
International DFG Workshop 2007

Quantum Information Processing

Cochem/Ediger-Eller, 28.–30. März 2007

Quantum Convolutional Codes

Markus Grassl

joint work with

Martin Rötteler, NEC Laboratories America, Inc.

David Forney, Saikat Guha, MIT

Salah A. Aly, Andreas Klappenecker, Pradeep Kiran Sarvepalli, Texas A&M



Institut für Algorithmen und Kognitive Systeme
Fakultät für Informatik, Universität Karlsruhe (TH)
Germany

<http://iaks-www.ira.uka.de/home/grassl>

Motivation

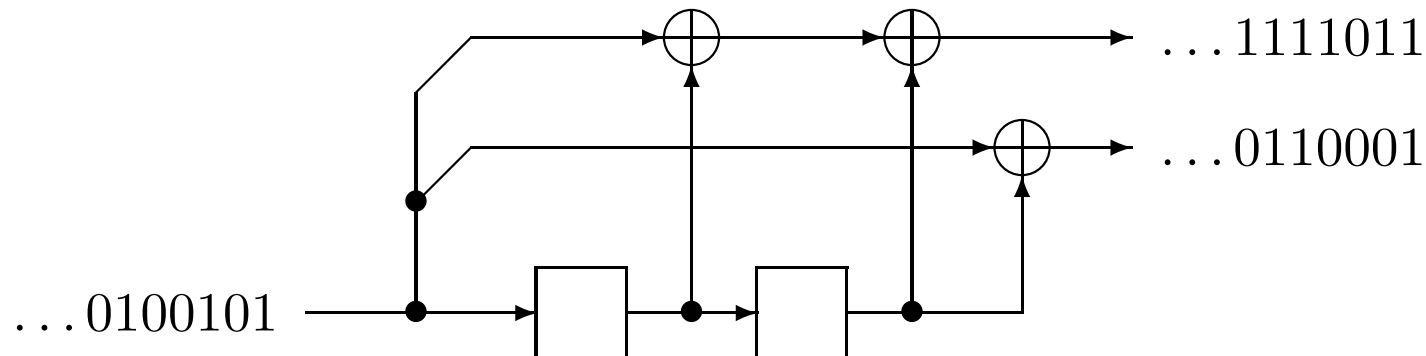
Problem: Send a stream of qubits along a channel

- Solution 1: Use the code $[[5, 1, 3]]$ for every qubit
⇒ rate $1/5$, correcting one error in every block of five qubits
- Solution 2: Use a long code to encode larger blocks/all qubits
⇒ better rate & more errors can be corrected, but
 - more complicated operations
 - large delay
- Solution 3: Quantum Convolutional Codes
 - “online” encoding/decoding
 - local encoding/inverse encoding operations
 - good classical convolutional codes are used in practice

Classical Convolutional Codes

Based on linear shift registers

Example: Code of rate 1/2, min. distance 5:



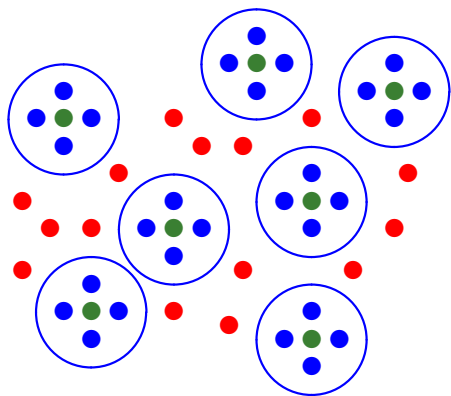
in general:

- outputs are linear functions of the input and the memory
- the new memory state is a linear function of the input and the old memory

The Basic Idea of QECC

Classical codes

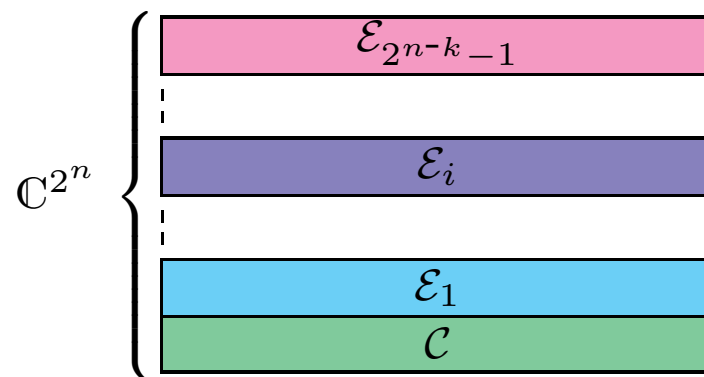
Partition of the set of all words of length n over an alphabet of size 2.



- codewords
- errors of bounded weight
- other errors

Quantum codes

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



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

$$\text{Encoding: } |\mathbf{x}\rangle \mapsto U_{\text{enc}}(|\mathbf{x}\rangle |0\rangle)$$

Discretization of Quantum Errors

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

“Pauli” matrices (real version):

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

The **weight** of E is the number of $E_i \neq I$. 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 all errors E of weight t or less, then \mathcal{C} can correct **arbitrary errors** affecting $\leq t$ qubits.

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 $\mathcal{H}_C \leq \mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2$

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

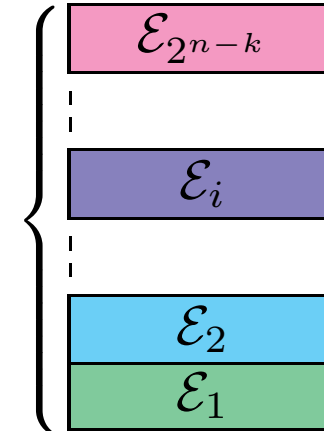
Hence we have an **orthogonal decomposition** of $\mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2$

Stabilizer Codes

Observables

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

decomposition into
common eigenspaces



the orthogonal spaces are labeled by the eigenvalues

\implies operations that change the eigenvalues can be detected

The Stabilizer of a Quantum Code

Pauli group:

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

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

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

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

A quantum code \mathcal{C} with stabilizer \mathcal{S} is called a **stabilizer code** if and only if

$$M |v\rangle = |v\rangle \text{ for all } M \in \mathcal{S} \implies |v\rangle \in \mathcal{C}.$$

\mathcal{S} is an abelian (commutative) group and \mathcal{C} is the joint +1-eigenspace of all $M \in \mathcal{S}$.

Stabilizer Codes and Classical Codes

Notation:

Denote by $X_{\mathbf{a}}$ where $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_2^n$ and $\mathbb{F}_2 = \{0, 1\}$ the operator

$$X_{\mathbf{a}} = X^{a_1} \otimes X^{a_2} \otimes \dots \otimes X^{a_n}.$$

Similar

$$Z_{\mathbf{b}} = Z^{b_1} \otimes Z^{b_2} \otimes \dots \otimes Z^{b_n}.$$

For instance $X_{110} = X \otimes X \otimes I$ and $Z_{101} = Z \otimes I \otimes Z$.

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

Stabilizer Codes and Classical Codes

Example: The repetition code is a stabilizer code with stabilizer $\mathcal{S} = \{III, ZZI, ZIZ, IZZ\} = \langle ZIZ, IZZ \rangle$.

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

in general

$$\mathcal{S} \hat{=} (\mathbf{X}|\mathbf{Z}) \in \mathbb{F}_2^{(n-k) \times 2n}$$

The matrix $(\mathbf{X}|\mathbf{Z})$ generates a symplectic self-orthogonal code with

$$\mathbf{XZ}^t - \mathbf{ZX}^t = \mathbf{0}.$$

Encoding Stabilizer Codes

Basic idea:

Use operations of the *generalized Clifford group* (or Jacobi group) to transform the stabilizer \mathcal{S} into a trivial stabilizer $\mathcal{S}_0 := \langle Z^{(1)}, \dots, Z^{(n-k)} \rangle$, corresponding to the code $|0^{n-k}\rangle |\phi\rangle$.

- row/column operations on the binary matrix $(\mathbf{X}|\mathbf{Z})$ to obtain “normal form” $(\mathbf{0}|\mathbf{I0})$
- operations on $(\mathbf{X}|\mathbf{Z})$ correspond to
 - “elementary” single-qubit gates
 - CNOT-gate

- single qubit gate $P := \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \in \mathbb{C}^{2 \times 2}$

Action on Pauli Matrices

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

in \mathbb{C}
mod 2

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

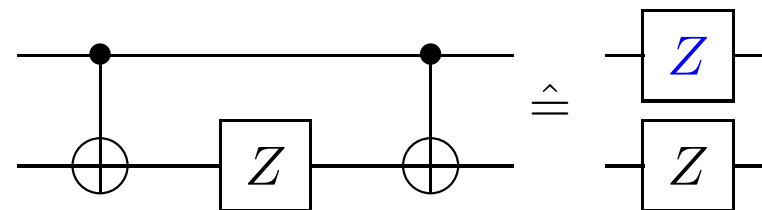
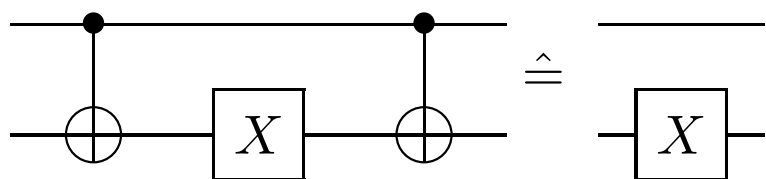
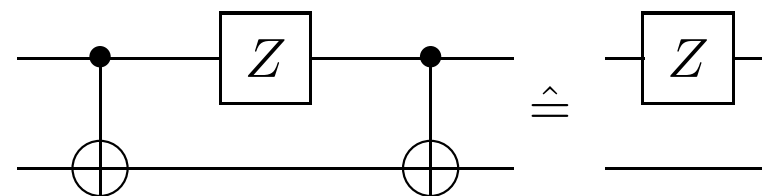
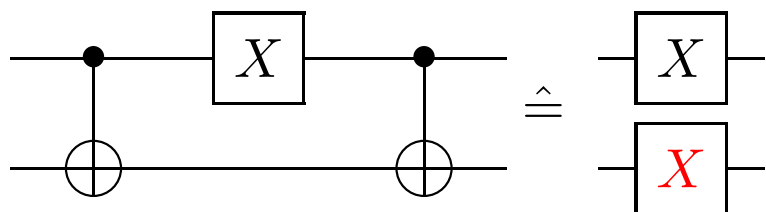
$$\overline{H} \hat{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \overline{P} \hat{=} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

local operation on $(\mathbf{X}|\mathbf{Z})$:

multiplying column i in submatrix \mathbf{X} and column i in submatrix \mathbf{Z} by \overline{M}

Action of CNOT

Modifying stabilizers



add X from source to target

add Z from target to source

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \in \mathbb{C}^{4 \times 4}$$

$$\overline{\text{CNOT}} \hat{=} \left(\begin{array}{cc|cc} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{array} \right) \in \mathbb{F}_2^{4 \times 4}$$

Example: 5 Qubit Code $[[5, 1, 3]]$

Generators of stabilizer

$$\left[\begin{array}{l} XXZIZ \\ ZXXZI \\ IZXXZ \\ ZIZXX \end{array} \right] \hat{=} \left(\begin{array}{ccccc|ccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{array} \right)$$

Step I: X -Only Generator

Local operations $\hat{=}$ operations on corresponding \mathbf{X} and \mathbf{Z} columns

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

$$T_1 := I \otimes I \otimes I \otimes I \otimes I$$

Step I: X -Only Generator

Local operations $\hat{=}$ operations on corresponding \mathbf{X} and \mathbf{Z} columns

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

$$T_1 := I \otimes I \otimes H \otimes I \otimes I$$

Step I: X -Only Generator

Local operations $\hat{=}$ operations on corresponding \mathbf{X} and \mathbf{Z} columns

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

$$T_1 := I \otimes I \otimes H \otimes I \otimes H$$

Step II: X -Generator of Weight One

CNOT $\hat{=}$ operations on pairs of corresponding X and Z columns

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

$$T_1 := I \otimes I \otimes H \otimes I \otimes H$$

$$T_2 := I$$

Step II: X -Generator of Weight One

CNOT $\hat{=}$ operations on pairs of corresponding X and Z columns

$$\left(\begin{array}{ccccc|ccccc} \color{red}{1} & 1 & 1 & 0 & 1 & 0 & \color{blue}{0} & 0 & 0 & 0 \\ \color{red}{0} & 1 & 0 & 0 & 0 & 1 & \color{blue}{0} & 1 & 1 & 0 \\ \color{red}{0} & 0 & 0 & 1 & 1 & 0 & \color{blue}{1} & 1 & 0 & 0 \\ \color{red}{0} & 0 & 1 & 1 & 0 & 1 & \color{blue}{0} & 0 & 0 & 1 \end{array} \right)$$

$$T_1 := I \otimes I \otimes H \otimes I \otimes H$$

$$T_2 := I$$

Step II: X -Generator of Weight One

CNOT $\hat{=}$ operations on pairs of corresponding X and Z columns

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

$$T_1 := I \otimes I \otimes H \otimes I \otimes H$$

$$T_2 := \text{CNOT}^{(1,2)}$$

Step II: X -Generator of Weight One

CNOT $\hat{=}$ operations on pairs of corresponding X and Z columns

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

$$T_1 := I \otimes I \otimes H \otimes I \otimes H$$

$$T_2 := \text{CNOT}^{(1,2)}$$

Step III: Row Operations

multiplying generators $\hat{=}$ adding/permuting rows

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

$$T_1 := I \otimes I \otimes H \otimes I \otimes H$$

$$T_2 := \text{CNOT}^{(1,2)} \text{CNOT}^{(1,3)} \text{CNOT}^{(1,5)}$$

Pre-Final Result: Only X -Generators

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

Final Result: Only Z -Generators

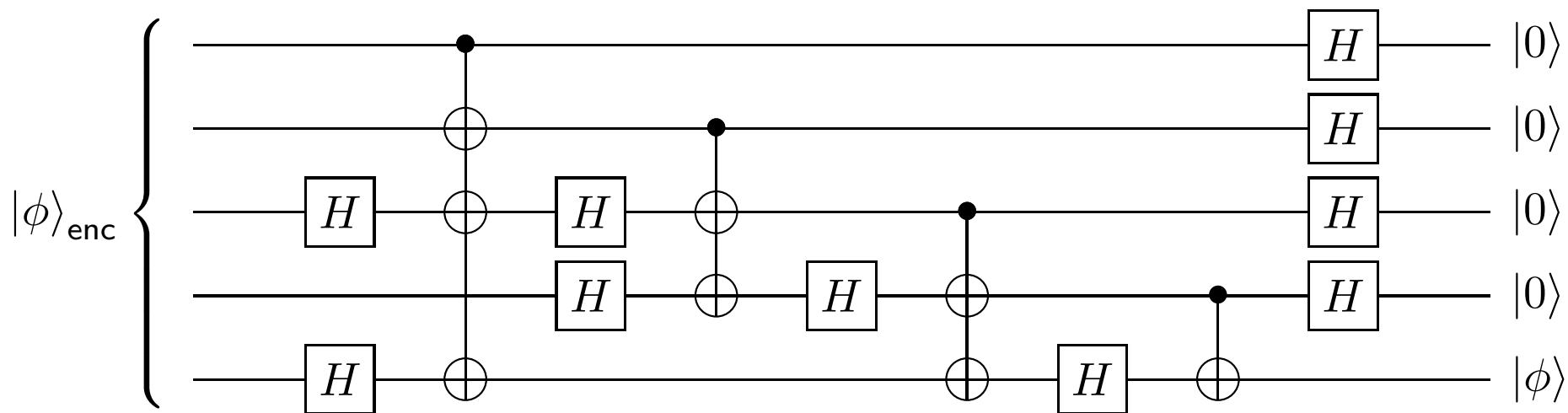
$$\left(\begin{array}{ccccc|ccccc} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array} \right)$$

$$T_{\text{final}} := H \otimes H \otimes H \otimes H \otimes I$$

combining all transformations:

quantum circuit that maps the encoded state $|\phi\rangle_{\text{enc}}$
to the un-encoded state $|0000\rangle |\phi\rangle$

Inverse Encoding Circuit



Quantum circuit mapping a state $|\phi\rangle_{\text{enc}}$ of the code $[[5, 1, 3]]$ to an unencoded one-qubit state $|\phi\rangle$.

Quantum Convolutional Codes

Quantum Block Codes

The code is the common eigenspace of the stabilizers.

Quantum Convolutional Codes

Idea: impose local constraints by stabilizers

Example:

$$s_1 = \dots III XXX XZY III III \dots$$

$$s_2 = \dots III ZZZ ZYX III III \dots$$

shift the stabilizers by three qubits:

$$s'_1 = \dots III III XXX XZY III \dots$$

$$s'_2 = \dots III III ZZZ ZYX III \dots$$

Semi-infinite Stabilizer

Compact representation of the semi-infinite stabilizer matrix

$$\begin{aligned}
 & \left(\begin{array}{cc} XXX & XZY \\ ZZZ & ZYX \\ & XXX & XZY \\ & ZZZ & ZYX \\ & & \ddots \end{array} \right) \\
 & \hat{=} \left(\begin{array}{ccc|cc} 111 & 101 & & 000 & 011 \\ 000 & 011 & & 111 & 110 \\ & 111 & 101 & & 000 & 011 \\ & 000 & 011 & & 111 & 110 \\ & & & & & \ddots \end{array} \right) \\
 & \hat{=} \left(\begin{array}{ccc|ccc} 1 + D & 1 & 1 + D & 0 & D & D \\ 0 & D & D & 1 + D & 1 + D & 1 \end{array} \right) = \mathbf{S}(D)
 \end{aligned}$$

Quantum Convolutional Codes

Quantum Block Codes

The stabilizer 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 $(\mathbf{X}(D) | \mathbf{Z}(D))$ 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:

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

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

\implies local errors spread unboundedly

\implies further constraints on $\mathbf{S}(D)$ (must have polynomial inverse)

Quantum Convolutional Codes: Error Correction

Basic Ideas:

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

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

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in \mathbb{C}^{2 \times 2}$$

$$\overline{H} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathbb{F}_2^{2 \times 2}$$

$$P = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi/2) \end{pmatrix} \in \mathbb{C}^{2 \times 2}$$

$$\overline{P} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathbb{F}_2^{2 \times 2}$$

$$\text{CNOT}^{(i, j+\ell n)}, i \not\equiv j \pmod{n} \quad \overline{\text{CNOT}} = \left(\begin{array}{cc|cc} 1 & D^\ell & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & D^{-\ell} & 1 \end{array} \right)$$

$$P_\ell := \text{CSIGN}^{(i, i+\ell n)}, \ell \neq 0$$

$$\overline{P}_\ell = \begin{pmatrix} 1 & D^{-\ell} + D^\ell \\ 0 & 1 \end{pmatrix}$$

Quantum Circuits

Single qubit gates

operation on stabilizer matrix in D -transform notation

\implies expand to semi-infinite matrix

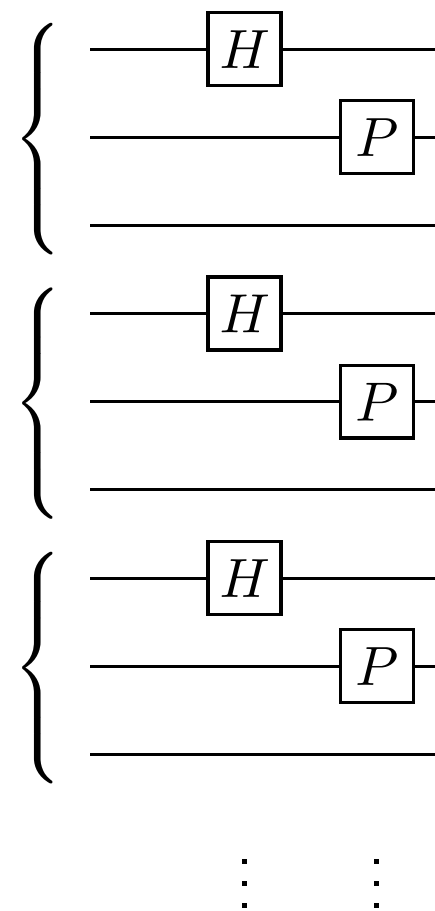
\implies repeat the operations infinitely often

Example:

blocks of three qubits each

operation H on first position

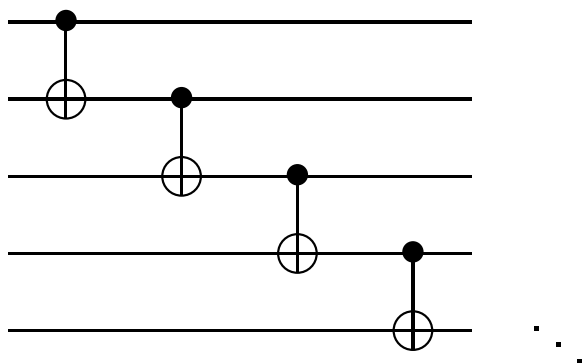
operation P on second position



Quantum Circuits

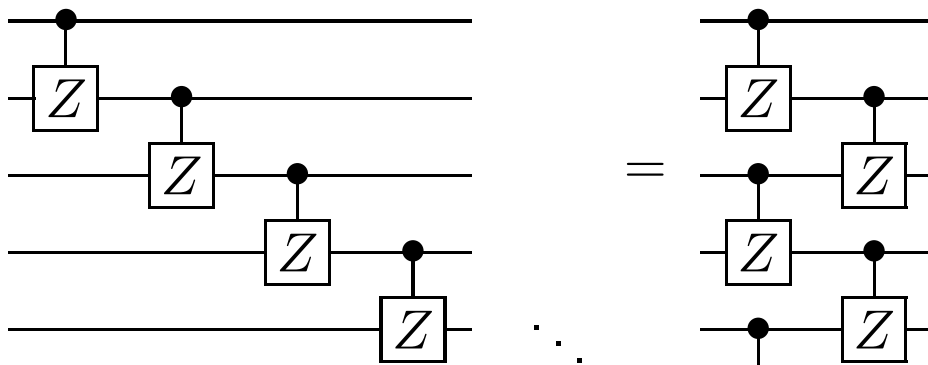
Two-qubit gates

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



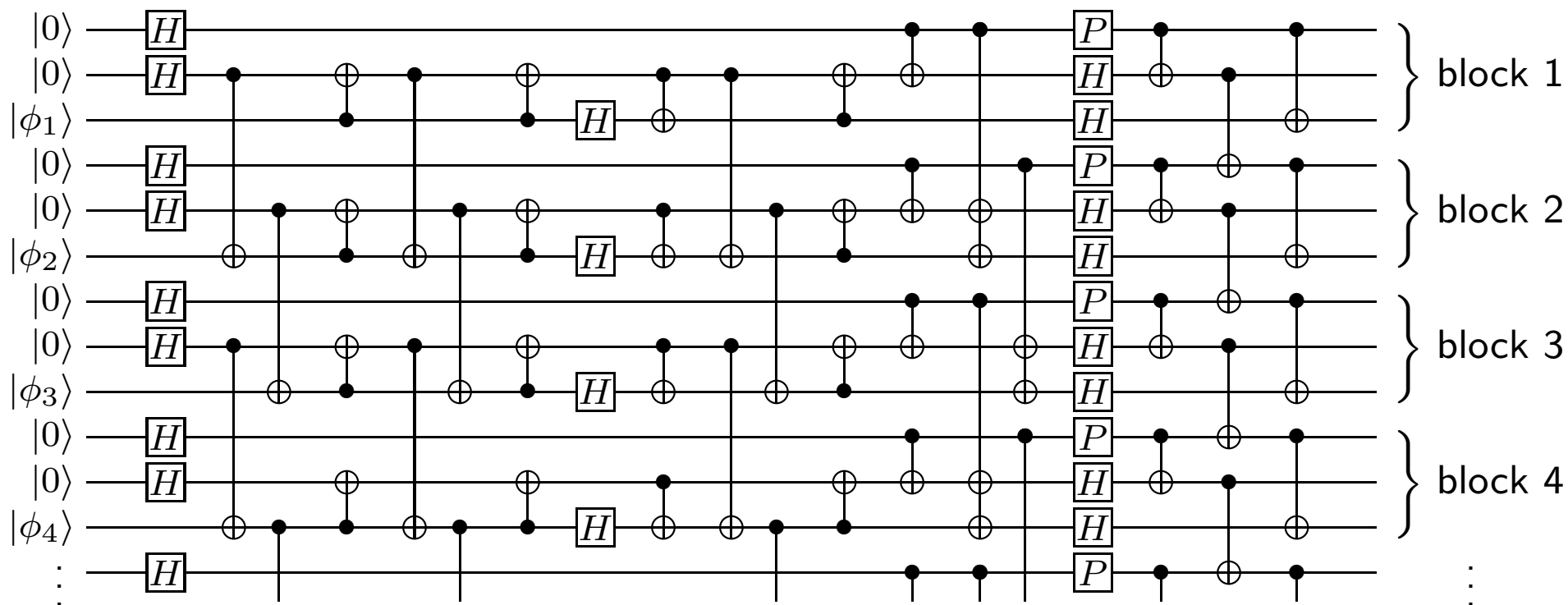
\implies infinite depth

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



\implies finite depth

Example: Rate 1/3 Quantum Convolutional Code



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

Summary

- Quantum stabilizer codes are common eigenspaces of the stabilizer
- The stabilizer corresponds to a classical code
- Use both block and convolutional codes to define stabilizer codes
- Encoding circuits from transformations on the binary matrix
- Quantum circuits with finite depth for convolutional quantum codes with non-catastrophic generator matrix
- Two-qubit gates span a bounded number of blocks.
- Generators of stabilizer act non-trivially on a bounded number of qubits.

References

- M. Grassl, M. Rötteler, and Th. Beth, “Efficient Quantum Circuits for Non-Qubit Quantum Error-Correcting Codes”, *International Journal of Foundations of Computer Science*, 14(5):757–775, 2003, [quant-ph/0211014](#).
- H. Ollivier and J.-P. Tillich, “Quantum convolutional codes: fundamentals,” 2004, [quant-ph/0401134](#).
- G. D. Forney, Jr., M. Grassl, and S. Guha, “Convolutional and tail-biting quantum error-correcting codes,” *IEEE Trans. Inform. Theory*, vol. 53, no. 3, pp. 865–880, 2007, [quant-ph/0511016](#).
- M. Grassl and M. Rötteler, “Non-catastrophic encoders and encoder inverses for quantum convolutional codes,” in *Proc. 2006 IEEE Intl. Symp. Inform. Theory*, Seattle, USA, 2006, pp. 1109–1113, [quant-ph/0602129](#).
- S. A. Aly, M. Grassl, A. Klappenecker, M. Rötteler, P. K. Sarvepalli, “Quantum Convolutional BCH Codes,” *2007 Canadian Information Theory Workshop*, [quant-ph/0703113](#).