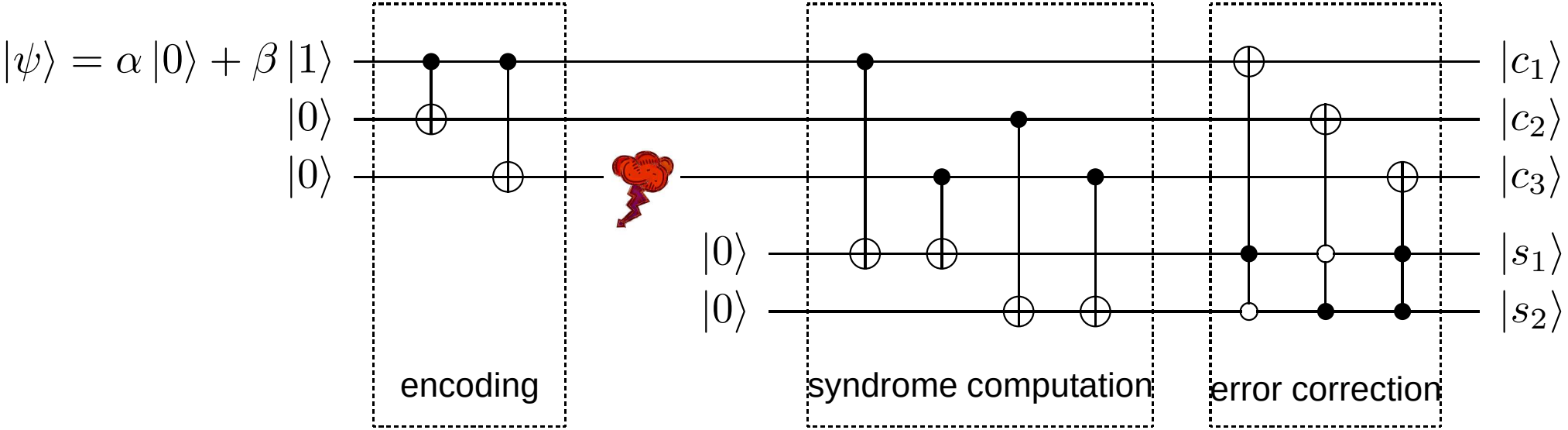
Simple Quantum Error-Correcting Code



- Coherent error correction by conditional unitary transformation.
- Information about the error is contained in $|s_1\rangle$ and $|s_2\rangle$.
- To do it again, we need either "fresh" qubits which are again in the ground state $|0\rangle$ or need to "cool" syndrome qubits to $|0\rangle$.

Effect of a Single Qubit Error

Suppose an error  corresponding to the bit-flip $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ happens.



Encoder maps $|\psi\rangle$ to $\alpha|000\rangle + \beta|111\rangle = |\psi_{\text{enc}}\rangle$

Error maps this to $\alpha|001\rangle + \beta|110\rangle$

Syndrome computation maps this to $\alpha|00111\rangle + \beta|11011\rangle$

Correction maps this to $\alpha|00011\rangle + \beta|11111\rangle = |\psi_{\text{enc}}\rangle|11\rangle$

Linearity of Syndrome Computation

Different Errors:

Error	$X \otimes I \otimes I$	syndrome	10
Error	$I \otimes X \otimes I$	syndrome	01

Suppose the (non-unitary) error is of the form

$$E = \alpha\, X \otimes I \otimes I + \beta\, I \otimes X \otimes I.$$

Then syndrome computation yields

$$\alpha(X \otimes I \otimes I\, |\psi_{\text{enc}}\rangle \otimes |10\rangle) + \beta(I \otimes X \otimes I\, |\psi_{\text{enc}}\rangle \otimes |01\rangle).$$

$$\mapsto |\psi_{\text{enc}}\rangle\, (\alpha\, |10\rangle + \beta\, |01\rangle)$$

Theorem: Suppose we have a QECC $|\psi\rangle \mapsto |\psi_{\text{enc}}\rangle$ which corrects errors E and F. Then this QECC corrects $\alpha E + \beta F$ for all α, β.

Shor's Nine-Qubit Code

Hadamard basis:

$$|+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

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

Phase-flip code: $|0\rangle \mapsto |+++\rangle, \quad |1\rangle \mapsto |---\rangle.$

Concatenation with bit-flip code gives:

$$|0\rangle \mapsto \tfrac{1}{\sqrt{2^3}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$|1\rangle \mapsto \tfrac{1}{\sqrt{2^3}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

Claim: This code can correct one error, i. e., it is an $[\![n, k, d]\!] = [\![9, 1, 3]\!]$.

Shor's Nine-Qubit Code

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

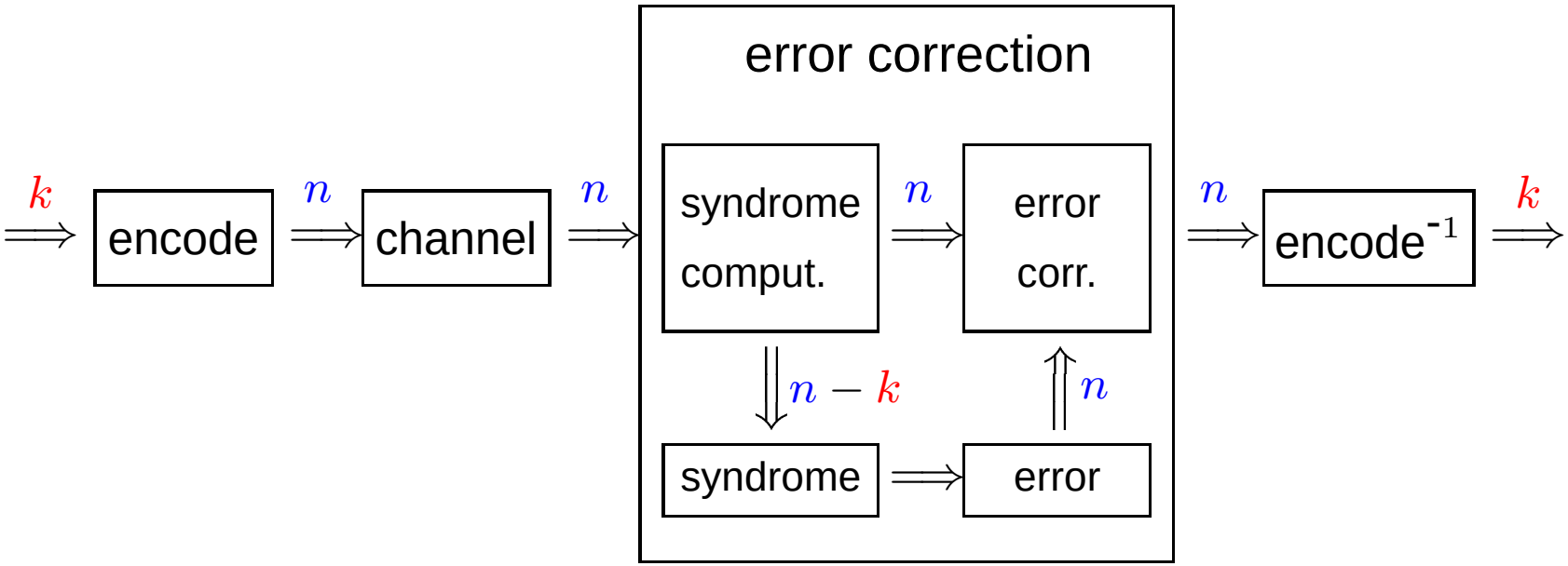
Effect of single-qubit errors:

- X-errors change the basis states, but can be corrected
- Z-errors at any of the three positions:

$$\left.\begin{aligned} Z|000\rangle &= |000\rangle \\ Z|111\rangle &= -|111\rangle \end{aligned}\right\} \text{“encoded” } Z\text{-operator}$$

$\Longrightarrow$ can be corrected by the second level of encoding

Encoding/Decoding: Overview



QECC $[\![n, k]\!]$ with length n and dimension 2^k

Quantum Error-Correcting Codes (QECC)

Characterization [Knill & Laflamme, PRA **55**, 900–911 (1997)]

Let $\mathcal{C}$ have orthonormal basis $\{|c_1\rangle, \ldots, |c_K\rangle\}$. Then $\mathcal{C}$ is a quantum error-correcting code for the error operators $\mathcal{E} = \{E_1, \ldots, E_N\}$ iff there are constants $\alpha_{k,l} \in \mathbb{C}$ such that for all $|c_i\rangle$, $|c_j\rangle$ and for all $E_k, E_l \in \mathcal{E}$:

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

Note:

- If $\mathcal{E}$ is a vector space it is enough to check this for a basis of $\mathcal{E}$.
- The conditions imply that there exists a measurement which detects any error with non-trivial action on $\mathcal{C}$.
- The also imply that there exists a unitary transformation which corrects any error.

General Decoding Algorithm

	$E_1\mathcal{C}$	$E_2\mathcal{C}$	$\cdots$	$E_k\mathcal{C}$	$\cdots$
$\mathcal{V}_0$	$E_1 \lvert c_0\rangle$	$E_2 \lvert c_0\rangle$	$\cdots$	$E_k \lvert c_0\rangle$	$\cdots$
$\mathcal{V}_1$	$E_1 \lvert c_1\rangle$	$E_2 \lvert c_1\rangle$	$\cdots$	$E_k \lvert c_1\rangle$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	
$\mathcal{V}_i$	$E_1 \lvert c_i\rangle$	$E_2 \lvert c_i\rangle$	$\cdots$	$E_k \lvert c_i\rangle$	$\cdots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\ddots$

$$\langle c_i| E_k^\dagger E_l |c_j\rangle = \delta_{i,j}\alpha_{k,l} \tag{1}$$

General Decoding Algorithm

	$E_1\mathcal{C}$	$E_2\mathcal{C}$	$\cdots$	$E_k\mathcal{C}$	$\cdots$
$\mathcal{V}_0$	$E_1 \lvert c_0\rangle$	$E_2 \lvert c_0\rangle$	$\cdots$	$E_k \lvert c_0\rangle$	$\cdots$
$\mathcal{V}_1$	$E_1 \lvert c_1\rangle$	$E_2 \lvert c_1\rangle$	$\cdots$	$E_k \lvert c_1\rangle$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	
$\mathcal{V}_i$	$E_1 \lvert c_i\rangle$	$E_2 \lvert c_i\rangle$	$\cdots$	$E_k \lvert c_i\rangle$	$\cdots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\ddots$

rows are orthogonal as $\langle c_i| E_k^\dagger E_l |c_j\rangle = 0$ for $i \neq j$

$$\langle c_i| E_k^\dagger E_l |c_j\rangle = \delta_{i,j}\alpha_{k,l} \tag{1}$$

General Decoding Algorithm

	$E_1\mathcal{C}$	$E_2\mathcal{C}$	$\cdots$	$E_k\mathcal{C}$	$\cdots$
$\mathcal{V}_0$	$E_1 \lvert c_0\rangle$	$E_2 \lvert c_0\rangle$	$\cdots$	$E_k \lvert c_0\rangle$	$\cdots$
$\mathcal{V}_1$	$E_1 \lvert c_1\rangle$	$E_2 \lvert c_1\rangle$	$\cdots$	$E_k \lvert c_1\rangle$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	
$\mathcal{V}_i$	$E_1 \lvert c_i\rangle$	$E_2 \lvert c_i\rangle$	$\cdots$	$E_k \lvert c_i\rangle$	$\cdots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\ddots$

rows are orthogonal as $\langle c_i| E_k^\dagger E_l |c_j\rangle = 0$ for $i \neq j$

inner product between columns is constant as $\langle c_i| E_k^\dagger E_l |c_i\rangle = \alpha_{k,l}$

$$\langle c_i| E_k^\dagger E_l |c_j\rangle = \delta_{i,j}\alpha_{k,l} \tag{1}$$

General Decoding Algorithm

	$E_1\mathcal{C}$	$E_2\mathcal{C}$	$\cdots$	$E_k\mathcal{C}$	$\cdots$
$\mathcal{V}_0$	$E_1 \lvert c_0\rangle$	$E_2 \lvert c_0\rangle$	$\cdots$	$E_k \lvert c_0\rangle$	$\cdots$
$\mathcal{V}_1$	$E_1 \lvert c_1\rangle$	$E_2 \lvert c_1\rangle$	$\cdots$	$E_k \lvert c_1\rangle$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	
$\mathcal{V}_i$	$E_1 \lvert c_i\rangle$	$E_2 \lvert c_i\rangle$	$\cdots$	$E_k \lvert c_i\rangle$	$\cdots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\ddots$

rows are orthogonal as $\langle c_i| E_k^\dagger E_l |c_j\rangle = 0$ for $i \neq j$

inner product between columns is constant as $\langle c_i| E_k^\dagger E_l |c_i\rangle = \alpha_{k,l}$

$\Longrightarrow$ simultaneous Gram-Schmidt orthogonalization within the spaces $\mathcal{V}_i$

Orthogonal Decomposition

	$E'_1\mathcal{C}$	$E'_2\mathcal{C}$	$\cdots$	$E'_k\mathcal{C}$	$\cdots$
$\mathcal{V}_0$	$E'_1 \lvert c_0\rangle$	$E'_2 \lvert c_0\rangle$	$\cdots$	$E'_k \lvert c_0\rangle$	$\cdots$
$\mathcal{V}_1$	$E'_1 \lvert c_1\rangle$	$E'_2 \lvert c_1\rangle$	$\cdots$	$E'_k \lvert c_1\rangle$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	
$\mathcal{V}_i$	$E'_1 \lvert c_i\rangle$	$E'_2 \lvert c_i\rangle$	$\cdots$	$E'_k \lvert c_i\rangle$	$\cdots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\ddots$

columns are mutually orthogonal

rows are mutually orthogonal

- new error operators E'_k are linear combinations of the E_l
- projection onto $E'_k\mathcal{C}$ determines the error
- exponentially many orthogonal spaces $E'_k\mathcal{C}$

International Summer School on
Quantum Information
MPIPKS, Dresden, August 29 – September 30, 2005

Quantum Error Correction

Part II: Classical & Quantum Codes

Markus Grassl

Arbeitsgruppe *Quantum Computing*, Prof. Beth
Institut für Algorithmen und Kognitive Systeme
Fakultät für Informatik, Universität Karlsruhe (TH)
Germany
http://iaks-www.ira.uka.de/QIV

Reprise

Quantum Channel

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

Code Conditions

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

Orthogonal Decomposition

	$E_1'\mathcal{C}$	$E_2'\mathcal{C}$	$\cdots$	$E_k'\mathcal{C}$	$\cdots$
$\mathcal{V}_0$	$E_1'\|c_0\rangle$	$E_2'\|c_0\rangle$	$\cdots$	$E_k'\|c_0\rangle$	$\cdots$
$\mathcal{V}_1$	$E_1'\|c_1\rangle$	$E_2'\|c_1\rangle$	$\cdots$	$E_k'\|c_1\rangle$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	
$\mathcal{V}_i$	$E_1'\|c_i\rangle$	$E_2'\|c_i\rangle$	$\cdots$	$E_k'\|c_i\rangle$	$\cdots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\ddots$

CSS Prelims: Linear Binary Codes

The field $\mathbb{F}_2$:

The set $\{0, 1\}$ with addition/multiplication modulo 2.

The vector space $\mathbb{F}_2^n$:

The set of all binary sequences of length n with componentwise addition.

Linear binary block codes:

Subset of $\mathbb{F}_2^n$ which is closed under addition.

Hamming distance of a and b:

Number of positions where $\boldsymbol{a}$ and $\boldsymbol{b}$ differ.

Hamming weight of a:

Number of positions where $\boldsymbol{a}$ is non-zero.

CSS Prelims: Linear Binary Codes

Minimum distance:

$$d = \min\{\mathrm{dist}(\boldsymbol{a}, \boldsymbol{b}) : \boldsymbol{a}, \boldsymbol{b} \in C | \boldsymbol{a} \neq \boldsymbol{b}\}$$

$$\mathrm{dist}(\boldsymbol{a}, \boldsymbol{b}) = \mathrm{dist}(\boldsymbol{a} - \boldsymbol{b}, \boldsymbol{0})$$

Minimum weight:

$$d = \min\{\mathrm{wgt}(\boldsymbol{a}) : \boldsymbol{a} \in C | \boldsymbol{a} \neq \boldsymbol{0}\}$$

Notation: $C = [n, k, d]$

- subset of $\mathbb{F}_2^n$, i. e. codewords of length n
- k-dimensional subspace, i. e. 2^k codewords
- minimum distance/weight d

CSS Prelims: Linear Binary Codes

Generator matrix:

$C = [n, k, d]$ is a k-dim. subspace of $\mathbb{F}_2^n$

$\Longrightarrow$ basis with k (row) vectors, $G \in \mathbb{F}_2^{k \times n}$

$$C = \{\boldsymbol{i}G : \boldsymbol{i} \in \mathbb{F}_2^k\}$$

Parity check matrix:

$C = [n, k, d]$ is a k-dim. subspace of $\mathbb{F}_2^n$

$\Longrightarrow$ kernel of $n - k$ homogeneous linear equations, $H \in \mathbb{F}_2^{(n-k) \times n}$

$$C = \{\boldsymbol{v} : \boldsymbol{v} \in \mathbb{F}_2^n | \boldsymbol{v}H^t = 0\}$$

Error syndrome:

erroneous codeword $\boldsymbol{v} = \boldsymbol{c} + \boldsymbol{e}$

$\Longrightarrow$ error syndrome $\boldsymbol{v}H^t = \boldsymbol{c}H^t + \boldsymbol{e}H^t = \boldsymbol{e}H^t$

CSS Prelims: Dual of a Classical Code

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

$$C^{\perp} := \left\{ \boldsymbol{y} \in \mathbb{F}_2^n : \sum_{i=1}^{n} x_i y_i = 0 \text{ for all } \boldsymbol{x} \in C \right\}$$

We denote the scalar product by $\boldsymbol{x} \cdot \boldsymbol{y} := \sum_{i=1}^{n} x_i y_i$.

Lemma: Let C be a linear code. Then

$$\sum_{\boldsymbol{c} \in C} (-1)^{\boldsymbol{x} \cdot \boldsymbol{c}} = \begin{cases} |C| & \text{for } \boldsymbol{x} \in C^{\perp}, \\ 0 & \text{for } \boldsymbol{x} \notin C^{\perp}. \end{cases}$$

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 a bit-flip $\boldsymbol{x} \in \mathbb{F}_2^n$ and a phase-flip $\boldsymbol{z} \in \mathbb{F}_2^n$ 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

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

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

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

Theorem: Then the vector space $\mathcal{C}$ spanned by these states is a quantum code with parameters $[\![n, k_1 + k_2 - n, d]\!]$ where $d \geq \min(d_1, d_2)$.

CSS Codes — how they work

Basis states:

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

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

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

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 $\boldsymbol{x} \in C_1$.

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

Then 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

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

Then $H^{\otimes n}$ 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).

Encoding

Classical code

$$\begin{aligned} \text{information} &\longmapsto \text{codeword} \\ \boldsymbol{i} = (i_1, i_2, \ldots, i_k) &\longmapsto \boldsymbol{i} \cdot G = \sum_{j=1}^{k} i_j \boldsymbol{g}_j \end{aligned}$$

Quantum code

$$\begin{aligned} \text{information} &\longmapsto \text{cosets of the code } C_2^{\perp} \text{ in } C_1 \\ |\boldsymbol{i}\rangle = |i_1, i_2, \ldots, i_k\rangle &\longmapsto \sum_{\boldsymbol{c} \in C_2^{\perp}} |\boldsymbol{c} + \boldsymbol{x}_i\rangle = \sum_{\boldsymbol{c} \in C_2^{\perp}} |\boldsymbol{c} + \sum_{j=1}^{k} i_j \boldsymbol{g}_j\rangle \\ &= \sum_{\boldsymbol{x} \in \{0,1\}^k} |\boldsymbol{x} \cdot \tilde{G} + \sum_{j=1}^{k} i_j \boldsymbol{g}_j\rangle \end{aligned}$$

$C_2^{\perp} \subseteq C_1$, $\tilde{G}$ is generator matrix for $C_2^{\perp}$,
the $\boldsymbol{g}_j$ are linear independent coset representatives of $C_1/C_2^{\perp}$

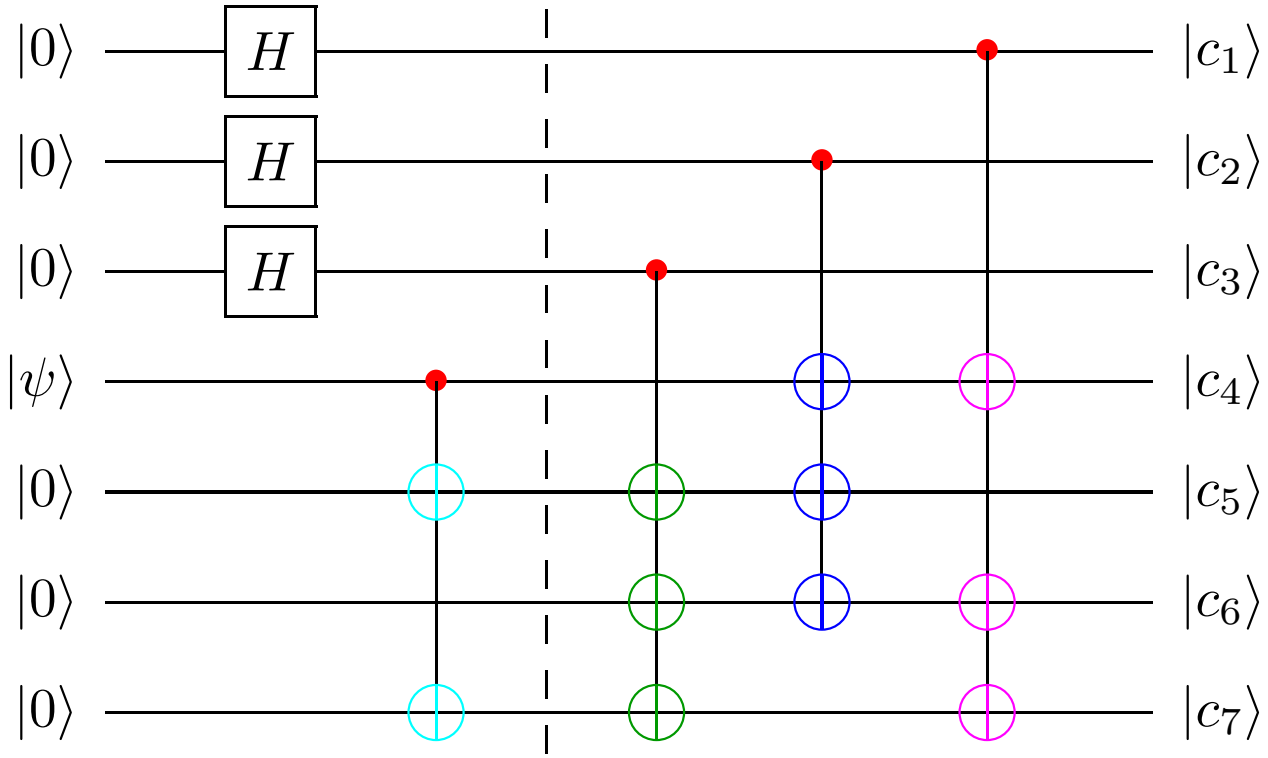
Example: Seven Qubit Code

Given binary Hamming code C with generator matrix

$$G = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix},$$

then C is a $[7, 3, 4]$ and $C \leq C^{\perp}$. The dual code $C^{\perp}$ is a $[7, 4, 3]$ and has generator matrix

$$G' = \left(\begin{array}{ccccccc} 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right)$$



$$G^t = \left(\begin{array}{c|ccc} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{array}\right)$$

$$\alpha|0\rangle + \beta|1\rangle \quad \mapsto \quad \alpha\frac{1}{\sqrt{8}} \sum_{i_1,i_2,i_3\in\{0,1\}} |0\boldsymbol{g}_4 + i_3\boldsymbol{g}_3 + i_2\boldsymbol{g}_2 + i_1\boldsymbol{g}_1\rangle$$

$$+\beta\frac{1}{\sqrt{8}} \sum_{i_1,i_2,i_3\in\{0,1\}} |1\boldsymbol{g}_4 + i_3\boldsymbol{g}_3 + i_2\boldsymbol{g}_2 + i_1\boldsymbol{g}_1\rangle$$

Computation of an Error Syndrome

Classical code:

received vector $\longmapsto$ syndrome

$$\boldsymbol{r} = (r_1, r_2, \ldots, r_k) \quad \longmapsto \quad \boldsymbol{r} \cdot H^t = \sum_{j=1}^{n-k} r_j \boldsymbol{h}_j = (\boldsymbol{c} + \boldsymbol{e}) \cdot H^t = \boldsymbol{e} \cdot H^t$$

Quantum code:

quantum state $\longmapsto$ quantum state $\otimes$ syndrome

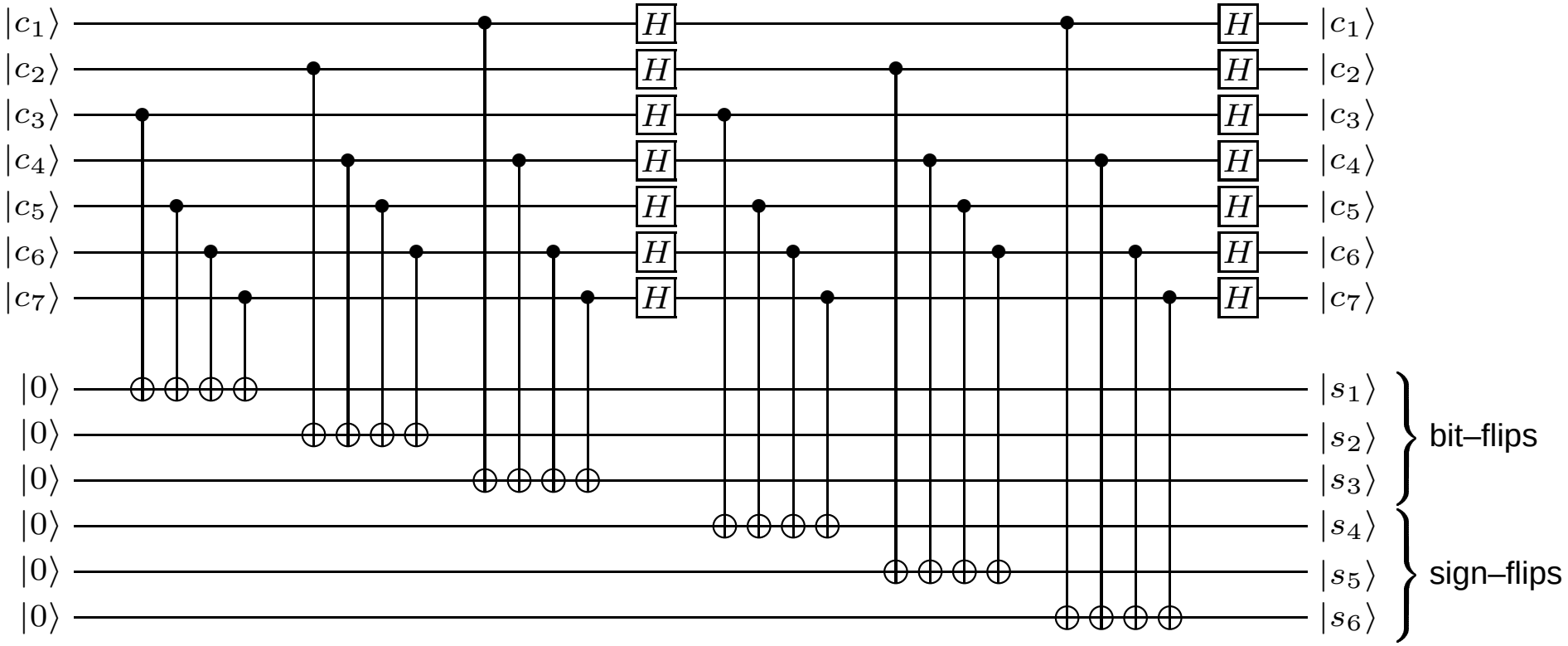
$$\sum_{\boldsymbol{c} \in \boldsymbol{C_2^\perp}} |\boldsymbol{c} + \boldsymbol{x}_i + \boldsymbol{e}\rangle \quad \longmapsto \quad \sum_{\boldsymbol{c} \in C_2^\perp} |\boldsymbol{c} + \boldsymbol{x}_i + \boldsymbol{e}\rangle \otimes \left|(\boldsymbol{c} + \boldsymbol{x}_i + \boldsymbol{e}) \cdot \tilde{H}^t\right\rangle$$

$$= \quad \left(\sum_{\boldsymbol{c} \in C_2^\perp} |\boldsymbol{c} + \boldsymbol{x}_i + \boldsymbol{e}\rangle \right) \otimes \left|\boldsymbol{e} \cdot \tilde{H}^t\right\rangle$$

$\tilde{H}$ is a parity check matrix of C_1

Syndrome Computation of CSS Codes

$$|\psi_i\rangle = \sum_{\boldsymbol{c}\in C_2^{\perp}} |\boldsymbol{c}+\boldsymbol{x}_i\rangle\,, \qquad H^{\otimes N}\,|\psi_i\rangle = \sum_{\boldsymbol{c}\in C_2} (-1)^{\boldsymbol{c}\cdot\boldsymbol{x}_i}\,|\boldsymbol{c}\rangle$$

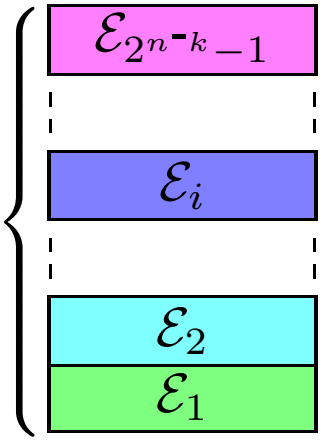


Stabilizer Codes

Observables

$\mathcal{C}$ is a common eigenspace of the stabilizer group $\mathcal{S}$

decomp. into
common eigenspaces



the orthogonal spaces are labeled by the eigenvalues

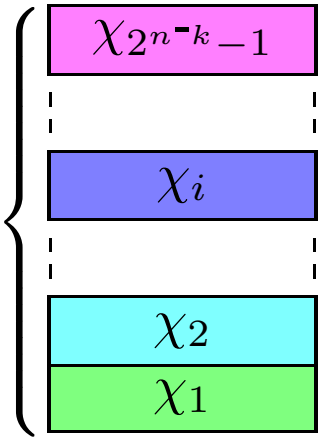
$\Longrightarrow$ operations that change the eigenvalues can be detected

Stabilizer Codes

Representation Theory

$\mathcal{C}$ is an eigenspace of $\mathcal{S}$ w.r.t. some irred. character χ_1

decomp. into
irred. components



the orthogonal spaces are labeled by the character (values)

$\Longrightarrow$ operations that change the character (value) can be detected

The Stabilizer of a Quantum Code

Pauli group:

$$\mathcal{G}_n = \left\{ \pm E_1 \otimes \ldots \otimes E_n : E_i \in \{I, X, Y, Z\} \right\}$$

Let $\mathcal{C} \leq \mathbb{C}^{2^n}$ be a quantum code.

The stabilizer of $\mathcal{C}$ is defined to be the set

$$S = \left\{ M \in \mathcal{G}_n : M\,|v\rangle = |v\rangle \text{ for all } |v\rangle \in \mathcal{C} \right\}.$$

S is an abelian (commutative) group!

The Stabilizer of the Repetition Code

Repetition code: Recall that $\mathcal{C}$ is the two-dimensional code spanned by

$$\begin{aligned} |\overline{0}\rangle &= |000\rangle \\ |\overline{1}\rangle &= |111\rangle \end{aligned}$$

What is the stabilizer of $\mathcal{C}$?

$$S = \{III,\ ZZI,\ ZIZ,\ IZZ\}.$$

Stabilizer Codes

Let $\mathcal{C}$ be a quantum code with stabilizer S.

The code $\mathcal{C}$ is called a stabilizer code if and only if

$$M|v\rangle = |v\rangle \text{ for all } M \in S$$

implies that $|v\rangle \in \mathcal{C}$.

In this case $\mathcal{C}$ is the joint $+1$-eigenspace of all $M \in S$.

Example: The repetition code is a stabilizer code.

Errors in Stabilizer Codes

Important identity:

$$ZX = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -XZ.$$

For error operators in the Pauli group $\mathcal{G}_n$ (i. e. tensor products of I, X, Y, Z) there are two possibilities: either

- they commute: $EF = FE$
- or they anticommute: $EF = -FE$

Errors in Stabilizer Codes

Let S be the stabilizer of a quantum code $\mathcal{C}$. Let $P_{\mathcal{C}}$ be the projector onto $\mathcal{C}$.

If an error E anticommutes with some $M \in S$ then E is detectable by $\mathcal{C}$.

Indeed,

$$P_{\mathcal{C}} E P_{\mathcal{C}} = P_{\mathcal{C}} E M P_{\mathcal{C}} = -P_{\mathcal{C}} M E P_{\mathcal{C}} = -P_{\mathcal{C}} E P_{\mathcal{C}}.$$

Hence $P_{\mathcal{C}} E P_{\mathcal{C}} = 0$, i. e. the spaces $\mathcal{C}$ and $E\mathcal{C}$ are orthogonal.

Errors: the Good, the Bad, and the Ugly

Let S be the stabilizer of a stabilizer code $\mathcal{C}$.

An error E is good if it does not affect the encoded information, i. e., if $E \in S$.

An error E is bad if it is detectable, e. g., it anticommutes with some $M \in S$.

An error E is ugly if it cannot be detected.

Examples of the Good, the Bad, and the Ugly

Let $\mathcal{C}$ the repetition code

Good: $Z \otimes Z \otimes I$ since $Z \otimes Z \otimes I \, |111\rangle = |111\rangle$

$Z \otimes Z \otimes I \, |000\rangle = |000\rangle$

Bad: $X \otimes I \otimes I$ since $X \otimes I \otimes I \, |111\rangle = |011\rangle$

$X \otimes I \otimes I \, |000\rangle = |100\rangle$

Ugly: $X \otimes X \otimes X$ since $X \otimes X \otimes X \, |111\rangle = |000\rangle$

Error Correction Capabilities

Let $\mathcal{C}$ be a stabilizer code with stabilizer S.

Let $N(S)$ be the normalizer of S in $\mathcal{G}_n$. This is the set of all matrices in $\mathcal{G}$ which commute with all of S. Clearly, we have $S \leq N(S)$.

All errors outside $N(S)$ can be detected.

Good	do not affect encoded information:	$x \in S$
Bad	anticommute with an element in S:	$x \notin N(S)$
Ugly	errors that cannot be detected:	$x \in N(S) \setminus S$

We need to find stabilizers such that the minimum weight of an element in $N(S) \setminus S$ is as large as possible.

Error Correction Capabilities

Summary: Any two elements M_1, M_2 of S commute.

Detectable errors anticommute with some $M \in S$.

Task: Find a nice characterization of these properties.

Notation: Denote by $X_{\boldsymbol{a}}$ where $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$ the operator

$$X_{\boldsymbol{a}} = X^{a_1} \otimes X^{a_2} \otimes \ldots \otimes X^{a_n}.$$

For instance $X_{110} = X \otimes X \otimes I$.

Hence, any operator in $\mathcal{G}_n$ is of the form $\pm X_{\boldsymbol{a}} Z_{\boldsymbol{b}}$ for some $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n$.

Symplectic Geometry

Consider $M_1 = X_{\boldsymbol{a}} Z_{\boldsymbol{b}}$, $M_2 = X_{\boldsymbol{c}} Z_{\boldsymbol{d}}$. When do M_1 and M_2 commute?

$$M_1 M_2 = X_{\boldsymbol{a}} Z_{\boldsymbol{b}} X_{\boldsymbol{c}} Z_{\boldsymbol{d}} = (-1)^{\boldsymbol{b}\cdot\boldsymbol{c}} X_{\boldsymbol{a}+\boldsymbol{c}} Z_{\boldsymbol{b}+\boldsymbol{d}}$$

$$M_2 M_1 = X_{\boldsymbol{c}} Z_{\boldsymbol{d}} X_{\boldsymbol{a}} Z_{\boldsymbol{b}} = (-1)^{\boldsymbol{a}\cdot\boldsymbol{d}} X_{\boldsymbol{a}+\boldsymbol{c}} Z_{\boldsymbol{b}+\boldsymbol{d}}$$

Hence, M_1 and M_2 commute iff $\boldsymbol{a}\cdot\boldsymbol{d} - \boldsymbol{b}\cdot\boldsymbol{c} = 0 \bmod 2$.

Suppose that S is the stabilizer of a 2^k-dimensional stabilizer code. Then $|S| = 2^{n-k}$. S can be generated by $n-k$ operators $X_{\boldsymbol{a}} Z_{\boldsymbol{b}}$. Let $H = (\mathbf{X}|\mathbf{Z})$ be an $(n-k) \times 2n$ matrix over $\mathbb{F}_2$. This matrix is used to describe the stabilizer. The rows of H contain the vectors $(\boldsymbol{a}|\boldsymbol{b})$.

Short Description of a Stabilizer

Example: Let $S = \{III,\ ZZI,\ IZZ,\ ZIZ\}$

Note that S is generated by ZZI and ZIZ.

$$H = (\mathbf{X}|\mathbf{Z}) = \left(\begin{array}{ccc|ccc} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right)$$

$(\boldsymbol{a}|\boldsymbol{b}) = (000|110)$ and $(\boldsymbol{c}|\boldsymbol{d}) = (000|101)$ are orthogonal:

$$\boldsymbol{a}\cdot\boldsymbol{d} - \boldsymbol{b}\cdot\boldsymbol{c} = 000\cdot 101 + 110\cdot 000 = 0$$

In this case we also write $(\boldsymbol{a}|\boldsymbol{b}) \perp (\boldsymbol{c}|\boldsymbol{d})$ with respect to the symplectic inner product $\langle(\boldsymbol{a}|\boldsymbol{b})|(\boldsymbol{c}|\boldsymbol{d})\rangle := \boldsymbol{a}\cdot\boldsymbol{d} - \boldsymbol{b}\cdot\boldsymbol{c}$.

Shor's nine-qubit code

Hadamard basis:

$$|+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Phase-flip code: $|0\rangle \mapsto |+++\rangle, \quad |1\rangle \mapsto |---\rangle.$

Concatenation with bit-flip code gives:

$$|0\rangle \mapsto \tfrac{1}{\sqrt{2^3}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$|1\rangle \mapsto \tfrac{1}{\sqrt{2^3}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

This code can correct one error, i. e., it is a $[\![9, 1, 3]\!]$.

Stabilizer for the nine-qubit code

$$\begin{pmatrix}
Z & Z & . & . & . & . & . & . & . \\
Z & . & Z & . & . & . & . & . & . \\
. & . & . & Z & Z & . & . & . & . \\
. & . & . & Z & . & Z & . & . & . \\
. & . & . & . & . & . & Z & Z & . \\
. & . & . & . & . & . & Z & . & Z \\
X & X & X & X & X & X & . & . & . \\
X & X & X & . & . & . & X & X & X
\end{pmatrix}$$

Generates an abelian subgroup of $\mathcal{G}_9$. This generating system of eight generators is minimal. Each generator divides the space by 2.

Hence we obtain a $[\![9, 1, 3]\!]$ quantum code.

The Five Qubit Code

Stabilizer: $\mathcal{S} = \langle YZZYI,\ IYZZY,\ YIYZZ,\ ZYIYZ \rangle$

$(\mathbf{X}|\mathbf{Z})$ matrix given by (recall: $X = (1,0)$, $Y = (1,1)$, $Z = (0,1)$):

$$G = \left(\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{array}\right)$$

$$\mathcal{C} = [\![5, 1, 3]\!]$$

shortest qubit code which encodes one qubit and can correct one error

Example: CSS-Code $\mathcal{C} = [\![7, 1, 3]\!]_2$

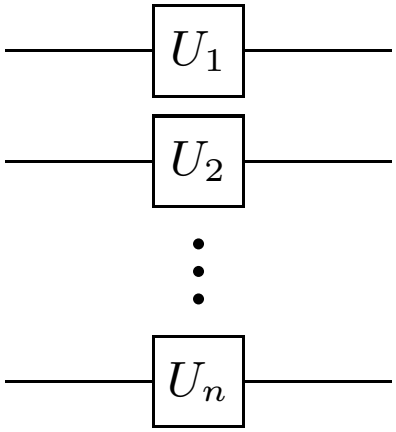
Here $H = (\mathbf{X}|\mathbf{Z})$ is of a special form:

$$H = \left(\begin{array}{ccccccc|ccccccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 & & & & & & & \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & & & & & & & \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & & & & & & & \\ \hline & & & & & & & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ & & & & & & & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ & & & & & & & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right)$$

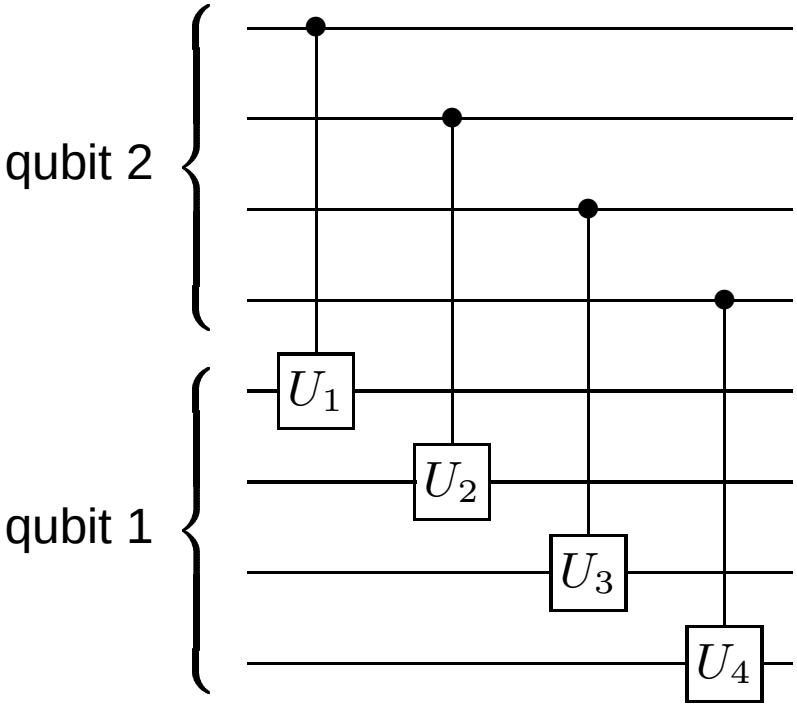
- Can be applied for (binary) codes $C_2^{\perp} \subseteq C_1$. If $C_1 = [n, k_1, d_1]$ and $C_2 = [n, k_2, d_2]$, this gives a QECC $[\![n, k_1 + k_2 - n, \min(d_1, d_2)]\!]$.
- Has been used to derive asymptotic good codes (explicitly).
- CSS codes have nice properties for fault-tolerant computing.

Fault Tolerant Quantum Computing

- Operate on encoded data (map codewords to codewords).
- Prevent spreading of errors.



local operations



transversal operations

Bounds

Quantum Hamming Bound: Set of vectors obtained by applying each error to each basis vector has to be linear independent. The subspace they span has to fit into the Hilbert space of n qubits. For a pure[a] QECC $[\![n, k, 2t+1]\!]$ this implies:

$$2^n \geq 2^k \sum_{i=0}^{t} 3^i \binom{n}{i}$$

Quantum Singleton Bound/Knill–Laflamme Bound: For all quantum codes $[\![n, k, d]\!]_q$ we have that

$$n + 2 \geq k + 2d.$$

Codes which meet the bound are called quantum MDS codes. They exist only for q large, i. e., for higher-dimensional alphabets.

[a] all error-syndromes are different

Optimal Small QECC

n/k	0	1	2	3	4	5	6
2	$[\![2,0,2]\!]$						
3	$[\![3,0,2]\!]$						
4	$[\![4,0,2]\!]$	$[\![4,1,2]\!]$	$[\![4,2,2]\!]$				
5	$[\![5,0,3]\!]$	$[\![5,1,3]\!]$	$[\![5,2,2]\!]$				
6	$[\![6,0,4]\!]$	$[\![6,1,3]\!]$	$[\![6,2,2]\!]$	$[\![6,3,2]\!]$	$[\![6,4,2]\!]$		
7	$[\![7,0,3]\!]$	$[\![7,1,3]\!]$	$[\![7,2,2]\!]$	$[\![7,3,2]\!]$	$[\![7,4,2]\!]$		
8	$[\![8,0,4]\!]$	$[\![8,1,3]\!]$	$[\![8,2,3]\!]$	$[\![8,3,3]\!]$	$[\![8,4,2]\!]$	$[\![8,5,2]\!]$	$[\![8,6,2]\!]$
9	$[\![9,0,4]\!]$	$[\![9,1,3]\!]$	$[\![9,2,3]\!]$	$[\![9,3,3]\!]$	$[\![9,4,2]\!]$	$[\![9,5,2]\!]$	$[\![9,6,2]\!]$

$[\![n,k,d]\!]$ means that n minimal for fixed (k,d).

$[\![n,k,d]\!]$ means that d maximal for fixed (n,k).

For more tables see `http://iaks-www.ira.uka.de/home/grassl/QECC`

References

- P. Shor. Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A, 52(4):2493–2496, 1995.
- D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. Phys. Rev. A, 54(3):1862–1868, 1996. quant-ph/9604038.
- A. Steane. Error correcting codes in quantum theory. Phys. Rev. Lett., 77(5):793–797, 1996.
- R. Calderbank, P. Shor. Good quantum error-correcting codes exist. Phys. Rev. A, 54(2):1098–1105, 1996. quant-ph/9512032.
- E. Knill, R. Laflamme. A theory of quantum error-correcting codes. Phys. Rev. A, 55(2):900–911, 1997. quant-ph/9604034.
- P. Shor. Fault-tolerant quantum computation. Proc. FOCS, pp. 56–65, 1996. quant-ph/9605011
- D. Gottesman. A theory of fault-tolerant quantum computation. Phys. Rev. A, 57(1):127–137, 1998. quant-ph/9702029.

References

- M. Grassl. Algorithmic aspects of quantum error-correcting codes, in: R. K. Brylinski and G. Chen (Eds.), Mathematics of Quantum Computation, Chapman & Hall/CRC, 2002, pp. 223–252.
- M. Grassl. Fehlerkorrigierende Codes für Quantensysteme: Konstruktionen und Algorithmen Aachen: Shaker Verlag, August 2002.
- tables of QECCs: `http://iaks-www.ira.uka.de/home/grassl/QECC/`
- more specific publications: `http://iaks-www.ira.uka.de/home/grassl/publications.html`