Quantum Convolutional Codes

Markus Grassl
International Centre for Theory of Quantum Technologies
University of Gdansk

markus.grassl@ug.edu.pl
www.markus-grassl.de

11 July 2022
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:

\[ "0" \doteq |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{C}^2, \quad "1" \doteq |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{C}^2 \]

general state:

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

measurement (read-out):

result "0" with probability \(|\alpha|^2\)
result "1" with probability \(|\beta|^2\)
Quantum register

basis states:

\[ |b_1\rangle \otimes \ldots \otimes |b_n\rangle =: |b_1 \ldots b_n\rangle = |b\rangle \quad \text{where } b_i \in \{0, 1\} \]

general state:

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

\[ \rightarrow \text{normalized vector in } (\mathbb{C}^2)^\otimes n \cong \mathbb{C}^{2^n} \]

Qudits

generalization to \((\mathbb{C}^q)^\otimes n\): basis states \(|b\rangle\) labelled by vectors \(b \in \mathbb{F}_q^n\)
Quantum Error-Correcting Block Codes

- **subspace** $\mathcal{C}$ of a complex vector space $\mathcal{H} \cong \mathbb{C}^N$
  
  usually: $\mathcal{H} \cong \mathbb{C}^q \otimes \mathbb{C}^q \otimes \ldots \otimes \mathbb{C}^q =: (\mathbb{C}^q)^\otimes n$  
  
  "$n$ qudits"

- **errors**: described by linear transformations acting on
  - some of the subsystems (local errors)
  - many subsystems in the same way (correlated errors)

- **notation**: $C = [n, k, d]_q$

  $q^k$-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-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

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

encoding a stream of qudits

unitary transformation $U$
Convolutional Quantum Encoder

encoding a stream of qudits

How to invert this circuit?

unitary transformation $U$
Quantum Convolutional Codes

Quantum Block (Stabilizer) Codes
The code is the common eigenspace of the stabilizers.

Quantum Convolutional Codes
Idea: impose local constraints by stabilizers

Example:

\[ s_1 = \ldots \text{III XXX XZY III III} \ldots \]
\[ s_2 = \ldots \text{III ZZZ ZYX III III} \ldots \]

shift the stabilizers by three qubits:

\[ s'_1 = \ldots \text{III III XXX XZY III} \ldots \]
\[ s'_2 = \ldots \text{III III ZZZ ZYX III} \ldots \]
Quantum Convolutional Codes (QCCs)


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

- semi-infinite stabilizer with block band structure

\[
S := \begin{pmatrix}
\begin{array}{c}
M \\
\ldots
\end{array}
\end{pmatrix}^{n-k}
\]

- \(S\) 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

\[
\begin{pmatrix}
XXX & XZY \\
ZZZ & ZYX \\
XXX & XZY \\
ZZZ & ZYX \\
\vdots
\end{pmatrix}
\]

\[
\overset{\hat{\ }}{=} \begin{pmatrix}
111 & 101 & 000 & 011 \\
000 & 011 & 111 & 110 \\
111 & 101 & 000 & 011 \\
000 & 011 & 111 & 110 \\
\vdots & \vdots & \vdots & \vdots \\
\end{pmatrix}
\]

\[
\overset{\hat{\ }}{=} \begin{pmatrix}
1 + D & 1 & 1 + D & 0 & D & D \\
0 & D & D & 1 + D & 1 + D & 1 \\
\end{pmatrix}
\]

\[= S(D)\]
Quantum Convolutional Codes

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

Quantum Convolutional Codes
The semi-infinite stabilizer corresponds to an additive self-orthogonal convolutional
code generated by $(X(D) \mid Z(D))$ with

$$X(D)Z(1/D)^t - Z(D)X(1/D)^t = 0$$

Example:

$$S(D) = \begin{pmatrix} 1 + D & 1 & 1 + D \\ 0 & D & D \end{pmatrix} \begin{pmatrix} 0 & D & D \\ 1 + D & 1 + D & 1 \end{pmatrix}$$
Catastrophic (Quantum) Convolutional Codes

Bad example:

\[
\begin{pmatrix}
Z & Z \\
Z & Z \\
Z & Z \\
\vdots
\end{pmatrix}
\hat{=} \begin{pmatrix} 0 \\ 1 + D \end{pmatrix} = S(D)
\]

Quantum code with basis states \(|0\rangle = |000\ldots\rangle\) and \(|1\rangle = |111\ldots\rangle\), contains in particular “infinite cat state”

\[\Rightarrow\text{ local errors spread unboundedly}\]

\[\Rightarrow\text{ further constraints on } S(D)\]
**Elementary Operations on** \( S(D) = (X(D)|Z(D)) \)

\[
H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in \mathbb{C}^{2 \times 2} \\
\overline{H} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathbb{F}_2^{2 \times 2}
\]

\[
P = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi/2) \end{pmatrix} \in \mathbb{C}^{2 \times 2} \\
\overline{P} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathbb{F}_2^{2 \times 2}
\]

\[
\text{CNOT}^{(i,j+\ell n)}, i \not\equiv j \pmod{n} \\
\overline{\text{CNOT}} = \begin{pmatrix}
1 & D^\ell & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & D^{-\ell} & 1
\end{pmatrix}
\]

\[
P_\ell := \text{CSIGN}^{(i,i+\ell n)}, \ell \neq 0 \\
\overline{P_\ell} = \begin{pmatrix}
1 & D^{-\ell} + D^\ell \\
0 & 1
\end{pmatrix}
\]
Computing an Inverse Encoding Circuit


Using the previous elementary operations on columns and (free) row operations $A(D)$, we can compute the Smith normal form of $S(D) = (X(D) | Z(D))$: $A(D)(X(D) | Z(D))T(D) = (0 | I_0)$

- if $S(D)$ has non-trivial elementary divisors, replace them by 1
- the stabilizer matrix $(0 | I_0)$ 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]).
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! Dziekuje!

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).
References


