



Workshop on Convolutional Codes

Universität Zürich, June 5-9, 2023

Quantum Convolutional Codes

Markus Grassl

International Centre for Theory of Quantum Technologies
University of Gdansk

markus.grassl@ug.edu.pl

www.markus-grassl.de

7 June 2023



Overview

- qubits and qudits
- quantum codes
- operational view on quantum convolutional codes
- stabilizer formalism
- basic operations
- encoding circuit
- open problems

Quantum Information

Quantum-bit (qubit)

basis states:

$$\text{"0"} \hat{=} |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{C}^2, \quad \text{"1"} \hat{=} |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{C}^2$$

general state:

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{where } \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

measurement (read-out):

result "0" with probability $|\alpha|^2$

result "1" with probability $|\beta|^2$

Quantum Information

Quantum register

basis states:

$$|b_1\rangle \otimes \dots \otimes |b_n\rangle =: |b_1 \dots b_n\rangle = |\mathbf{b}\rangle \quad \text{where } b_i \in \{0, 1\}$$

general state:

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

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

Qudits

generalization to $(\mathbb{C}^q)^{\otimes n}$: basis states $|\mathbf{b}\rangle$ labelled by vectors $\mathbf{b} \in \mathbb{F}_q^n$

Quantum Error-Correcting Block Codes

- **subspace** \mathcal{C} of a complex vector space $\mathcal{H} \cong \mathbb{C}^N$
usually: $\mathcal{H} \cong \mathbb{C}^q \otimes \mathbb{C}^q \otimes \dots \otimes \mathbb{C}^q =: (\mathbb{C}^q)^{\otimes n}$ “ n qudits”
- **errors:** described by linear transformations acting on
 - some of the subsystems (local errors)
 - many subsystems in the same way (correlated errors)
- **notation:** $\mathcal{C} = \llbracket n, k, d \rrbracket_q$
 q^k -dimensional subspace \mathcal{C} of $(\mathbb{C}^q)^{\otimes n}$
- **minimum distance** d :
 - detection of errors acting on $d - 1$ subsystems
 - correction of errors acting on $\lfloor (d - 1)/2 \rfloor$ subsystems
 - correction of erasures acting on $d - 1$ known subsystems

Quantum Error-Correcting Codes

quantum error-correction is “linear”

If the errors A and B can be corrected,
then all errors $\lambda A + \mu B$ ($\lambda, \mu \in \mathbb{C}$) can be corrected.

\implies consider only a vector space basis of the errors

Error Basis for Qudits

[A. Ashikhmin & E. Knill, Nonbinary quantum stabilizer codes, IEEE-IT **47**, pp. 3065–3072 (2001)]

$$\mathcal{E} = \{X^\alpha Z^\beta : \alpha, \beta \in \mathbb{F}_q\},$$

where (you may think of $\mathbb{C}^q \cong \mathbb{C}[\mathbb{F}_q]$)

$$X^\alpha := \sum_{x \in \mathbb{F}_q} |x + \alpha\rangle\langle x| \quad \text{for } \alpha \in \mathbb{F}_q$$

and

$$Z^\beta := \sum_{z \in \mathbb{F}_q} \omega^{\text{Tr}(\beta z)} |z\rangle\langle z| \quad \text{for } \beta \in \mathbb{F}_q \quad (\omega := \omega_p = \exp(2\pi i/p))$$

Encoding Stabilizer Block 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 stabilizer matrix $(\mathbf{X}|\mathbf{Z})$ to obtain “normal form” $(\mathbf{0}|\mathbf{I}\mathbf{0})$
- 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)

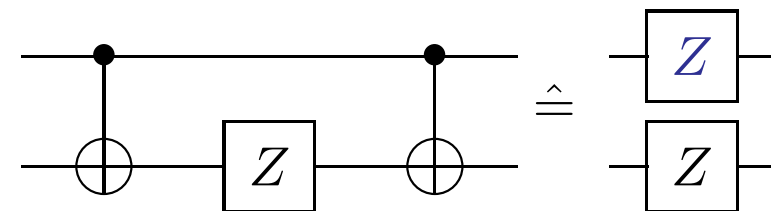
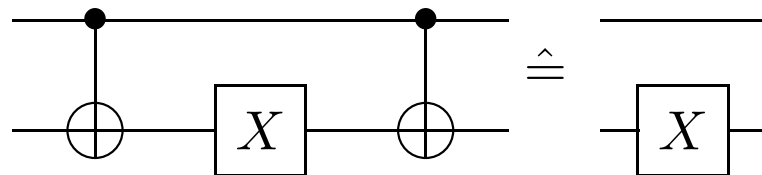
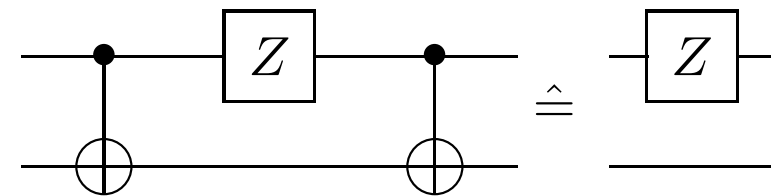
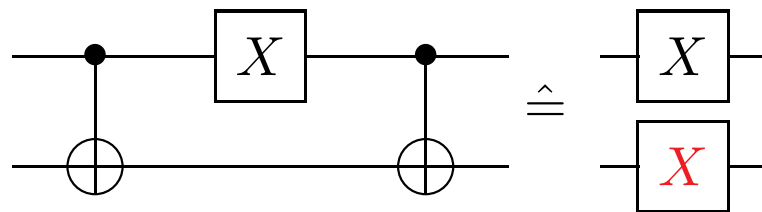
$$\overline{H} \hat{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \overline{P} \hat{=} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

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

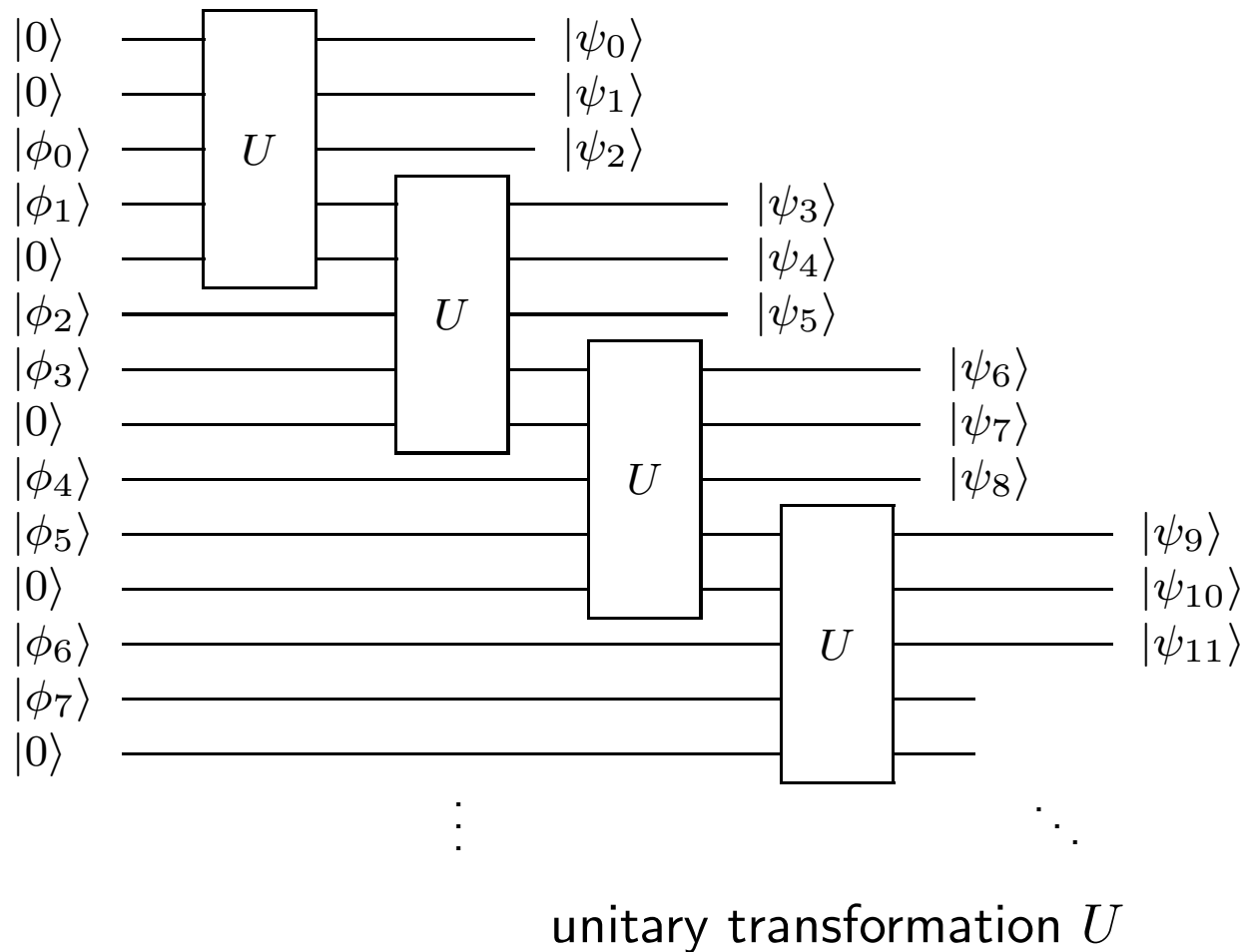
add Z from target to source

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

$$\overline{\text{CNOT}} \hat{=} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{4 \times 4}$$

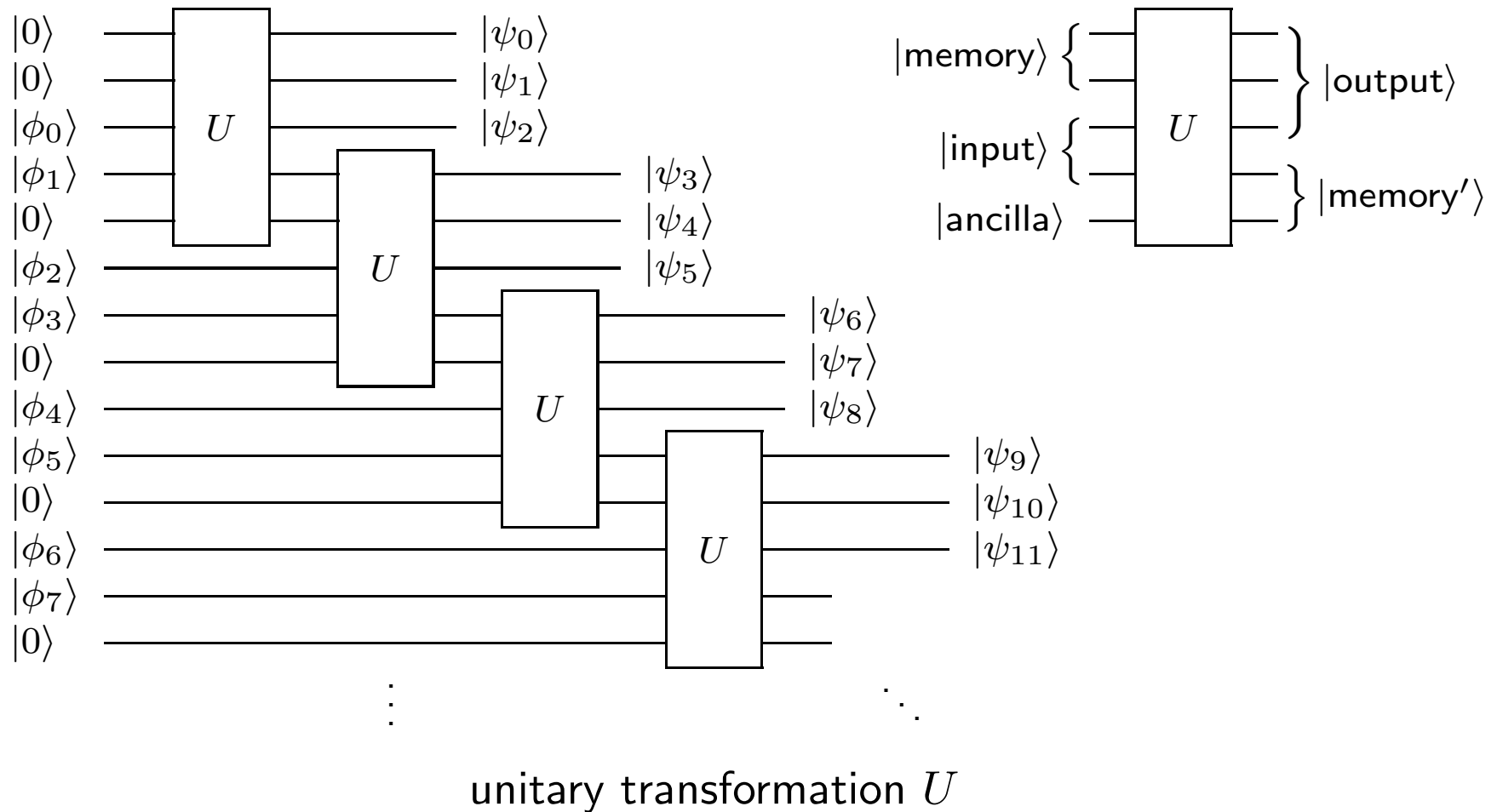
Convolutional Quantum Encoder

encoding a stream of qudits



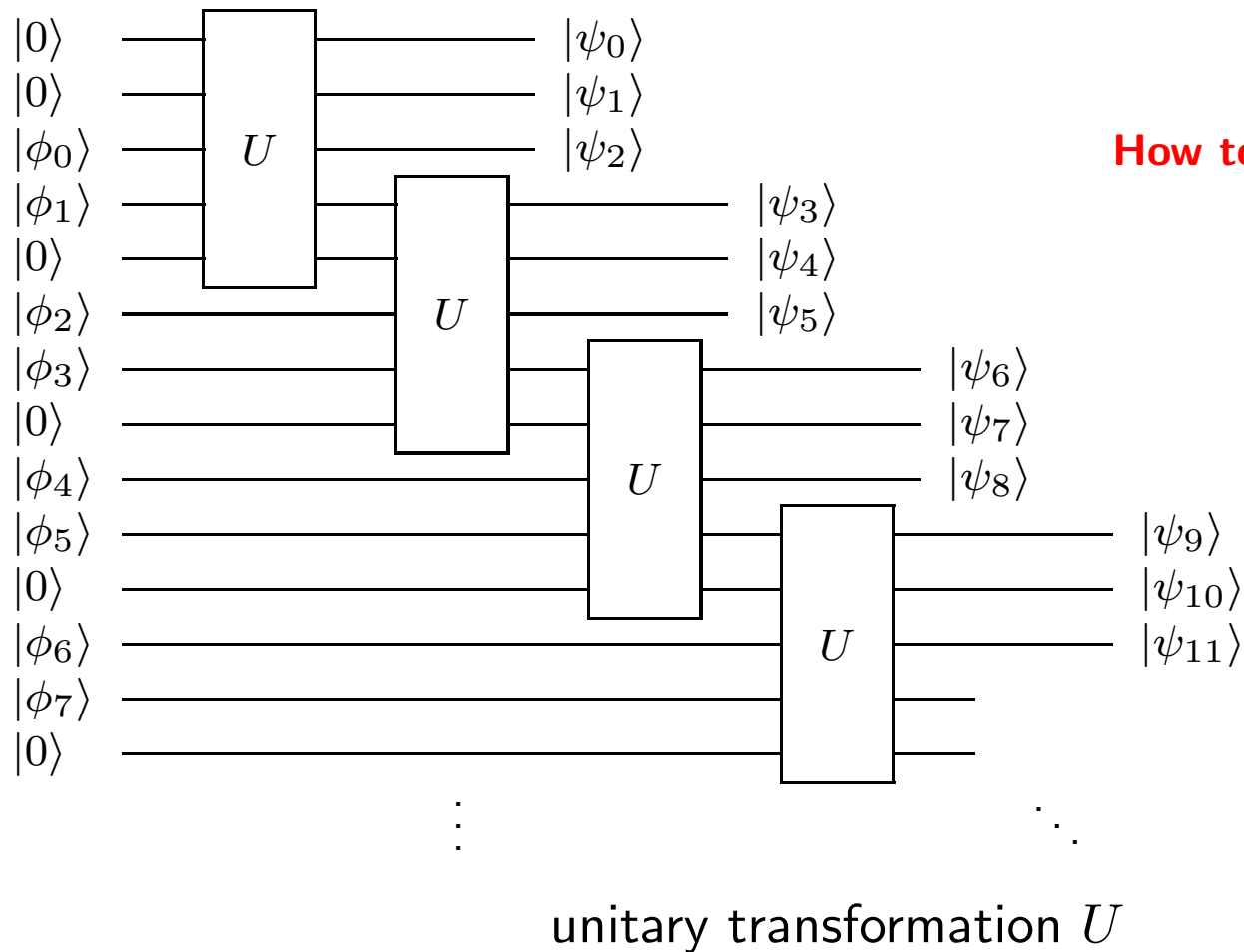
Convolutional Quantum Encoder

encoding a stream of qudits



Convolutional Quantum Encoder

encoding a stream of qudits



Quantum Convolutional Stabilizer Codes

Quantum Block (Stabilizer) 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:

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

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

Quantum Convolutional Codes (QCCs)

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

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

- semi-infinite stabilizer with block band structure

$$S := \left(\begin{array}{c} \overbrace{\hspace{2cm}}^n \quad \overbrace{\hspace{2cm}}^m \\ \boxed{M} \quad \left. \vphantom{\boxed{M}} \right\} n - k \\ \quad \boxed{M} \\ \quad \quad \boxed{M} \\ \quad \quad \quad \vdots \end{array} \right)$$

- 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

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

Quantum Convolutional Codes

Quantum Block Codes

The stabilizer \mathcal{S} corresponds to a self-orthogonal additive code over $\mathbb{F}_2 \times \mathbb{F}_2$ generated by the stabilizer matrix $(\mathbf{X}|\mathbf{Z})$.

Quantum Convolutional Codes

The semi-infinite stabilizer corresponds to an additive self-orthogonal convolutional code generated by $(\mathbf{X}(D) | \mathbf{Z}(D))$ 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 $\mathbf{S}(D)$

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.
⇒ syndrome of the corresponding classical convolutional code
- Use your favorite algorithm to decode the classical convolutional code (e. g. Viterbi algorithm).
- Only the cosets of the code in its dual matter (degeneracy).

Elementary 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

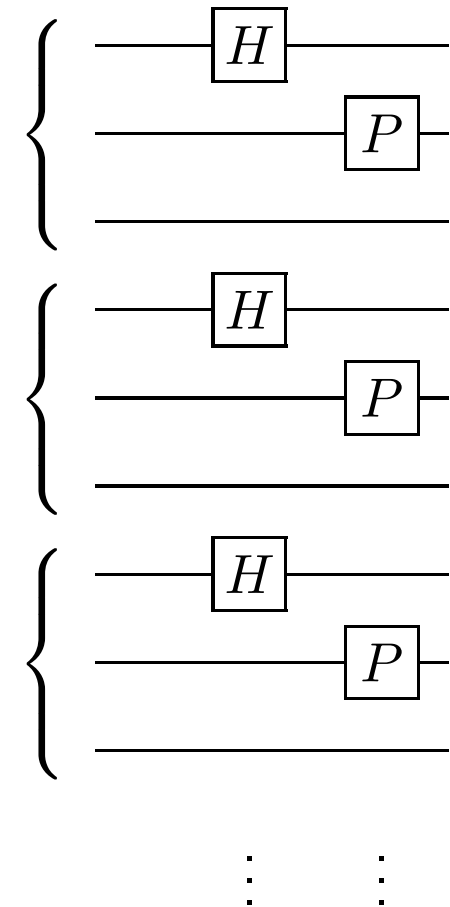
\implies repeat the operations infinitely often

Example:

blocks of three qubits each

operation H on first position

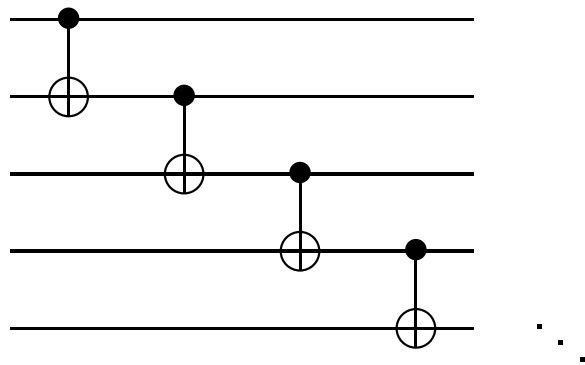
operation P on second position



Quantum Circuits

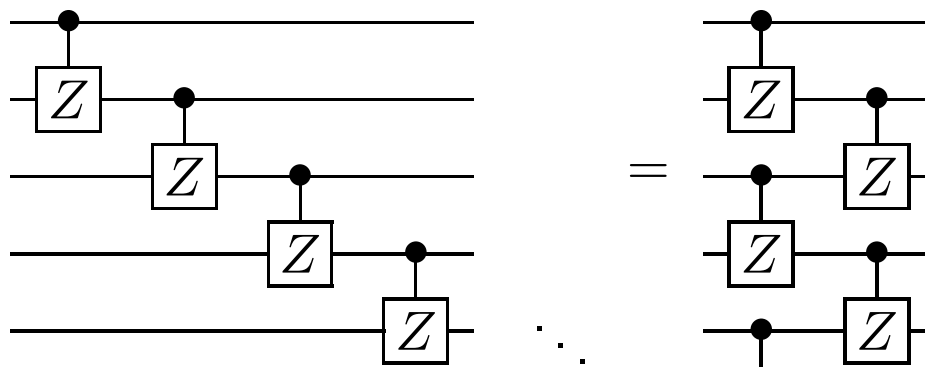
Two-qubit gates

- 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

Computing an Inverse Encoding Circuit

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

Using the previous elementary operations on columns and (free) row operations $A(D)$, we can compute the Smith normal form of $\mathbf{S}(D) = (\mathbf{X}(D)|\mathbf{Z}(D))$:

$$A(D)(\mathbf{X}(D)|\mathbf{Z}(D))T(D) = (0|I0)$$

- if $\mathbf{S}(D)$ has non-trivial elementary divisors, replace them by 1
- the stabilizer matrix $(0|I0)$ corresponds to a trivial code with no encoding
- the factorisation of $T(D)$ into elementary operations yields an inverse encoding circuit

open problem:

How many elementary operations are needed to implement $T(D)$?

So far, only exponential upper bound known (but see [Kannan 1985]).

Computing an Encoder

basic idea:

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

$$\left(\begin{array}{|c} \\ \\ \end{array} \right)$$

application of [\[Theorem 7, ITW 2010\]](#)

$$(f_1(D) \ f_2(D) \mid g_1(D) \ g_2(D)) \rightarrow (f'_1(D) \ 0 \mid g'_1(D) \ 0)$$

Computing an Encoder

basic idea:

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

$$\left(\begin{array}{c|c} \boxed{} & \boxed{} \end{array} \right)$$

application of [\[Theorem 7, ITW 2010\]](#)

$$(f_1(D) \ f_2(D) \mid g_1(D) \ g_2(D)) \rightarrow (f'_1(D) \ 0 \mid g'_1(D) \ 0)$$

Computing an Encoder

basic idea:

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

$$\left(\begin{array}{c|c} \text{[Diagram of a staircase-like matrix]} & \text{[Diagram of a staircase-like matrix]} \end{array} \right)$$

application of [\[Theorem 7, ITW 2010\]](#)

$$(f_1(D) \ f_2(D) \mid g_1(D) \ g_2(D)) \rightarrow (f'_1(D) \ 0 \mid g'_1(D) \ 0)$$

Computing an Encoder

basic idea:

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

$$\left(\begin{array}{c|c} \text{Step-like matrix} & \text{Step-like matrix} \end{array} \right)$$

application of [\[Theorem 7, ITW 2010\]](#)

$$(f_1(D) f_2(D) | g_1(D) g_2(D)) \rightarrow (f'_1(D) 0 | g'_1(D) 0)$$

Computing an Encoder

basic idea:

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

$$\left(\begin{array}{c|c} \text{[Diagram of } X(D) \text{]} & \text{[Diagram of } Z(D) \text{]} \end{array} \right)$$

The diagram shows two square matrices side-by-side, separated by a vertical line. Each matrix has a staircase pattern of steps on the left side, representing the polynomial matrices X(D) and Z(D) in a stabilizer matrix.

application of [\[Theorem 7, ITW 2010\]](#)

$$(f_1(D) \ f_2(D) \mid g_1(D) \ g_2(D)) \rightarrow (f'_1(D) \ 0 \mid g'_1(D) \ 0)$$

Computing an Encoder

basic idea:

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

$$\left(\begin{array}{c|c} \begin{array}{cccc} \square & & & \\ \square & \square & & \\ \square & \square & \square & \\ \square & \square & \square & \square \\ \square & \square & \square & \square \end{array} & \begin{array}{ccc} \square & & \\ \square & \square & \\ \square & \square & \square \end{array} \end{array} \right)$$

application of [Theorem 4, ITW 2010]

$$(f(D) | g(D)) \rightarrow (h(D) | 0)$$

if $(f(D) | g(D))$ commute

Computing an Encoder

basic idea:

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

$$\left(\begin{array}{c|c} \begin{array}{cccc} \square & & & \\ \square & \square & & \\ \square & \square & \square & \\ \square & \square & \square & \square \\ \square & \square & \square & \square \end{array} & \begin{array}{cc} & \\ \square & \\ \square & \square \end{array} \end{array} \right)$$

application of [Theorem 4, ITW 2010]

$$(f(D) | g(D)) \rightarrow (h(D) | 0)$$

if $(f(D) | g(D))$ commute

Computing an Encoder

basic idea:

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

$$\left(\begin{array}{c|c} \begin{array}{cccc} \square & & & \\ \square & \square & & \\ \square & \square & \square & \\ \square & \square & \square & \square \\ \square & \square & \square & \square \end{array} & \begin{array}{c} \\ \\ \\ \\ \end{array} \end{array} \right)$$

main problem:

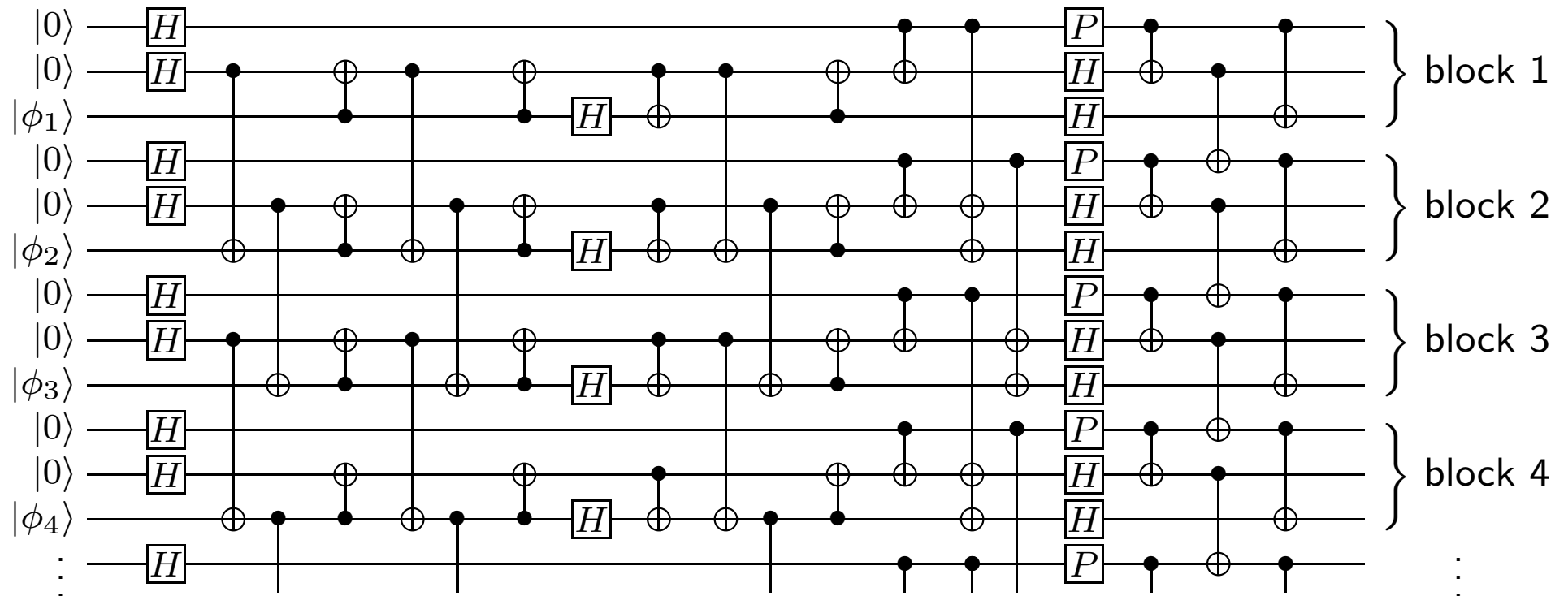
While clearing some entries, the degree of the other entries might double.

\implies exponential upper bound

possible solution:

use intermediate degree reductions

Example: Rate 1/3 Quantum Convolutional Code



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

Outlook

- “pearl-necklace” encoder with finite depth for quantum convolutional codes
- How much memory is required?
(see work by [Houshmand, Hosseini-Khayat & Wilde])
- Is there a pearl-necklace encoder with polynomial depth?
- When does a convolutional encoder with matrix U have an inverse with a similar convolutional structure?
- find optimal encoders
- develop bounds on the parameters
- develop “practical” decoding algorithms with good performance

Thank you!
Danke! Merci!
Dziękuję!

Acknowledgment

The 'International Centre for Theory of Quantum Technologies' project (contract no. 2018/MAB/5) is carried out within the International Research Agendas Programme of the Foundation for Polish Science co-financed by the European Union from the funds of the Smart Growth Operational Programme, axis IV: Increasing the research potential (Measure 4.3).



Republic
of Poland



Foundation for
Polish Science

European Union
European Regional
Development Fund



SNF grant 200021_188430

References

- G. D. Forney, Jr., M. Grassl, and S. Guha. Convolutional and tail-biting quantum error-correcting codes. *IEEE Transactions on Information Theory*, 53(3):865–880, March 2007. <https://doi.org/10.1109/TIT.2006.890698>
- M. Grassl and M. Rötteler. Non-catastrophic Encoders and Encoder Inverses for Quantum Convolutional Codes. *Proceedings 2006 IEEE International Symposium on Information Theory (ISIT 2006)*, Seattle, USA, July 2006, pp. 1109-1113. <https://doi.org/10.1109/ISIT.2006.261956>
- M. Grassl and M. Rötteler. On encoders for quantum convolutional codes. *Proceedings 2010 IEEE Information Theory Workshop (ITW 2010)*, Dublin, Ireland, September 2010. <https://doi.org/10.1109/CIG.2010.5592857>
- M. Houshmand, S. Hosseini-Khayat and M. M. Wilde. Minimal-Memory Requirements for Pearl-Necklace Encoders of Quantum Convolutional Codes. *IEEE Transactions on Computers*, 61(3):299–312, 2012. <https://doi.org/10.1109/TC.2010.226>
- M. Houshmand, S. Hosseini-Khayat and M. M. Wilde. Minimal-Memory, Noncatastrophic, Polynomial-Depth Quantum Convolutional Encoders. *IEEE Transactions on Information Theory* 59(2):1198–1210, 2013. <https://doi.org/10.1109/TIT.2012.2220520>

- **R. Kannan**. Solving systems of linear equations over polynomials. *Theoretical Computer Science*, 39:69–88, 1985. [https://doi.org/10.1016/0304-3975\(85\)90131-8](https://doi.org/10.1016/0304-3975(85)90131-8)
- **H. Ollivier and J.-P. Tillich**. Quantum convolutional codes: fundamentals. Preprint arXiv:quant-ph/0401134, 2004. <https://arxiv.org/abs/quant-ph/0401134>
- **E. Pelchat and D. Poulin**. Degenerate Viterbi decoding. Preprint arXiv:1204.2439 [quant-ph], 2012. <https://arxiv.org/abs/1204.2439>