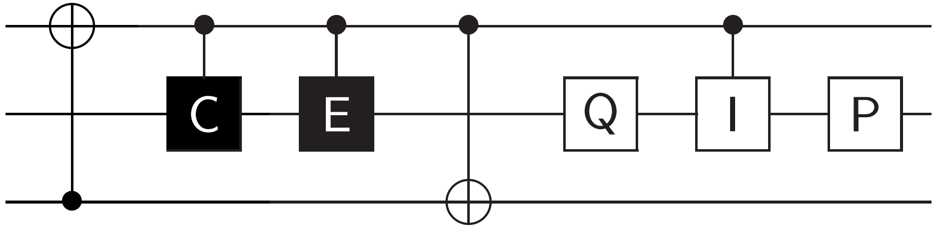
3rd Central European
Quantum Information Processing
Workshop
Znojmo, May 4–8, 2006



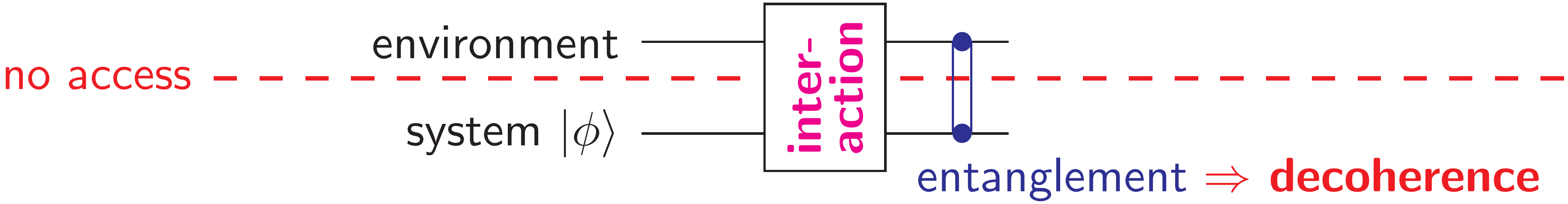

# Quantum Error-Correcting Codes

Markus Grassl

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

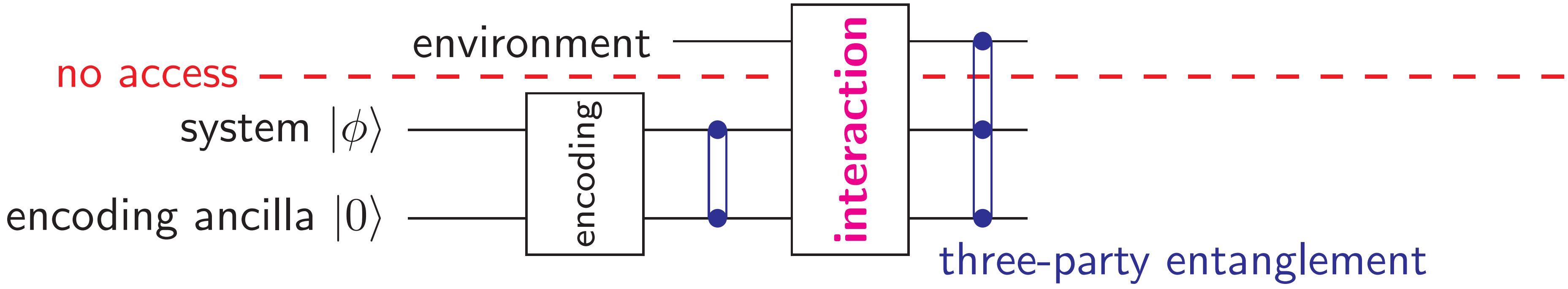
# Quantum Error Correction

## General scheme



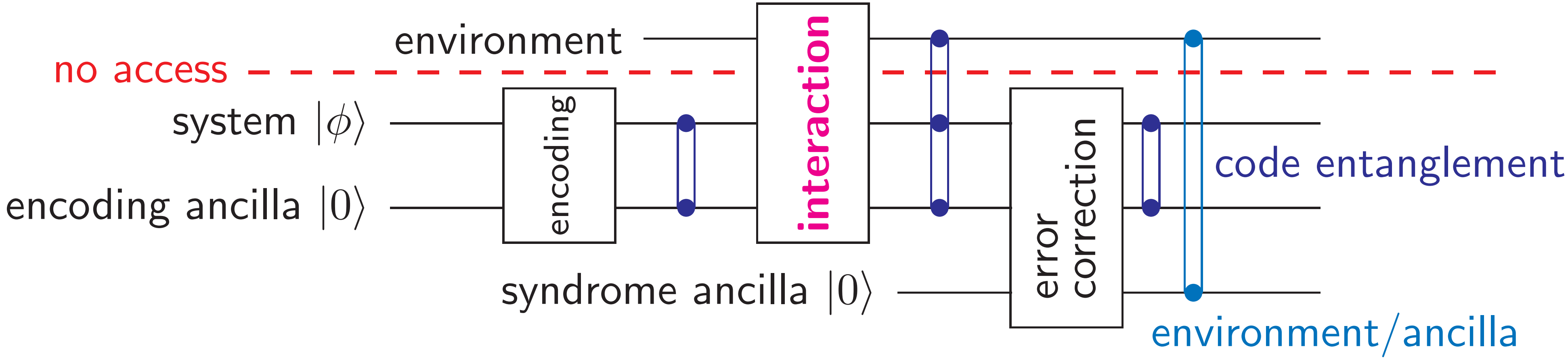
# Quantum Error Correction

## General scheme



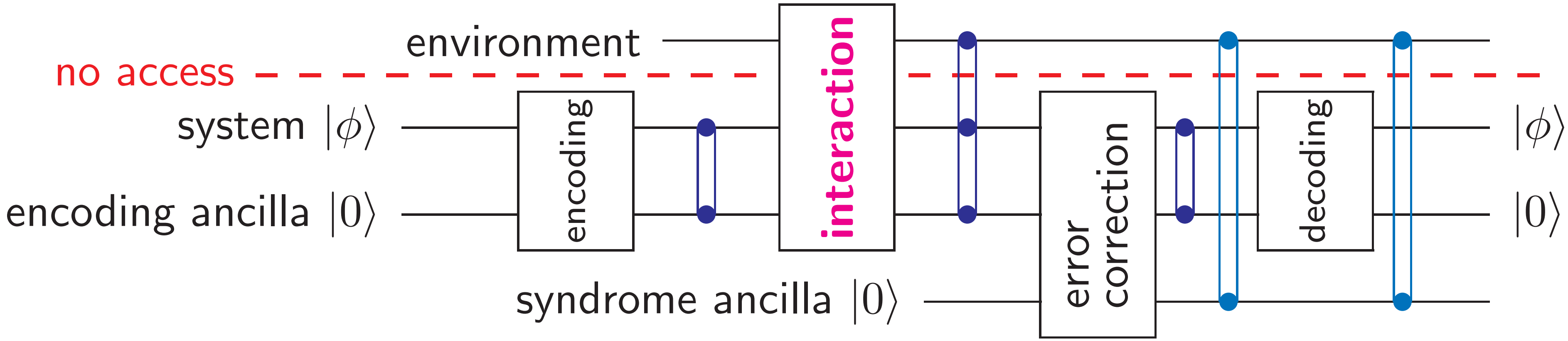
# Quantum Error Correction

## General scheme



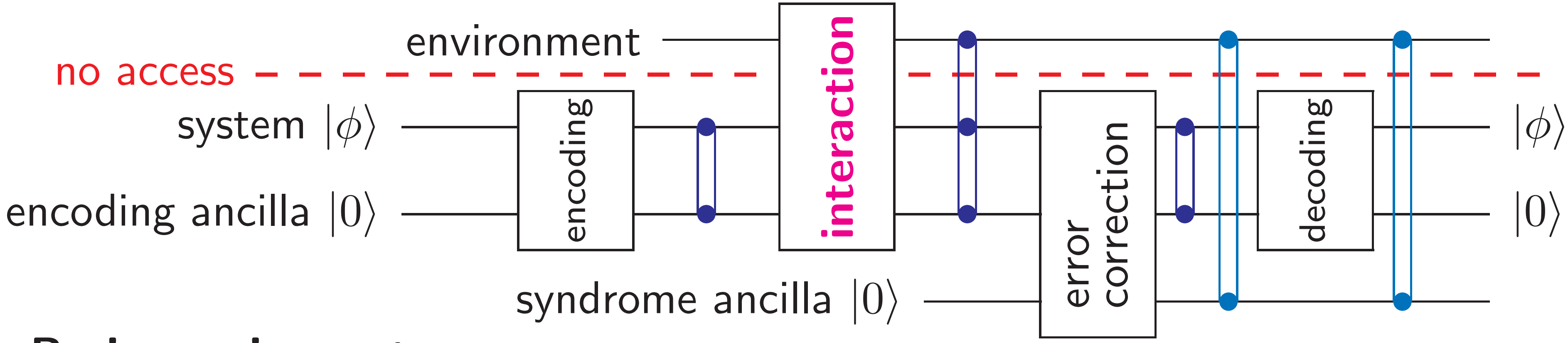
# Quantum Error Correction

## General scheme



# Quantum Error Correction

## General scheme




## Basic requirement

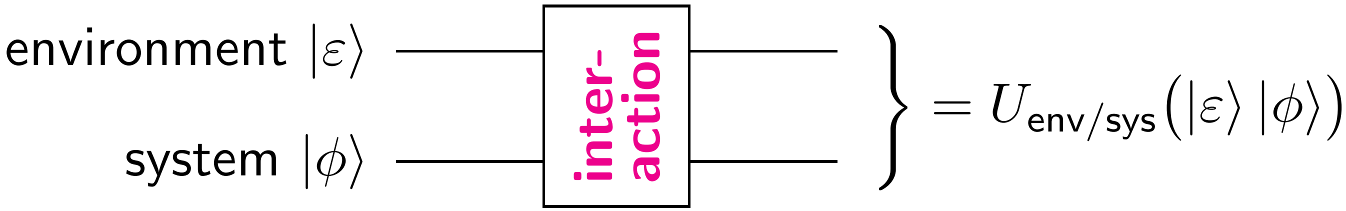
some knowledge about the interaction between system and environment

## 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"

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

with Kraus operators (error operators) $E_i$

## Local/low correlated errors

- product channel $\mathrm{Q}^{\otimes n}$ 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 $\mathcal{E}$.

# Discretization of Quantum Errors

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

"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:** 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

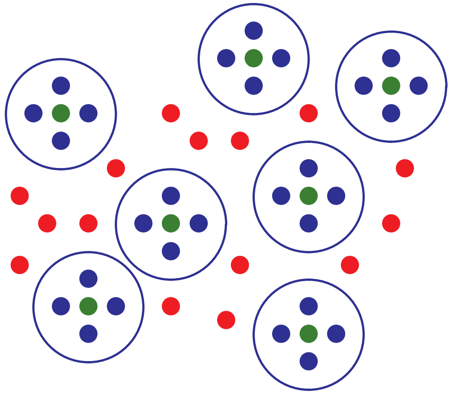
**but**: unknown quantum states can neither be copied

nor can they be disturbance-free compared

# The Basic Idea

## Classical codes

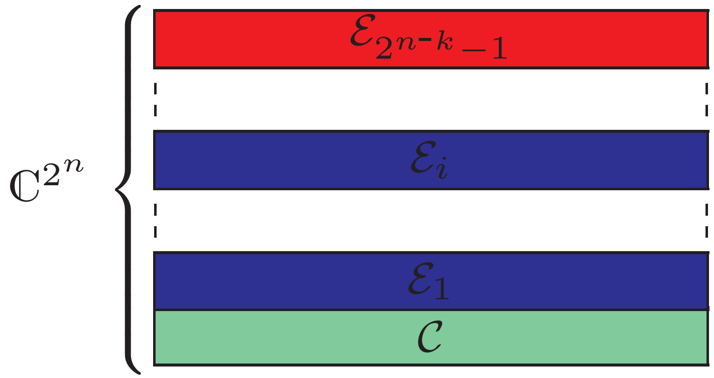
Partition of the set of all words of length $n$ over an alphabet of size $2$.



- 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 $\mathcal{H}_\mathcal{C} \le \mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2$

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

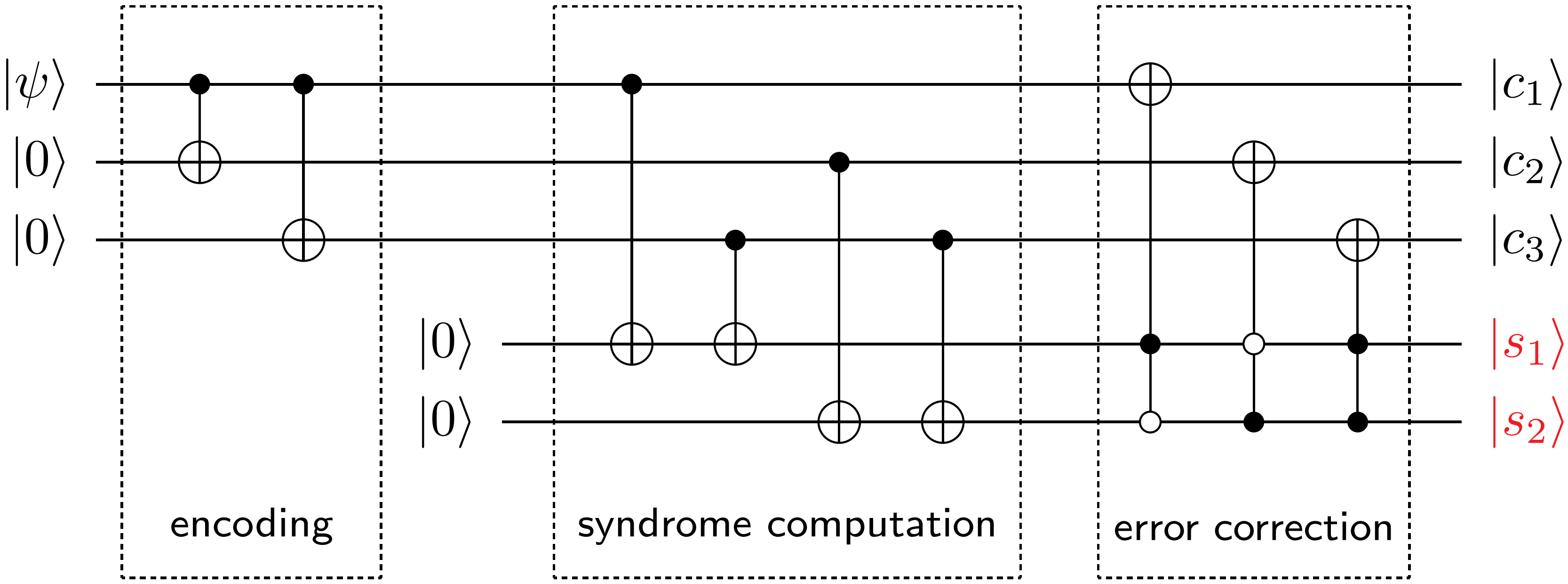
$$\begin{aligned} |0\rangle &\mapsto (H \otimes H \otimes H)\tfrac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = \tfrac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle) \\ |1\rangle &\mapsto (H \otimes H \otimes H)\tfrac{1}{\sqrt{2}}(|000\rangle - |111\rangle) = \tfrac{1}{2}(|001\rangle + |010\rangle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

# Simple Quantum Error-Correcting Code

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

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

# 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 $|0\rangle$.

# 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 $\alpha, \beta$.

# Shor's Nine-Qubit Code

**Hadamard basis:**

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

**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:

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

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

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:** $|0\rangle \mapsto |000\rangle$, $|1\rangle \mapsto |111\rangle$

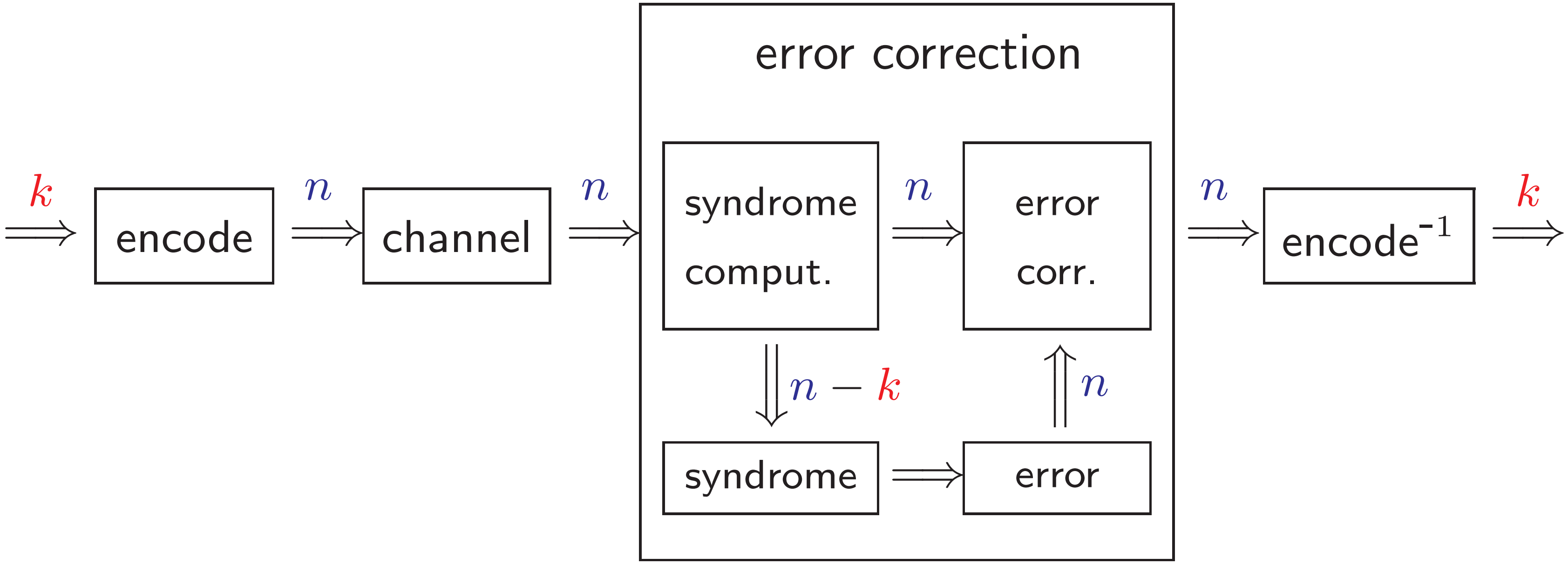
**Effect of single-qubit errors:**

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

$$\left.\begin{array}{rcr} Z\,|000\rangle & = & |000\rangle \\ Z\,|111\rangle & = & -\,|111\rangle \end{array}\right\} \text{"encoded" } Z\text{-operator}$$

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

# Encoding/Decoding: Overview




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

# General Decoding Algorithm

$$
\begin{array}{c|ccccc}
 & E_1\mathcal{C} & E_2\mathcal{C} & \cdots & E_k\mathcal{C} & \cdots \\
\hline
\mathcal{V}_0 & E_1\left|c_0\right\rangle & E_2\left|c_0\right\rangle & \cdots & E_k\left|c_0\right\rangle & \cdots \\
\mathcal{V}_1 & E_1\left|c_1\right\rangle & E_2\left|c_1\right\rangle & \cdots & E_k\left|c_1\right\rangle & \cdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \\
\mathcal{V}_i & E_1\left|c_i\right\rangle & E_2\left|c_i\right\rangle & \cdots & E_k\left|c_i\right\rangle & \cdots \\
\vdots & \vdots & \vdots & & \vdots & \ddots
\end{array}
$$

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

# General Decoding Algorithm

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

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

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

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

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

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

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

rows are mutually orthogonal

columns are mutually orthogonal

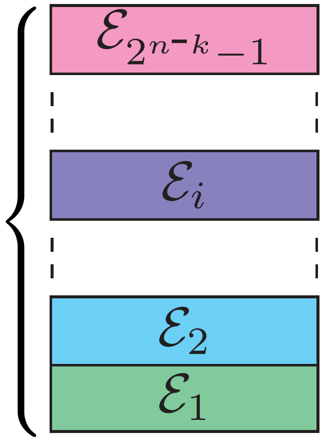
- new error operators $E'_k$ are linear combinations of the $E_l$
- projection onto $E'_k\mathcal{C}$ determines the error
- exponentially many orthogonal spaces $E'_k\mathcal{C}$

# 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

# 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 $\mathcal{C} \le \mathbb{C}^{2^n}$ 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!

# 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: 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

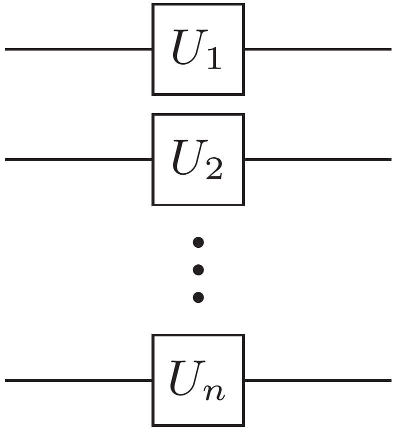
Good: $Z \otimes Z \otimes I$ since
$$Z \otimes Z \otimes I\,|111\rangle = |111\rangle$$
$$Z \otimes Z \otimes I\,|000\rangle = |000\rangle$$

Bad: $X \otimes I \otimes I$ since
$$X \otimes I \otimes I\,|111\rangle = |011\rangle$$
$$X \otimes I \otimes I\,|000\rangle = |100\rangle$$

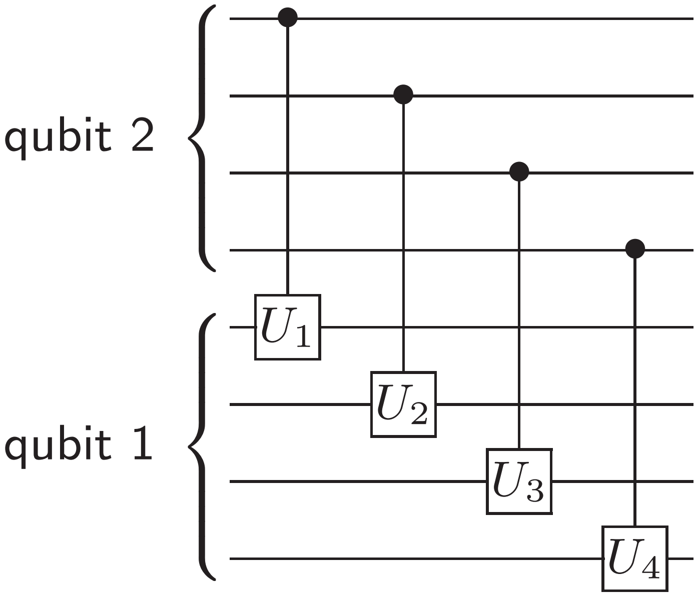
Ugly: $X \otimes X \otimes X$ since $X \otimes X \otimes X\,|111\rangle = |000\rangle$

# Key Ideas: Fault Tolerant Quantum Computing

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




local operations




transversal operations

# Key Ideas: Operator QECC

**QECC:** decomposition $\mathcal{H} = \mathcal{C} \oplus \mathcal{C}^\perp$

**Operator QECC:**

further decomposition $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$, i.e. $\mathcal{H} = (\mathcal{A} \otimes \mathcal{B}) \oplus \mathcal{C}^\perp$

- store information in $\mathcal{A}$
- detect/correct errors in $\mathcal{C}^\perp$
- ignore errors in $\mathcal{B}$

**simplified decoding algorithm**

- embed QECC $\mathcal{A} = [\![n, k, d]\!] \subset \mathcal{C} = [\![n, k, d]\!]$ such that $|x\rangle_{\mathcal{A}} = |x0\ldots0\rangle_{\mathcal{C}}$
- use $\mathcal{C}$ to correct some errors
- if embedding $\mathcal{A} \subset \mathcal{C}$ is properly choosen, remaining errors effect only $|0\ldots0\rangle$

# 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 fr Quantensysteme: Konstruktionen und Algorithmen Aachen: Shaker Verlag, August 2002.
- tables of QECCs:
  `http://www.codetables.de/`
  `http://iaks-www.ira.uka.de/home/grassl/QECC/`
- more specific publications:
  `http://iaks-www.ira.uka.de/home/grassl/publications.html`