網絡編碼研究所
Institute of Network Coding

Quantum Error-Correcting Codes — An Overview

Markus Grassl

7 March 2017

Markus.Grassl@mpl.mpg.de
www.codetables.de

MAX PLANCK INSTITUTE
for the science of light

Overview

- A brief introduction to quantum information & computation
- Basic principles of quantum codes
- Stabilizer quantum codes
- Transformation of stabilizers
- Standard form & encoders
- Graphical representation
- Quantum convolutional codes

Quantum Information

Quantum-bit (qubit)

basis states:

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

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:

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

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

MAX PLANCK INSTITUTE for the science of light

Quantum Information

Quantum register: generalization to higher dimensional systems

basis states:

$$|b_1\rangle \otimes \ldots \otimes |b_n\rangle =: |b_1 \ldots b_n\rangle = |\boldsymbol{b}\rangle \qquad \text{where } b_i \in \mathbb{F}_q$$

general state:

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

$\longrightarrow$ normalized vector in $(\mathbb{C}^q)^{\otimes n} \cong \mathbb{C}^{q^n} \cong \mathbb{C}[\mathbb{F}_q^n]$

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.

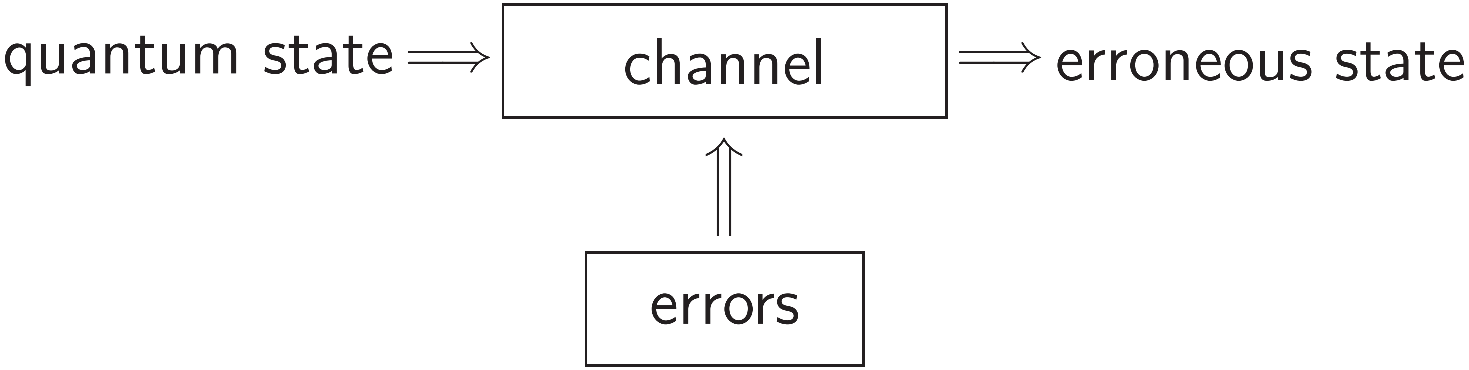
Proof: The copier would map $|0\rangle|\psi_{\text{in}}\rangle \mapsto |0\rangle|0\rangle$, $|1\rangle|\psi_{\text{in}}\rangle \mapsto |1\rangle|1\rangle$, and hence

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

Contradiction to the linearity of quantum mechanics!

QECCs: The Basic Problem

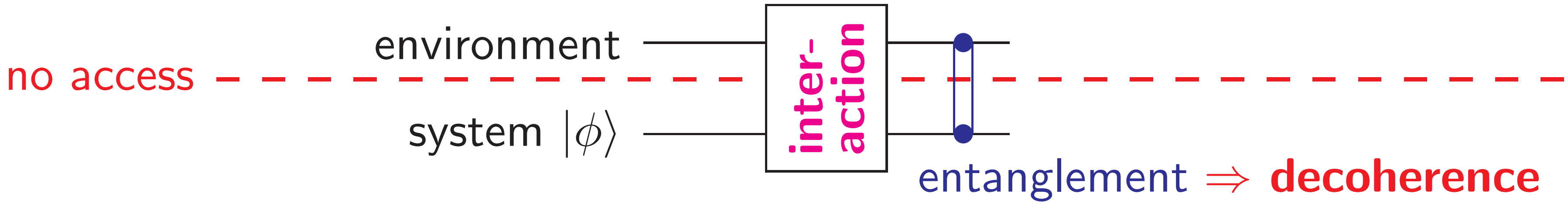
storage
transmission } of quantum information



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

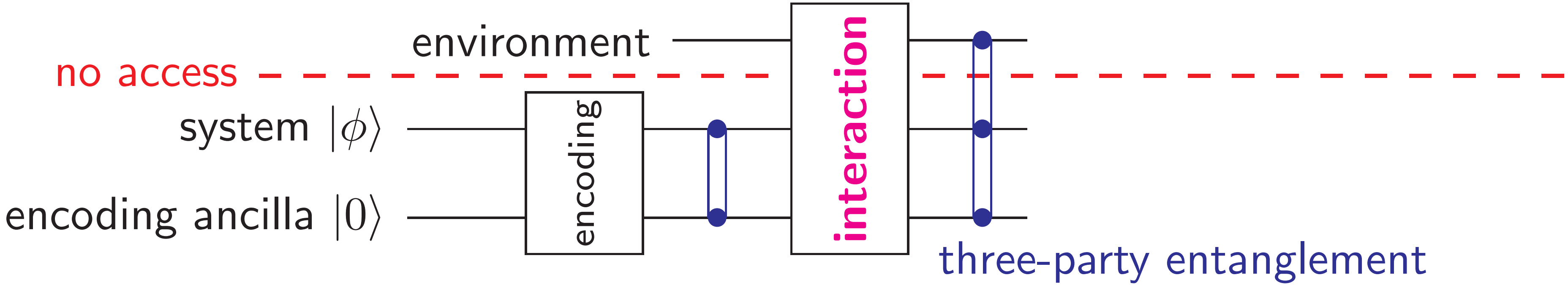
Quantum Error Correction

General scheme



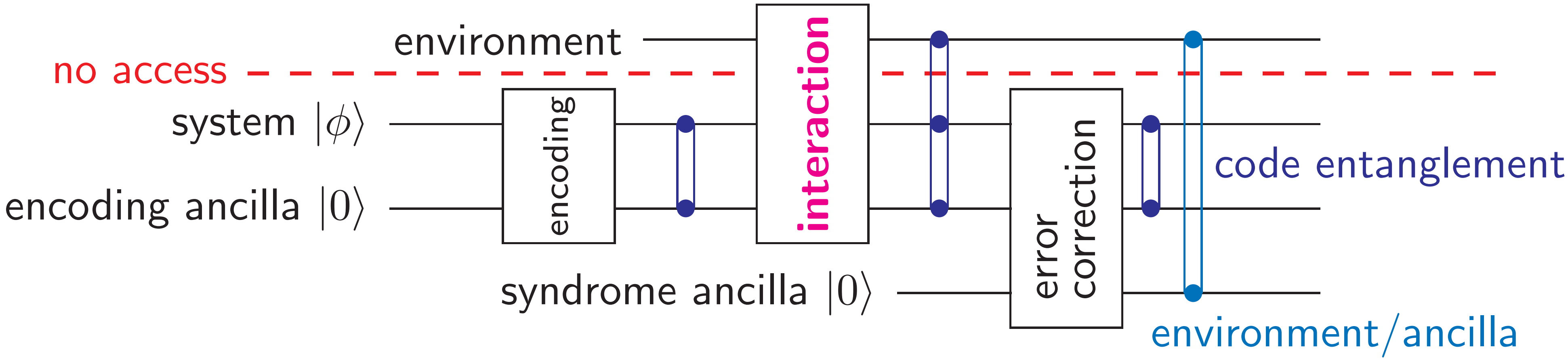
Quantum Error Correction

General scheme



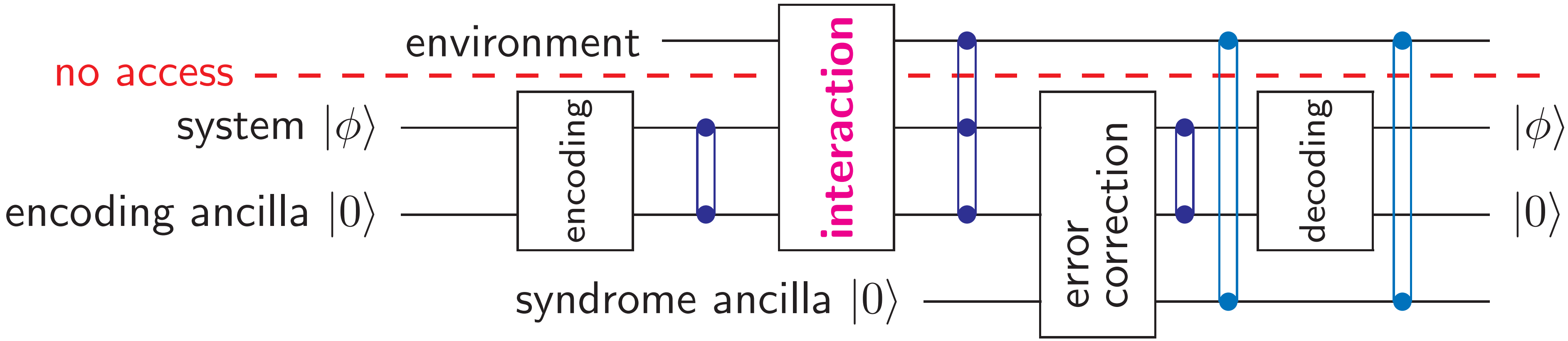
Quantum Error Correction

General scheme



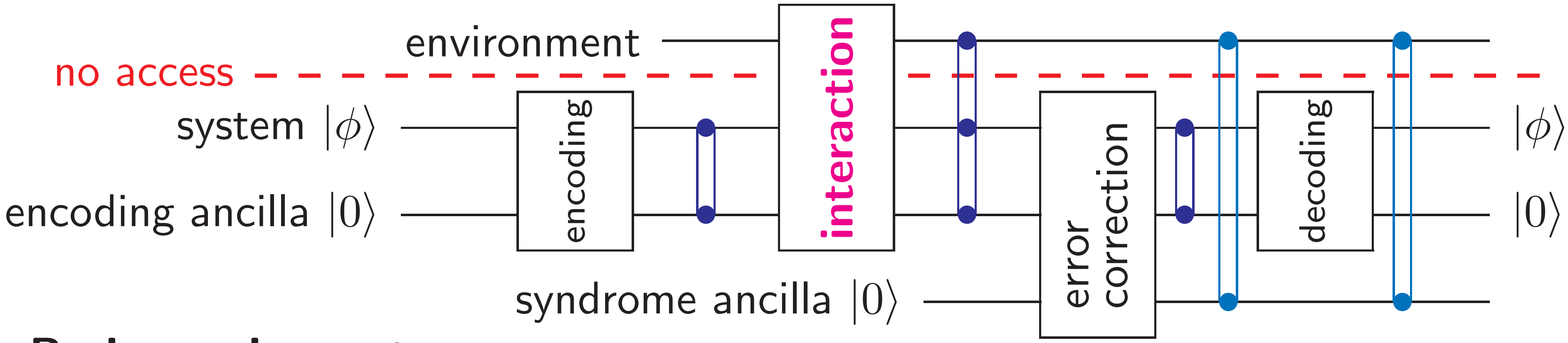
Quantum Error Correction

General scheme



Quantum Error Correction

General scheme



Basic requirement

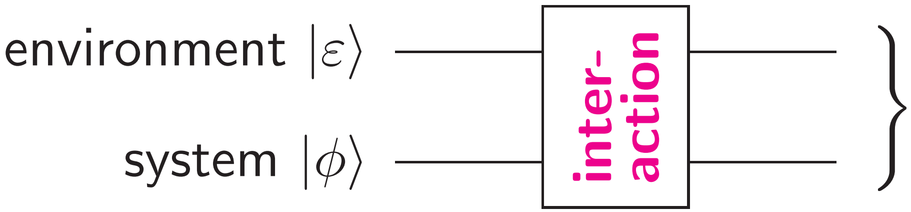
some knowledge about the interaction between system and environment

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



$$= U_{\text{env/sys}}\big(|\varepsilon\rangle|\phi\rangle\big)$$

"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

MAX PLANCK INSTITUTE
for the science of light

Computer Science Approach: Discretize

QECC Characterization

[E. Knill & R. 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 $\mathcal{E}$.

$\Longrightarrow$ 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 $E_i \neq I$

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

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 *nontrivially* on $d - 1$ subsystems
  - correction of errors acting on $\lfloor (d-1)/2 \rfloor$ subsystems
  - correction of erasures acting on $d - 1$ known subsystems

MAX PLANCK INSTITUTE
for the science of light

Simple Quantum Error-Correcting Code

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

Encoding of one qubit:

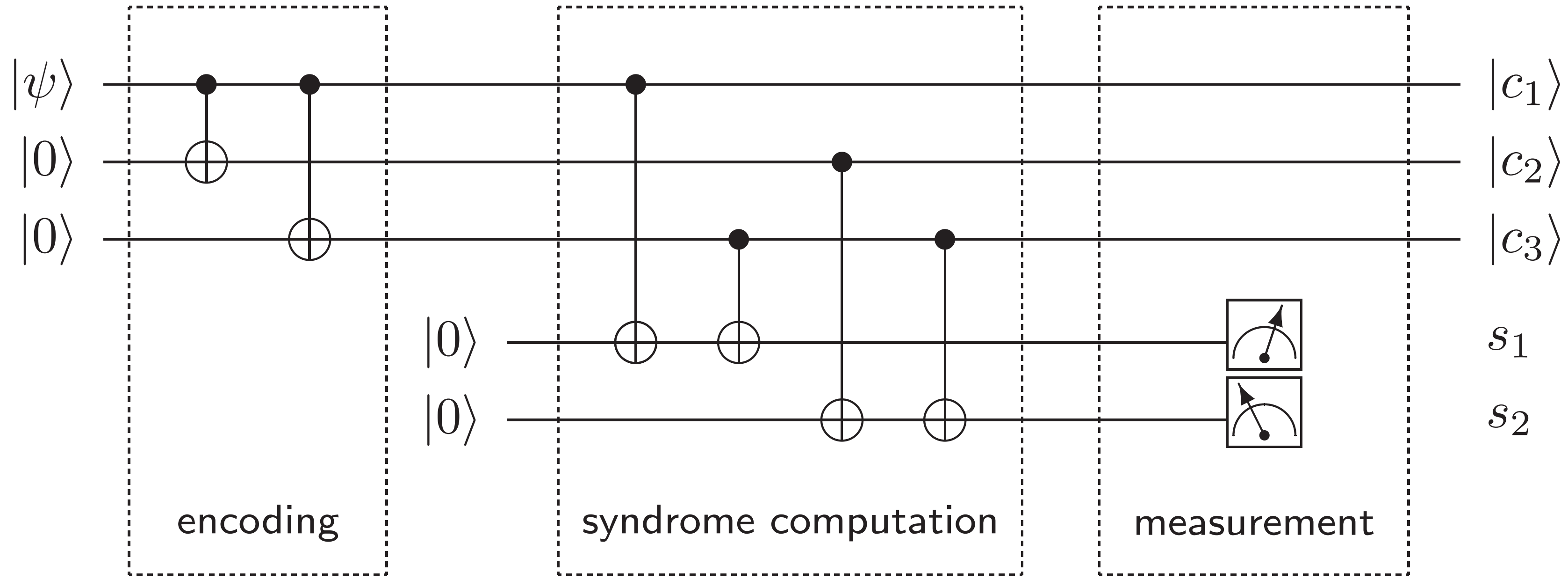
$$\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|000\rangle + \beta|111\rangle.$$

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	$\alpha|000\rangle + \beta|111\rangle$	$(\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1})\mathcal{H}_\mathcal{C}$
1st position	$\alpha|100\rangle + \beta|011\rangle$	$(X \otimes \mathbb{1} \otimes \mathbb{1})\mathcal{H}_\mathcal{C}$
2nd position	$\alpha|010\rangle + \beta|101\rangle$	$(\mathbb{1} \otimes X \otimes \mathbb{1})\mathcal{H}_\mathcal{C}$
3rd 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

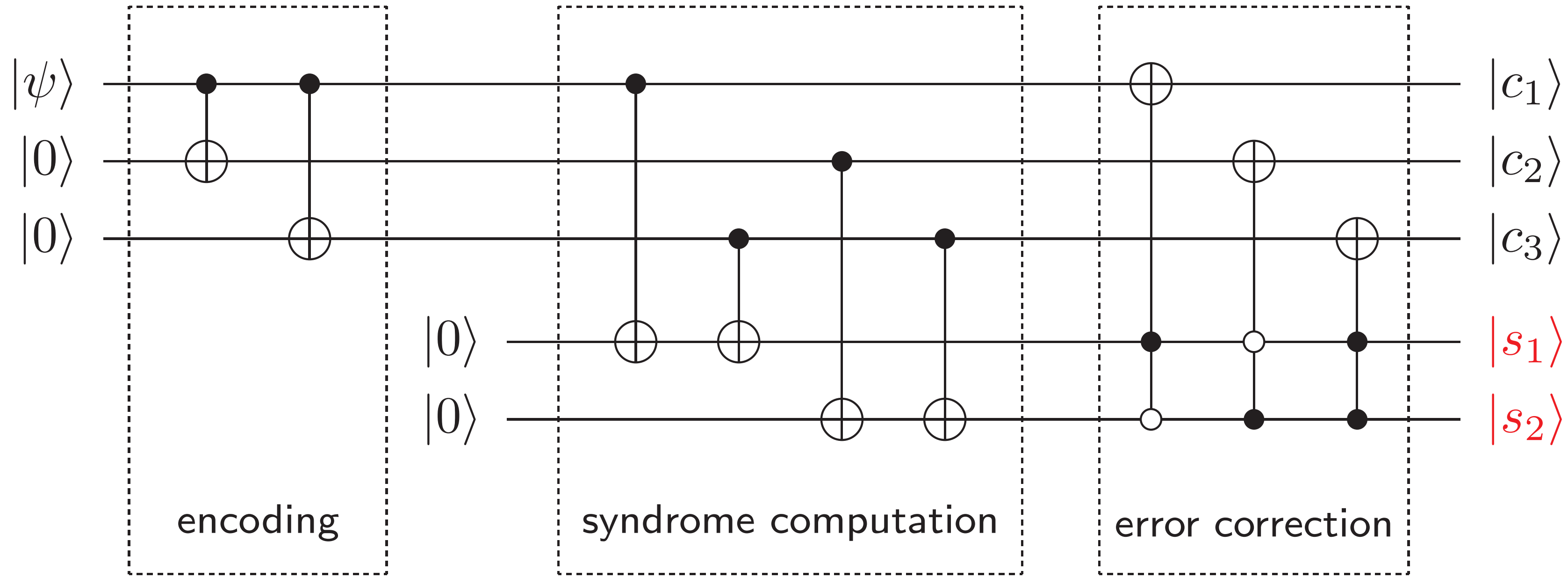


Error $X \otimes I \otimes I$ gives syndrome $s_1 s_2 = 10$

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

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

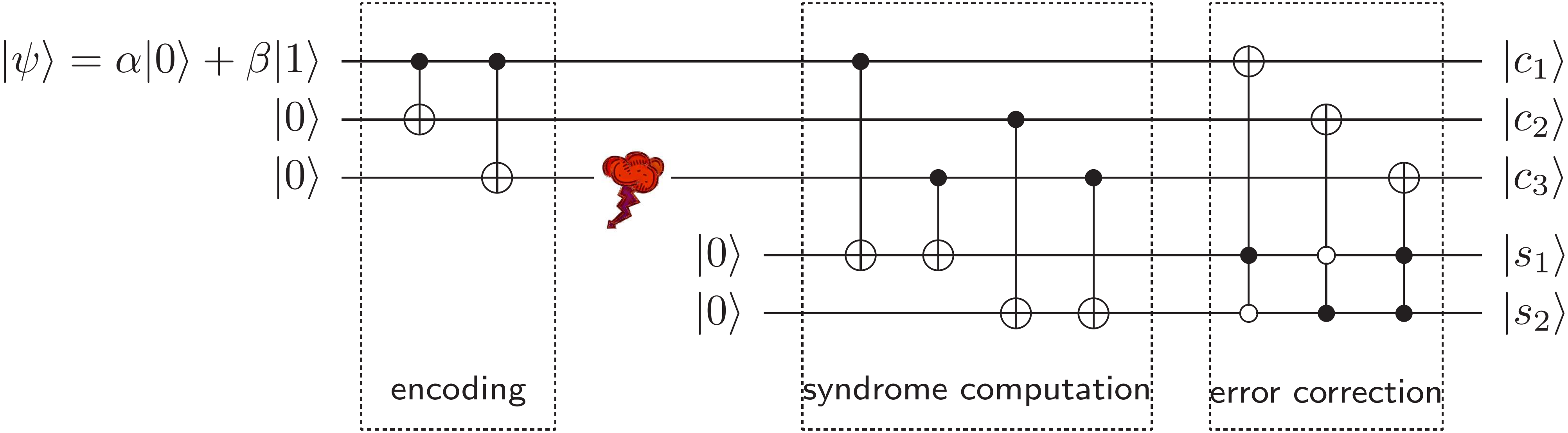
Simple Quantum Error-Correcting Code



- 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 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ happens.



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

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

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

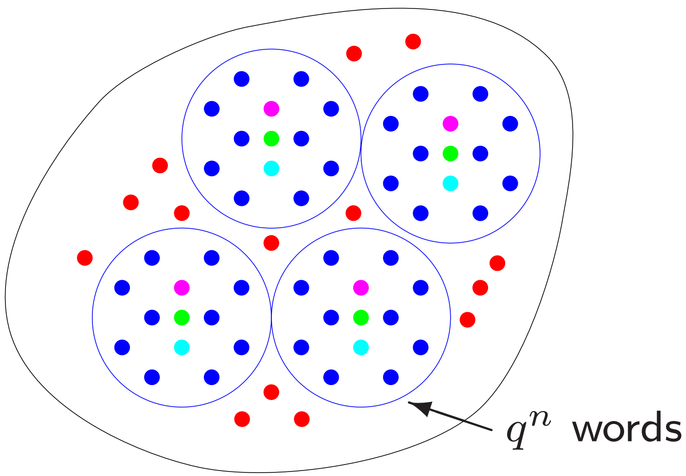
Correction maps this to $\quad \alpha|00011\rangle + \beta|11111\rangle = |\psi_{\text{enc}}\rangle|11\rangle$

Basic Ideas

partitioning of all words

– combinatorics

– (linear) algebra

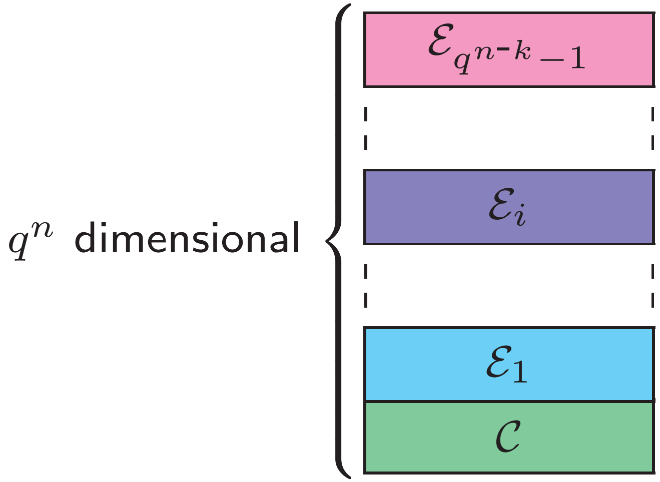


codewords

bounded weight errors

other errors

orthogonal decomposition



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

MAX PLANCK INSTITUTE for the science of light

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

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

special cases:

$\mathbb{F}_q$-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: ([A. Ashikhmin & E. Knill, IEEE-IT **47**, pp. 3065–3072 (2001)])
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 $\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$)

MAX PLANCK INSTITUTE
for the science of light

Stabilizer Group & Stabilizer Matrix

Example: $\mathcal{C} = [\![6, 2, 3]\!]_3$

stabilizer group

$$\mathcal{S} = \langle X \otimes I \otimes X^2Z \otimes Z^2 \otimes Z \otimes X^2Z,\ Z \otimes I \otimes X \otimes X^2Z^2 \otimes XZ \otimes X,$$
$$I \otimes X \otimes Z \otimes Z^2 \otimes Z^2 \otimes Z^2,\ I \otimes Z \otimes XZ \otimes X^2Z^2 \otimes X^2Z^2 \otimes X^2Z^2\rangle$$

stabilizer matrix

$$(X|Z) = \left(\begin{array}{cccccc|cccccc} 1 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 1 & 2 & 1 & 1 \\ 0 & 0 & 1 & 2 & 1 & 1 & 1 & 0 & 0 & 2 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 \\ 0 & 0 & 1 & 2 & 2 & 2 & 0 & 1 & 1 & 2 & 2 & 2 \end{array}\right)$$

Encoding Stabilizer Codes

[M. Grassl, M. Rötteler, and Th. Beth, IJFCS, **14** (2003), pp. 757–775]

Basic idea:

Use operations of the *generalized Clifford group* to transform the stabilizer S into a trivial stabilizer $S_0 := \left\langle Z^{(1)}, \ldots Z^{(n-k)} \right\rangle$.

$$\Longrightarrow \text{trivial code } |\underbrace{0\ldots0}_{n-k}\rangle|\psi\rangle$$

- row/column operations on the matrix $(X|Z)$ to obtain "normal form" $(\,0\,|\,I\;0\,)$
- operations on $(X|Z)$ correspond to
  - "elementary" single-qubit gates
  - CNOT-gate
  - single qudit gate $P := \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \in \mathbb{C}^{2\times 2}$

MAX PLANCK INSTITUTE
for the science of light

Action on Pauli Matrices

Hadamard matrix H	$HXH = Z$ $(1,0) \mapsto (0,1)$	$HYH = -Y$ $(1,1) \mapsto (1,1)$	$HZH = X$ $(0,1) \mapsto (1,0)$
	exchange X and Z		
matrix P	$P^\dagger XP = -Y$ $(1,0) \mapsto (1,1)$	$P^\dagger YP = X$ $(1,1) \mapsto (1,0)$	$P^\dagger ZP = Z$ $(0,1) \mapsto (0,1)$
	multiply X by Z		

in $\mathbb{C}$

$\bmod 2$

operation on binary row vectors: $(a,b)\widetilde{M} = (a',b')$ (arithmetic $\bmod 2$)

$$\widetilde{H} \mathrel{\hat{=}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \widetilde{P} \mathrel{\hat{=}} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

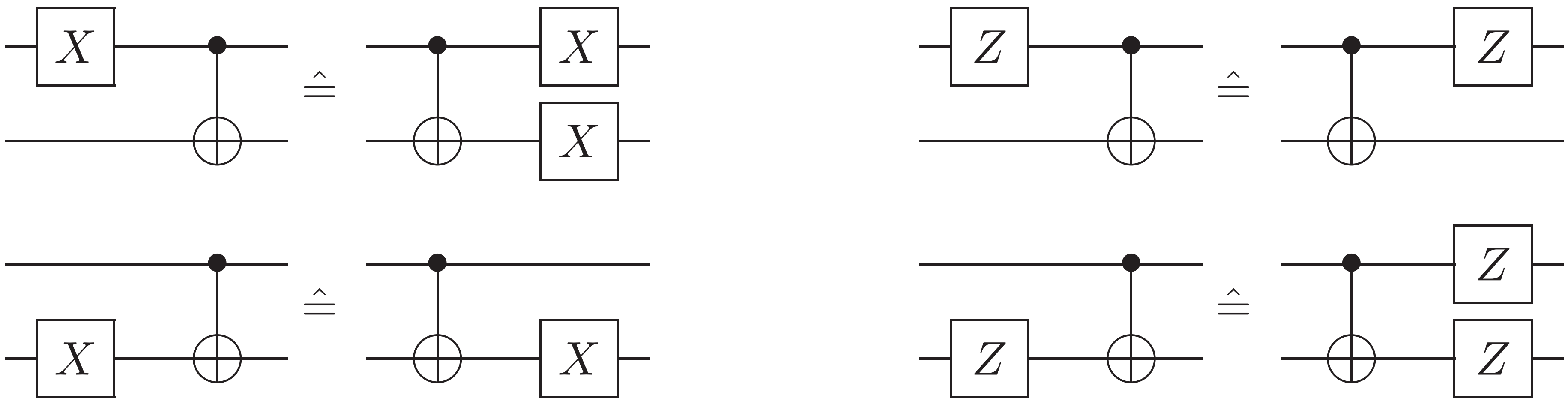
local operation on $(X|Z)$:

multiplying column i in submatrix X and column i in submatrix Z by $\widetilde{M}$

MAX PLANCK INSTITUTE for the science of light

Action of CNOT

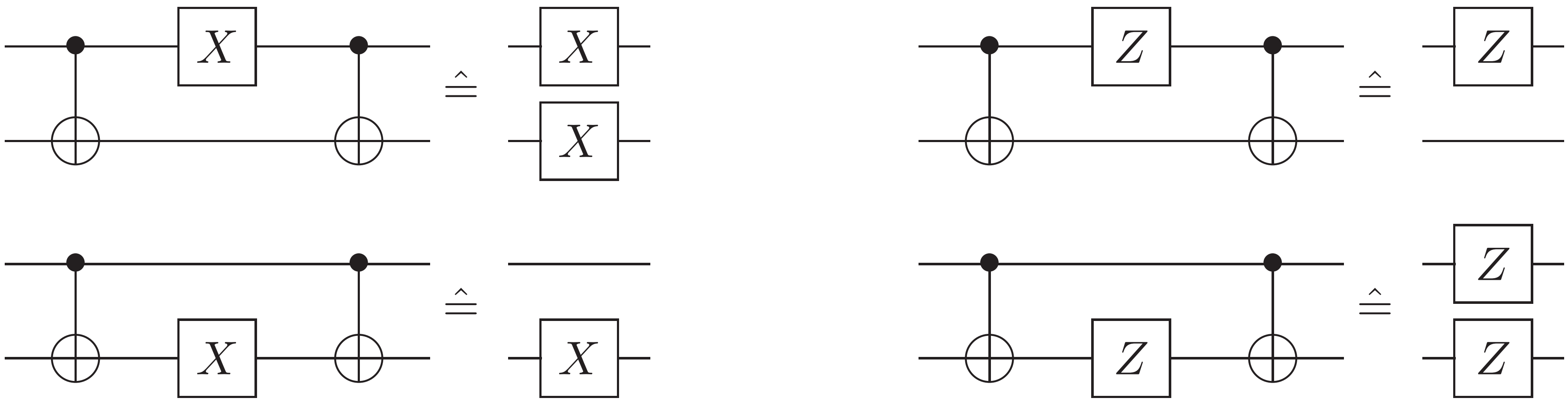
Error propagation



MAX PLANCK INSTITUTE
for the science of light

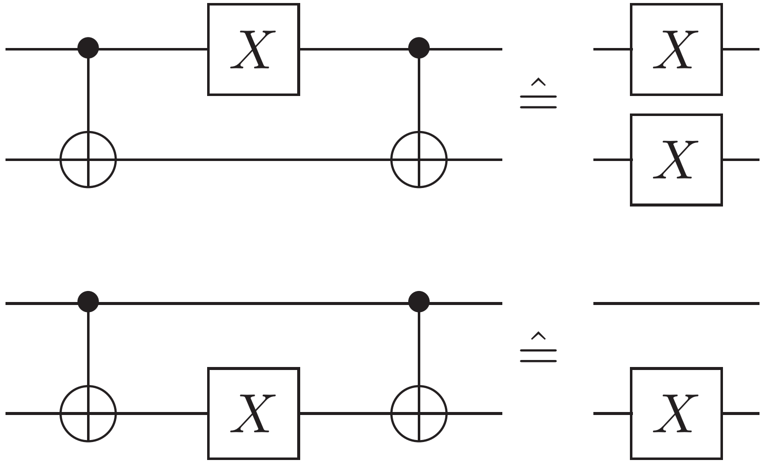
Action of CNOT

Modifying stabilizers

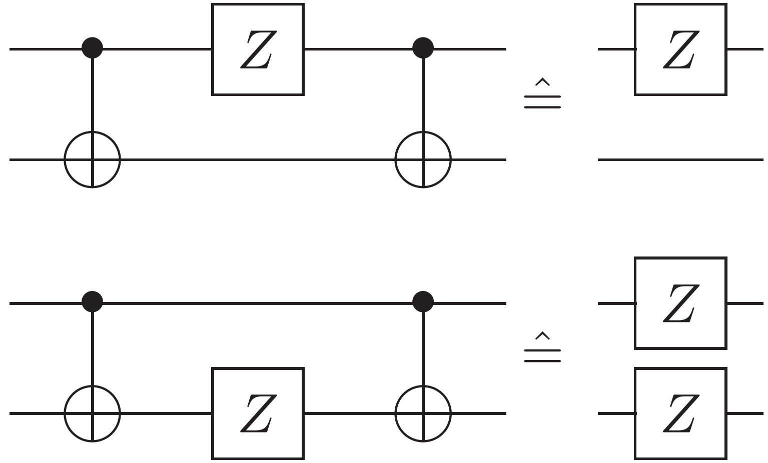


Action of CNOT

Modifying stabilizers



add X from source to target



add Z from target to source

Graphical Quantum Codes

[D. Schlingemann & R. F. Werner: QECC associated with graphs, PRA **65** (2002)]
[Grassl, Klappenecker, & Rötteler: Graphs, Quadratic Forms, & Quantum Codes, ISIT 2002]

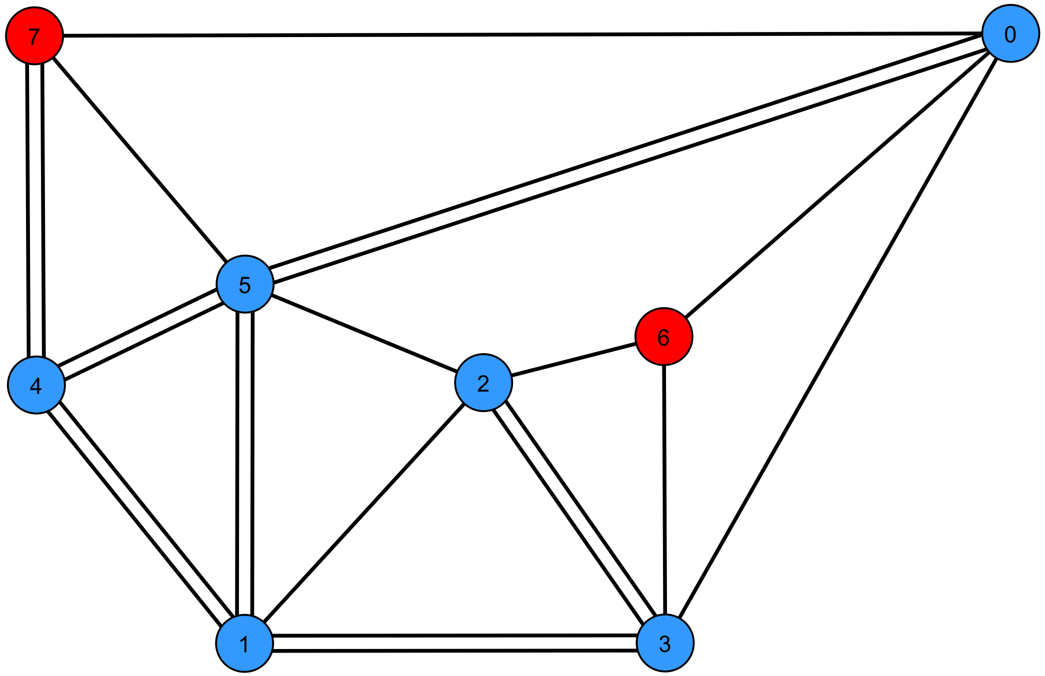
Basic idea

- a classical symplectic self-dual code defines a single quantum state $\mathcal{C}_0 = [\![n, 0, d]\!]_q$
- the standard form of the stabilizer matrix is $(I|C)$
- the generators have exactly one tensor factor X
- self-duality implies that C is symmetric
- C can be considered as adjacency matrix of a graph with n vertices
- so-called *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: $[\![6,2,3]\!]_3$

$$\left(\begin{array}{cccccc|cccccc}
1&0&0&0&0&0&0&0&0&1&0&2\\
0&1&0&0&0&0&0&0&1&2&2&2\\
0&0&1&0&0&0&0&1&0&2&0&1\\
0&0&0&1&0&0&1&2&2&0&0&0\\
0&0&0&0&1&0&0&2&0&0&0&2\\
0&0&0&0&0&1&2&2&1&0&2&0\\
\hline
0&0&0&0&0&0&1&0&1&1&0&0\\
0&0&0&0&0&0&1&0&0&0&2&1
\end{array}\right)$$

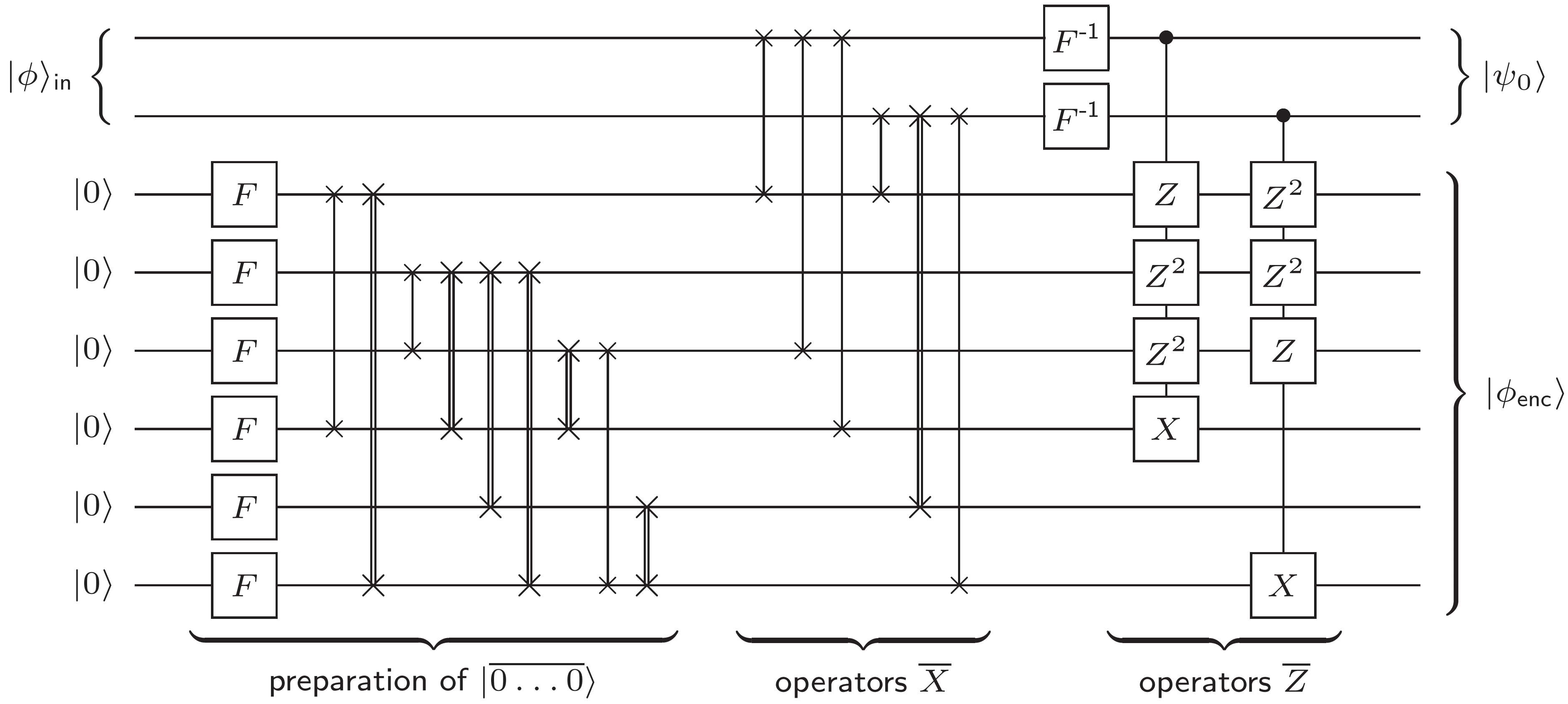
stabilizer & logical X-operators



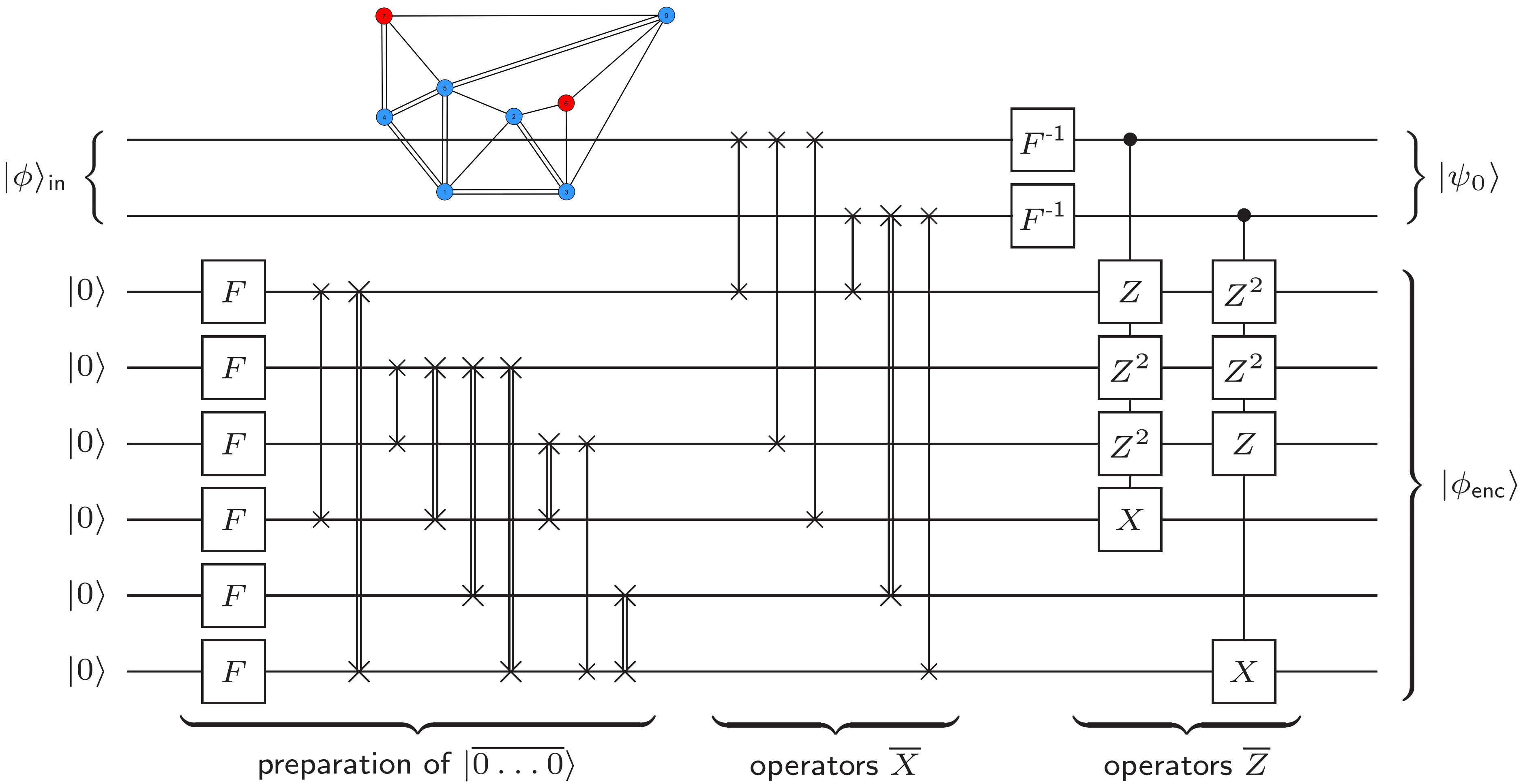
graphical representation

Encoder based on Graphical Representation

[Grassl, LNCS 6639, pp. 142–158, Springer, 2011]



Encoder based on Graphical Representation



Quantum Convolutional Codes

[M. Grassl and M. Rötteler, "On encoders for quantum convolutional codes", ITW 2010]

Quantum Block Codes

The code is the common eigenspace of the stabilizers.

Quantum Convolutional Codes

Idea: impose local constraints by stabilizers

Example:

$$s_1 = \ldots\ III\ XXX\ XZY\ III\ III\ \ldots$$
$$s_2 = \ldots\ III\ ZZZ\ ZYX\ III\ III\ \ldots$$

shift the stabilizers by three qubits:

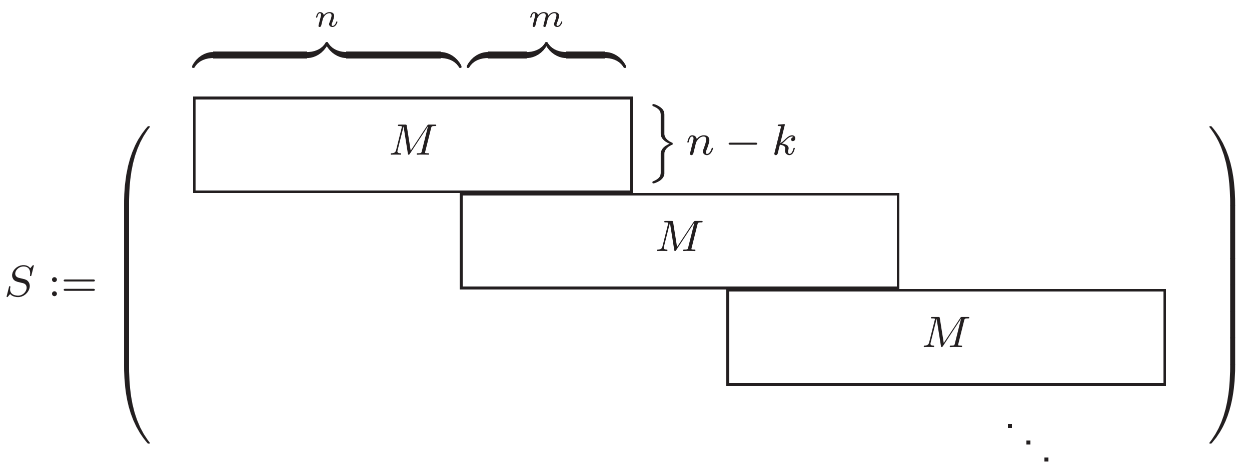
$$s_1' = \ldots\ III\ III\ XXX\ XZY\ III\ \ldots$$
$$s_2' = \ldots\ III\ III\ ZZZ\ ZYX\ III\ \ldots$$

Quantum Convolutional Codes (QCCs)

[H. Ollivier and J.-P. Tillich, "Quantum convolutional codes: fundamentals," Nov. 2004, preprint quant-ph/0401134.]

quantum convolutional code with parameters (n, k, m):

- semi-infinite stabilizer with block band structure



- S generates a self-orthogonal classical convolutional code
- M generates a self-orthogonal classical block code

Semi-infinite Stabilizer

Compact representation of the semi-infinite stabilizer matrix

$$
\begin{pmatrix}
XXX & XZY & & \\
ZZZ & ZYX & & \\
 & XXX & XZY & \\
 & ZZZ & ZYX & \\
 & & & \ddots
\end{pmatrix}
$$

$$
\hat{=} \left(\begin{array}{cccc|cccc}
111 & 101 & & & 000 & 011 & & \\
000 & 011 & & & 111 & 110 & & \\
 & 111 & 101 & & & 000 & 011 & \\
 & 000 & 011 & & & 111 & 110 & \\
 & & & \ddots & & & & \ddots
\end{array}\right)
$$

$$
\hat{=} \left(\begin{array}{ccc|ccc}
1+D & 1 & 1+D & 0 & D & D \\
0 & D & D & 1+D & 1+D & 1
\end{array}\right) = \mathbf{S}(D)
$$

Quantum Convolutional Codes

Quantum Block Codes

The stabilizer $\mathcal{S}$ corresponds to a binary code generated by the stabilizer matrix $(\mathbf{X}|\mathbf{Z})$.

Quantum Convolutional Codes

The semi-infinite stabilizer corresponds to a binary convolutional code generated by the matrix $\big(\mathbf{X}(D) \;\big|\; \mathbf{Z}(D)\big)$ with

$$\mathbf{X}(D)\mathbf{Z}(1/D)^t - \mathbf{Z}(D)\mathbf{X}(1/D)^t = \mathbf{0}$$

Example:

$$\mathbf{S}(D) = \left(\begin{array}{ccc|ccc} 1+D & 1 & 1+D & 0 & D & D \\ 0 & D & D & 1+D & 1+D & 1 \end{array}\right)$$

Catastrophic (Quantum) Convolutional Codes

Bad example:

$$\begin{pmatrix} Z & Z & & & \\ & Z & Z & & \\ & & Z & Z & \\ & & & & \ddots \end{pmatrix} \hat{=} \left(0 \,|1+D \right) = \mathbf{S}(D)$$

Quantum code with basis states $|\underline{0}\rangle = |000\ldots\rangle$ and $|\underline{1}\rangle = |111\ldots\rangle$, contains in particular "infinite cat state"

$\Longrightarrow$ local errors spread unboundedly

$\Longrightarrow$ further constraints on $\mathbf{S}(D)$ (see [Lemma 9, ITW 2010])

Quantum Convolutional Codes: Error Correction

Basic Ideas:

- Every stabilizer has bounded support.
- Measure the eigenvalue of the stabilizer when all correspondings qudits have been received.
  $\Longrightarrow$ syndrome of the corresponding classical convolutional code
- Use your favorite algorithm to decode the classical convolutional code (e. g. Viterbi algorithm).

Operations on $\mathbf{S}(D) = (\mathbf{X}(D)|\mathbf{Z}(D))$

$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \in \mathbb{C}^{2\times 2}$	$\overline{H} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \in \mathbb{F}_2^{2\times 2}$
$P = \begin{pmatrix}1 & 0\\ 0 & \exp(i\pi/2)\end{pmatrix} \in \mathbb{C}^{2\times 2}$	$\overline{P} = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \in \mathbb{F}_2^{2\times 2}$
$\mathrm{CNOT}^{(i,j+\ell n)}, i \not\equiv j \pmod{n}$	$\overline{\mathrm{CNOT}} = \left(\begin{array}{cc\|cc}1 & D^\ell & 0 & 0\\ 0 & 1 & 0 & 0\\ \hline 0 & 0 & 1 & 0\\ 0 & 0 & D^{-\ell} & 1\end{array}\right)$
$P_\ell := \mathrm{CSIGN}^{(i,i+\ell n)}, \ell \neq 0$	$\overline{P_\ell} = \begin{pmatrix}1 & D^{-\ell}+D^\ell\\ 0 & 1\end{pmatrix}$

Quantum Circuits

Single qubit gates

operation on stabilizer matrix in D-transform notation

$\Longrightarrow$ expand to semi-infinite matrix

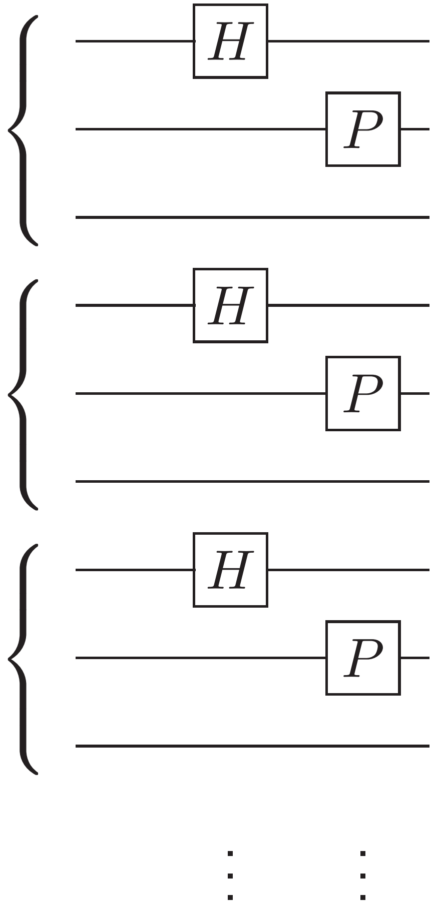
$\Longrightarrow$ repeat the operations infinitely often

Example:

blocks of three qubits each

operation H on first position

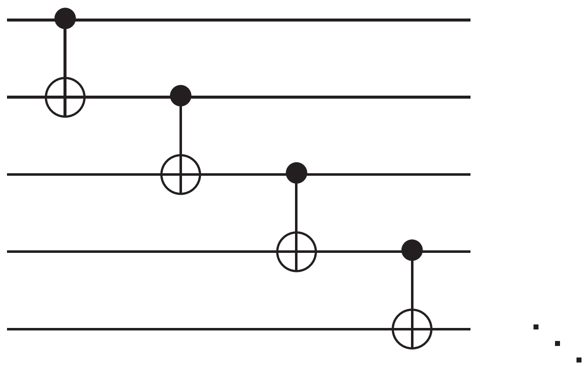
operation P on second position



Quantum Circuits

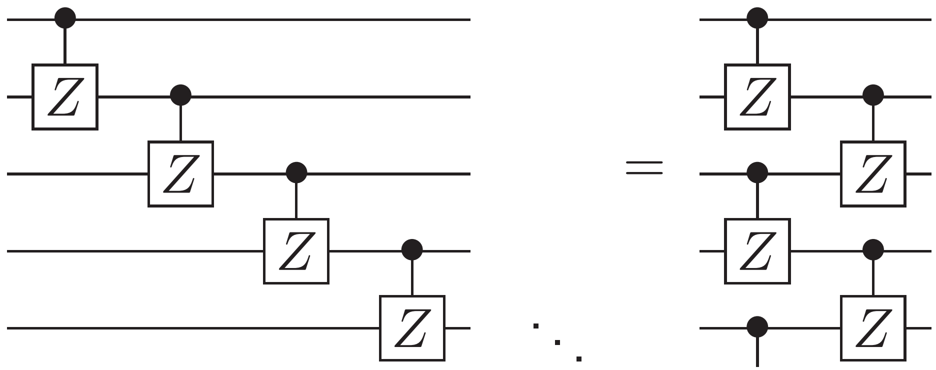
Two-qubit gates

- CNOT on qubit j in block ℓ and qubit j in block $\ell+1$:



$\Longrightarrow$ infinite depth

- CSIGN on qubit j in block ℓ and qubit j in block: $\ell+1$:



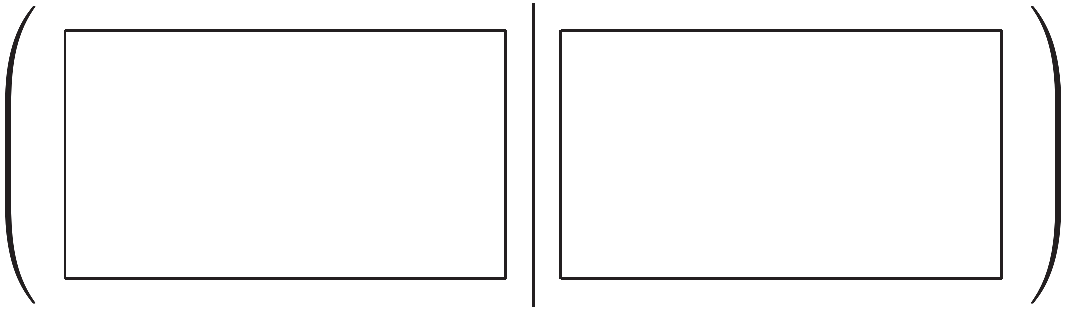
$\Longrightarrow$ finite depth

MAX PLANCK INSTITUTE
for the science of light

Computing an Encoder

basic idea:

transform the stabilizer matrix $(X(D)|Z(D))$ into $(0|\Delta\,0)$



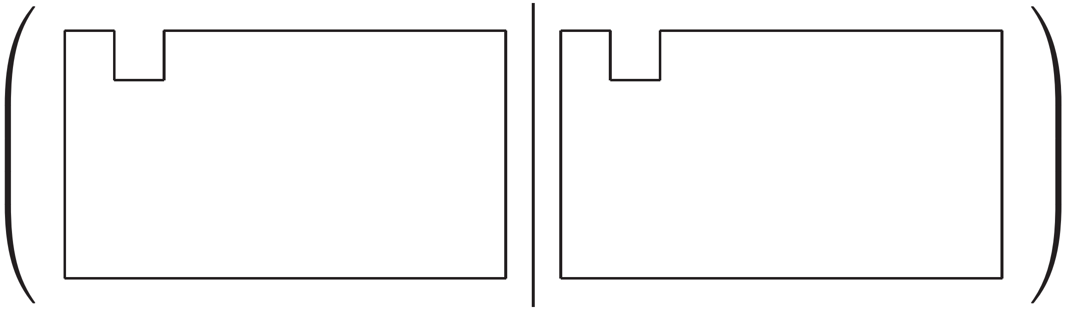
application of [Theorem 7, ITW 2010]

$$\big(f_1(D)\ f_2(D)\mid g_1(D)\ g_2(D)\big) \to \big(f_1'(D)\ 0 \mid g_1'(D)\ 0\big)$$

Computing an Encoder

basic idea:

transform the stabilizer matrix $(X(D)|Z(D))$ into $(0|\Delta\, 0)$



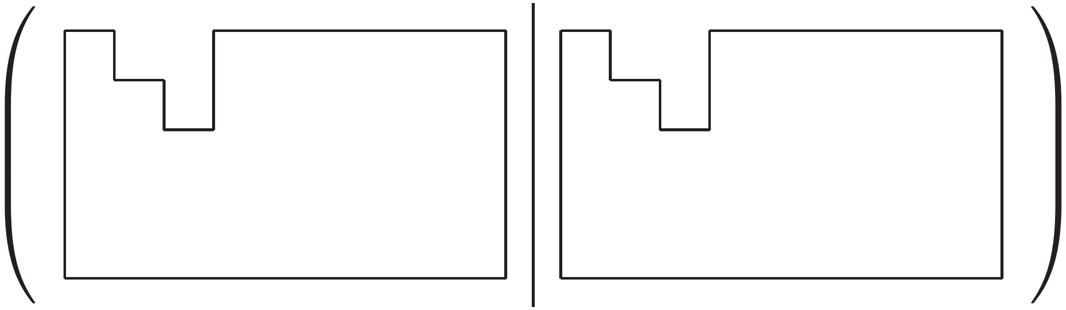
application of [Theorem 7, ITW 2010]

$$\big(f_1(D)\ f_2(D)\mid g_1(D)\ g_2(D)\big) \rightarrow \big(f_1'(D)\ 0 \mid g_1'(D)\ 0\big)$$

Computing an Encoder

basic idea:

transform the stabilizer matrix $(X(D)|Z(D))$ into $(0|\Delta\, 0)$



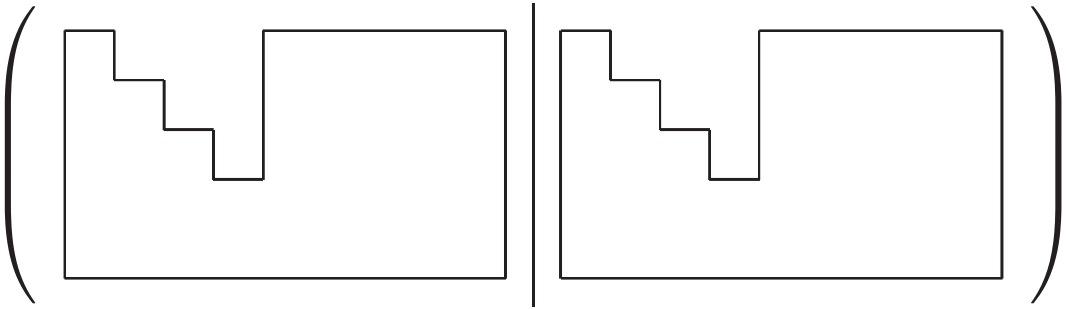
application of [Theorem 7, ITW 2010]

$$\big(f_1(D)\ f_2(D)\ |\ g_1(D)\ g_2(D)\big) \to \big(f_1'(D)\ 0\ |\ g_1'(D)\ 0\big)$$

Computing an Encoder

basic idea:

transform the stabilizer matrix $(X(D)|Z(D))$ into $(0|\Delta\, 0)$



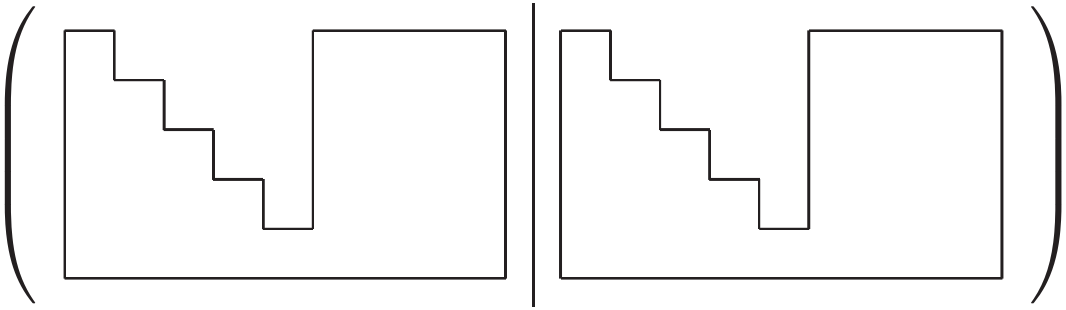
application of [Theorem 7, ITW 2010]

$$\big(f_1(D)\ f_2(D)\ |\ g_1(D)\ g_2(D)\big) \to \big(f_1'(D)\ 0\ |\ g_1'(D)\ 0\big)$$

Computing an Encoder

basic idea:

transform the stabilizer matrix $(X(D)|Z(D))$ into $(0|\Delta\, 0)$



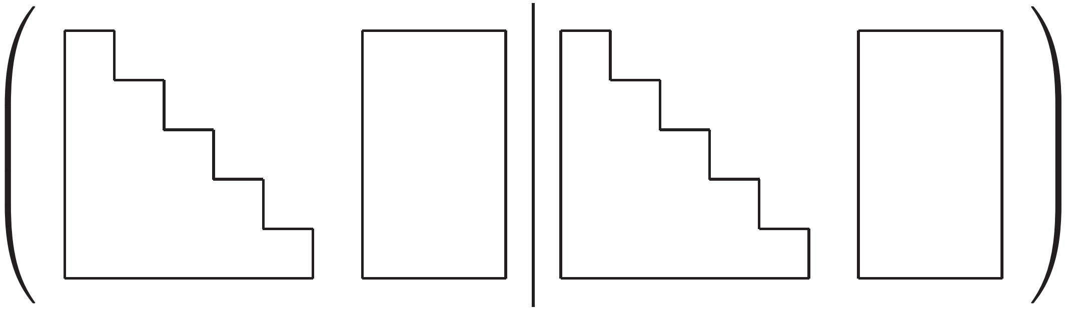
application of [Theorem 7, ITW 2010]

$$\big(f_1(D)\ f_2(D) \mid g_1(D)\ g_2(D)\big) \rightarrow \big(f_1'(D)\ 0 \mid g_1'(D)\ 0\big)$$

Computing an Encoder

basic idea:

transform the stabilizer matrix $(X(D)|Z(D))$ into $(0|\Delta\,0)$



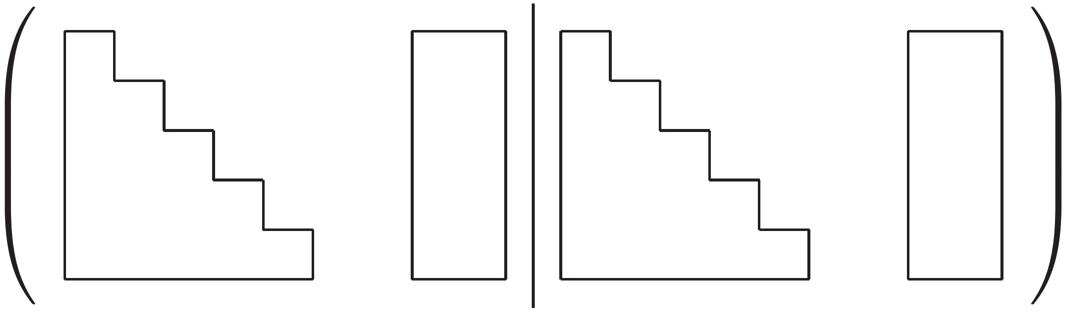
application of [Theorem 7, ITW 2010]

$$\big(f_1(D)\ f_2(D)\ |\ g_1(D)\ g_2(D)\big) \rightarrow \big(f_1'(D)\ 0\ |\ g_1'(D)\ 0\big)$$

Computing an Encoder

basic idea:

transform the stabilizer matrix $(X(D)|Z(D))$ into $(0|\Delta\, 0)$



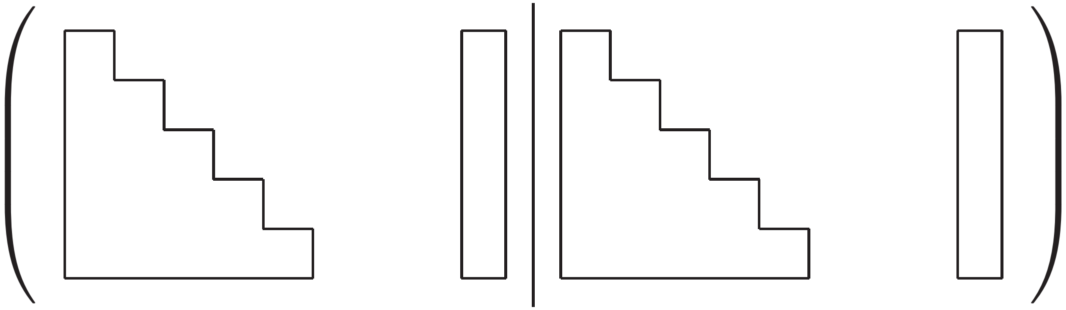
application of [Theorem 7, ITW 2010]

$$\big(f_1(D)\ f_2(D)\mid g_1(D)\ g_2(D)\big)\rightarrow\big(f_1'(D)\ 0\mid g_1'(D)\ 0\big)$$

Computing an Encoder

basic idea:

transform the stabilizer matrix $(X(D)|Z(D))$ into $(0|\Delta\, 0)$



application of [Theorem 7, ITW 2010]

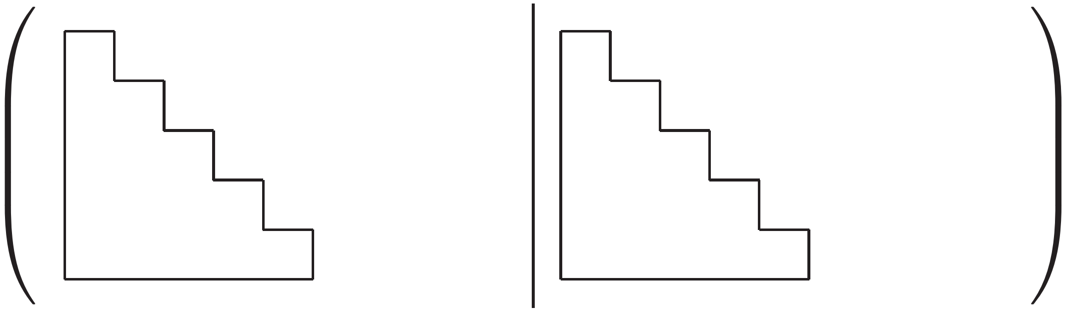
$$\big(f_1(D)\ f_2(D)\mid g_1(D)\ g_2(D)\big) \rightarrow \big(f_1'(D)\ 0 \mid g_1'(D)\ 0\big)$$

MAX PLANCK INSTITUTE for the science of light

Computing an Encoder

basic idea:

transform the stabilizer matrix $(X(D)|Z(D))$ into $(0|\Delta\, 0)$



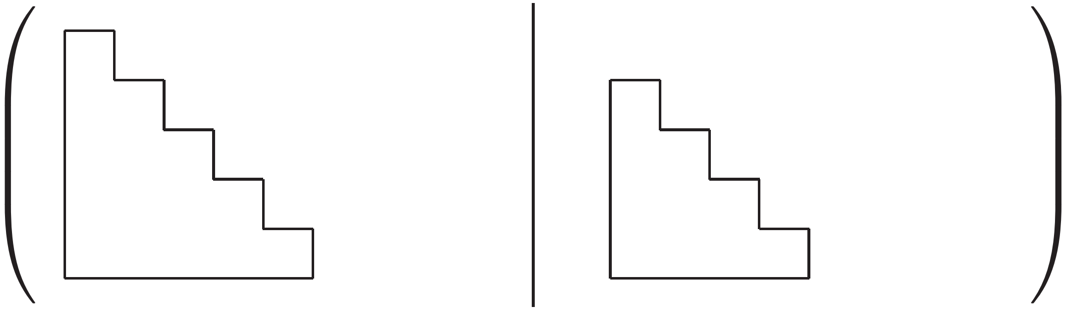
application of [Theorem 7, ITW 2010]

$$\big(f_1(D)\ f_2(D) \mid g_1(D)\ g_2(D)\big) \to \big(f_1'(D)\ 0 \mid g_1'(D)\ 0\big)$$

Computing an Encoder

basic idea:

transform the stabilizer matrix $(X(D)|Z(D))$ into $(0|\Delta\,0)$



application of [Theorem 4, ITW 2010]

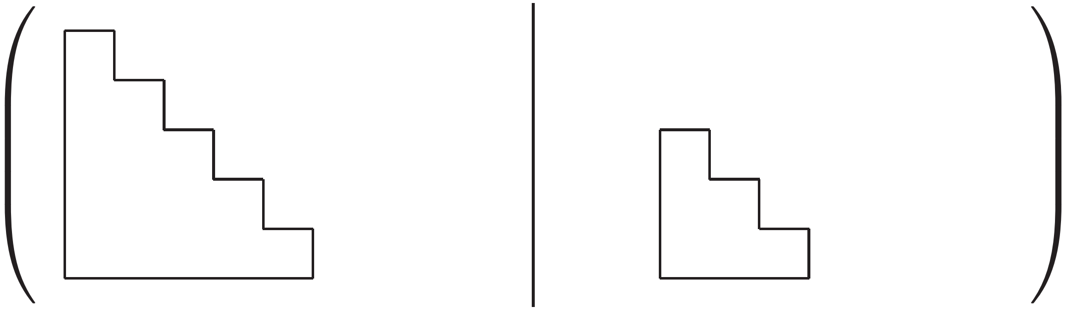
$$\big(f(D) \mid g(D)\big) \rightarrow \big(h(D) \mid 0\big)$$

if $\big(f(D) \mid g(D)\big)$ commute

Computing an Encoder

basic idea:

transform the stabilizer matrix $(X(D)|Z(D))$ into $(0|\Delta\, 0)$



application of [Theorem 4, ITW 2010]

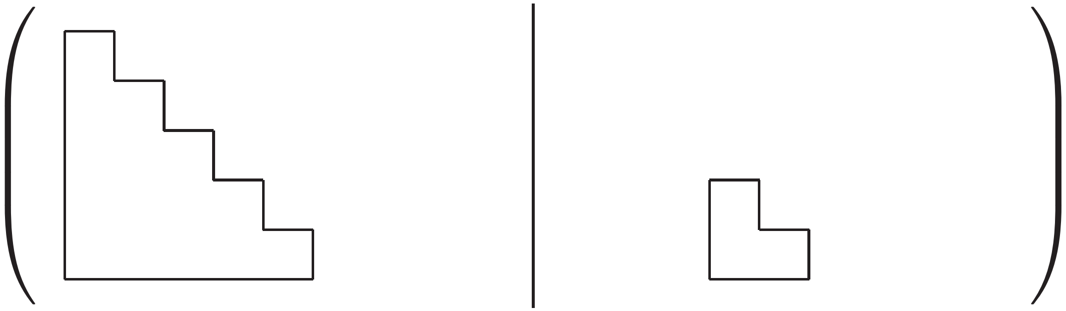
$$\big(f(D) \mid g(D)\big) \to \big(h(D) \mid 0\big)$$

if $\big(f(D) \mid g(D)\big)$ commute

Computing an Encoder

basic idea:

transform the stabilizer matrix $(X(D)|Z(D))$ into $(0|\Delta\,0)$



application of [Theorem 4, ITW 2010]

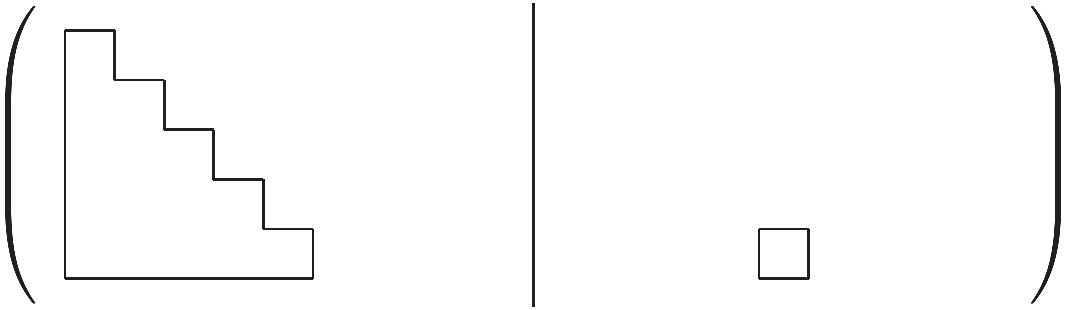
$$\big(f(D) \mid g(D)\big) \to \big(h(D) \mid 0\big)$$

if $\big(f(D) \mid g(D)\big)$ commute

Computing an Encoder

basic idea:

transform the stabilizer matrix $(X(D)|Z(D))$ into $(0|\Delta\, 0)$



application of [Theorem 4, ITW 2010]

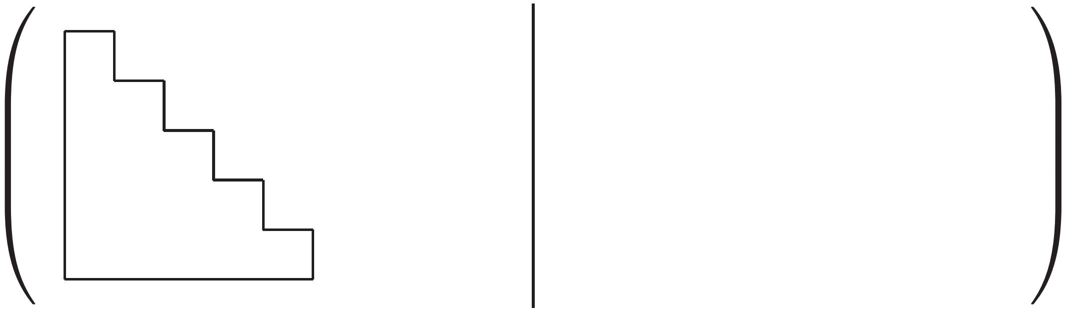
$$\big(f(D) \mid g(D)\big) \to \big(h(D) \mid 0\big)$$

if $\big(f(D) \mid g(D)\big)$ commute

Computing an Encoder

basic idea:

transform the stabilizer matrix $(X(D)|Z(D))$ into $(0|\Delta\ 0)$



application of [Theorem 4, ITW 2010]

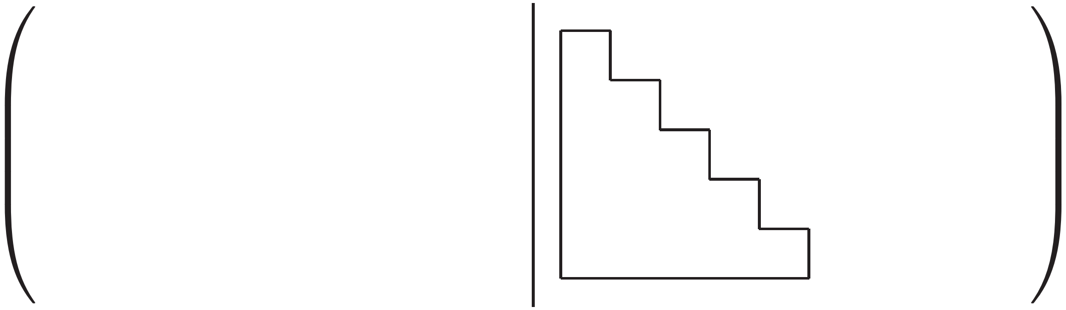
$$\big(f(D) \mid g(D)\big) \to \big(h(D) \mid 0\big)$$

if $\big(f(D) \mid g(D)\big)$ commute

Computing an Encoder

basic idea:

transform the stabilizer matrix $(X(D)|Z(D))$ into $(0|\Delta\, 0)$



Hadamard transformation

main problem:

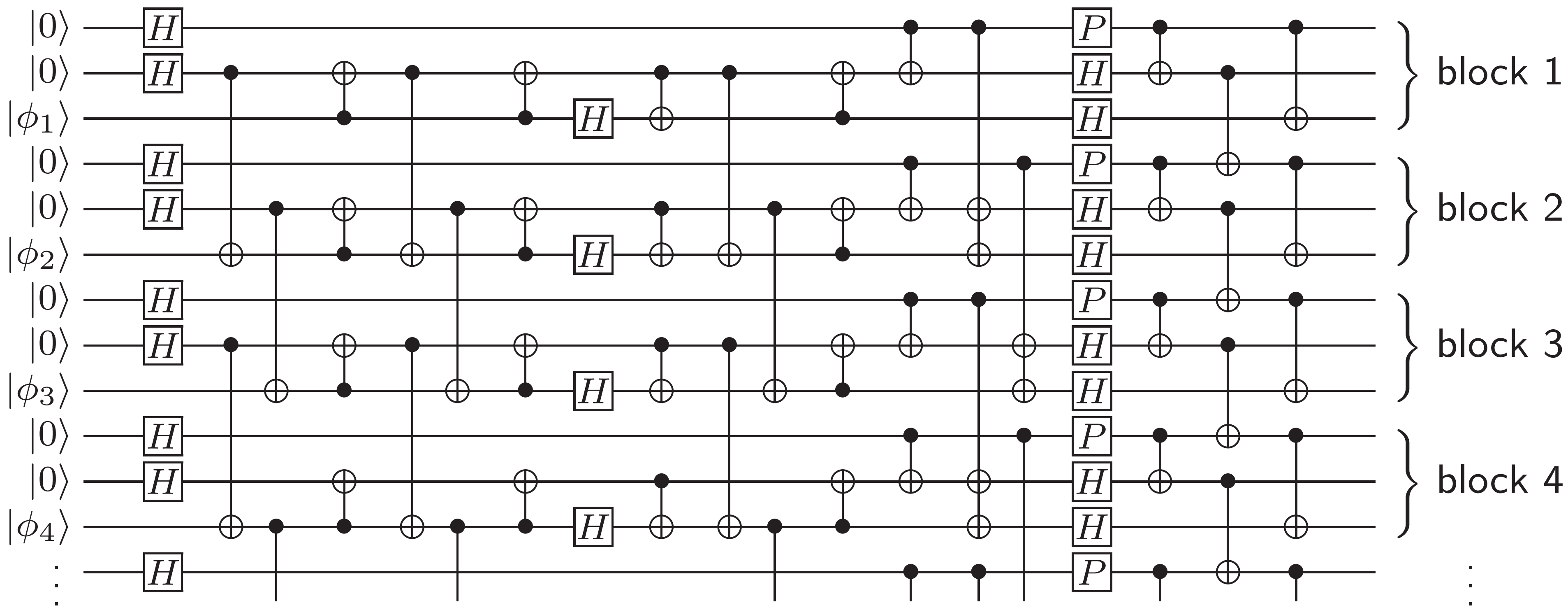
While clearing some entries, the degree of the other entries might double.

$\Longrightarrow$ exponential upper bound

possible solution:

use intermediate degree reductions (see [Lemma 6, ITW 2010] and the work by R. Kannan on Smith normal form computations)

Example: Rate $1/3$ Quantum Convolutional Code



Every gate has to be repeatedly applied shifted by one block.

谢谢

MAX PLANCK INSTITUTE
for the science of light