Quantum turbo-codes

Jean-Pierre Tillich (INRIA)
email: jean-pierre.tillich@inria.fr

January 23, 2008
1. Introduction

- nontrivial task to build such a quantum computer: need to address the issue of decoherence $\implies$ a way to protect quantum registers against unwanted evolutions. Quantum codes are a way to perform this and to do fault-tolerant computation.

- Quantum key distributions protocols could benefit from quantum codes (to increase the communication distance).
Quantum LDPC codes and quantum LDPC codes

Would have the same advantages as in the classical setting

▶ easy to decode by iterative decoding algorithms,
▶ possible to operate with them successfully at rates near capacity,
▶ better than concatenated coding schemes.
Quantum LDPC codes

- Suggested in 2003 by McKay-Ollivier-Tillich
- Have apparently drawbacks that classical LDPC codes do not have
  - parity-check matrix in the quantum case has to fulfill orthogonality constraints → random constructions impossible?
  - orthogonality constraints → many 4-cycles in the Tanner graph: problems with iterative decoding.
  - no family of quantum LDPC code is known with non-vanishing rate and unbounded minimum distance.
Serial quantum turbo-codes

- suggested by Ollivier-Tillich in 2005 as a way to overcome these problems.
- as for quantum LDPC codes it is possible to build such codes and decode them with iterative decoding algorithms.
- freedom to introduce randomness in the construction what we do not have for quantum LDPC codes.
- much simpler to construct.
2. Error Model

Much richer error model than in the classical setting

<table>
<thead>
<tr>
<th>qubit flip ((X))</th>
<th>phase flip ((Z))</th>
<th>both ! ((Y))</th>
</tr>
</thead>
<tbody>
<tr>
<td>(</td>
<td>0\rangle \rightarrow</td>
<td>1\rangle)</td>
</tr>
<tr>
<td>(</td>
<td>1\rangle \rightarrow</td>
<td>0\rangle)</td>
</tr>
</tbody>
</table>

\(X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\)

\(Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\)

\(Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\)
The Pauli group over $n$ qubits $\mathcal{G}_n$

$$\mathcal{G}_n = \{ \mathcal{E}_1 \otimes \mathcal{E}_2 \otimes \cdots \otimes \mathcal{E}_n | \mathcal{E}_i \in \mathcal{G}_1 \}$$

$$\cong \{ I, X, Y, Z \}^n \times \{ \pm 1, \pm i \}$$

$$x^2 = y^2 = z^2 = I,$$

$$xy = -yx = iz,$$

$$xz = -zx = -iy$$

$$\mathcal{G}_n / \{ \pm I, \pm iI \} \cong \mathbb{F}_4^n$$

$$[I] \leftrightarrow 0, [Z] \leftrightarrow 1, [X] \leftrightarrow \omega, [Y] \leftrightarrow \bar{\omega}$$
The depolarizing channel

The depolarizing channel of probability of error \( p : E = (E_i)_i \in \mathbb{F}_4^n \) such that the \( E_i \)'s are independent and

\[
\begin{align*}
\text{Prob}(E_i = 0) &= 1 - p \\
\text{Prob}(E_i = 1) &= \text{Prob}(E_i = \omega) = \text{Prob}(E_i = \bar{\omega}) = \frac{p}{3}.
\end{align*}
\]
3. Quantum code and encoding

- A quantum code $\mathcal{C}$ protecting $k$ qubits by embedding them in an $n$-qubit system: subspace of dimension $2^k$ of $\mathbb{C}^{2^n}$.
- An encoding for such a code: unitary transform $\mathcal{U}: \mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^n}$ such that

$$\mathcal{C} = \mathcal{U} \left( \mathbb{C}^{2^k} \otimes |0_{n-k}\rangle \right).$$
3. Definition of a stabilizer code

- **The Clifford group on \( n \) qubits**: subgroup of unitary transform \( \mathcal{U} \) on \( \mathbb{C}^{2^n} \) such that \( \mathcal{U} \mathcal{G}_n \mathcal{U}^\dagger = \mathcal{G}_n \).

- can be implemented by a quantum circuit of size \( O(n^2) \) by using elementary quantum gates over 1 and 2 qubits.

- **Stabilizer code**: code for which the encoding is a Clifford transform.
The discrete encoding matrix

A binary matrix $U$ of size $2n \times 2n$ such that for any $E \in G_n$ :

$$\alpha(E).U = \alpha(UEU^\dagger),$$

where

$$\alpha : G_n \rightarrow \mathbb{F}_2^{2n}$$

$$\varepsilon \varepsilon_1 \otimes \ldots \varepsilon_n \mapsto \beta(\varepsilon_1) \ldots \beta(\varepsilon_n)$$

and

$$\beta(\mathcal{X}) = (1, 0), \quad \beta(\mathcal{Z}) = (0, 1).$$
The encoding matrix

The encoding matrix $U$ is a symplectic matrix:

$$U \Lambda_n U^T = \Lambda_n$$

where

$$\Lambda_n = I_n \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$ 

Conversely, any symplectic matrix is the encoding matrix associated to a certain Clifford transform.
Stabilizer

Harmless errors for stabilizer codes

\[ Z_i \stackrel{\text{def}}{=} \underbrace{I \otimes \cdots \otimes I \otimes Z \otimes I}^{i - 1 \text{ times}} \otimes \underbrace{I \otimes \cdots \otimes I}_{n - i \text{ times}} \]

All errors of the form \( UZ_iU^{\dagger} \) are harmless for \( i > k \).

For \( |\psi\rangle \in \mathcal{C}, \exists |\phi\rangle \in \mathbb{C}^{2^k} \) s.t. \( |\psi\rangle = U (|\phi\rangle \otimes |0_{n-k}\rangle) \).

\[
UZ_iU^{\dagger}|\psi\rangle = UZ_iU^{\dagger}U (|\phi\rangle \otimes |0_{n-k}\rangle) \\
= UZ_i (|\phi\rangle \otimes |0_{n-k}\rangle) \\
= U (|\phi\rangle \otimes |0_{n-k}\rangle) \\
= |\psi\rangle
\]
Discrete harmless errors

\[ \alpha(UZ_iU^\dagger) = \alpha(Z_i)U \]

and

\[ \alpha(Z_i) = \begin{array}{c} \begin{array}{c} \text{i - 1 times} \\ \text{n - i times} \end{array} \\ 0 \ldots 0 \end{array} \begin{array}{c} 1 \\ 0 \ldots 0 \end{array} \]

\[ \Downarrow \]

harmless errors in \((\{0\}_k \times \{0, 1\}^{n-k}) \cdot U\)
Decoding

For quantum codes

DECODING =

1. performing the inverse of the encoding transformation \( \mathcal{U} \),
2. measuring the \( n - k \) last qubits,
3. estimating the “most likely” error given what was measured,
4. Performing the relevant unitary transform.
Measure of the syndrome

\[ |\psi\rangle = U (|\phi\rangle \otimes |0_{n-k}\rangle) \]

\[ |\psi\rangle \xrightarrow{\text{error}} E |\psi\rangle \]

\[ E = U^{\dagger} E |\psi\rangle \]

\[ U^{\dagger} E |\psi\rangle = U^{\dagger} E U (|\phi\rangle \otimes |0_{n-k}\rangle) \]

\[ U^{\dagger} E U = \varepsilon E_1 \otimes \cdots \otimes E_n \]

\[ E |\psi\rangle \xrightarrow{\text{measure}} s_1 \cdots s_{n-k} \]

with \( s_i = 0 \) if \( E_{k+i} \in \{I, Z\} \) and \( s_i = 1 \) otherwise.
Information symbols and syndrome

For $E \in \mathbb{F}_4^n$ let the information symbols corresponding to $E \in \mathbb{F}_4^n$ be given by $L_1, \ldots, L_k$ where

$$\begin{align*}
(L_1, L_2, \ldots L_k, S_1 \ldots, S_{n-k}) & \overset{\text{def}}{=} EU^{-1}, \quad L_i, S_i \in \mathbb{F}_4.
\end{align*}$$

$$\begin{align*}
C_0 & = \left(\{0_k\} \times \{0, 1\}^{n-k}\right).U \\
C & = \left(\mathbb{F}_4^k \times \{0, 1\}^{n-k}\right).U \\
s(E) & = (\text{tr}(S_i))_{1 \leq i \leq n-k} \\
d(C) & = \min \left\{|(L, S).U| : L \neq 0, S \in \{0, 1\}^{n-k}\right\}
\end{align*}$$
Stabilizer

Classical case

Let $C$ be a binary linear code of dimension $k$ and length $n$ with generating matrix $G$ (of size $k \times n$) and parity-check matrix $H$ (of size $(n - k) \times n$).

$$C = \{xG; x \in \mathbb{F}_2^k\}$$

$$= \{x \in \mathbb{F}_2^n | Hx^t = 0\}$$

Let $H^{-1}$ be a right-inverse for $H : HH^{-1} = I_{n-k}$. Let $U$ be the classical encoding matrix be defined by

$$U = \begin{pmatrix} G \\ (H^{-1})^T \end{pmatrix}.$$
**Classical case**

For $E \in \mathbb{F}_2^n$ let the information symbols corresponding to $E \in \mathbb{F}_2^n$ be given by $L_1, \ldots, L_k$ where

$$(L_1, L_2, \ldots L_k, S_1 \ldots, S_{n-k}) \overset{\text{def}}{=} EU^{-1}, \quad L_i, S_i \in \mathbb{F}_2.$$

$$C_0 = \{0_n\}$$

$$C = (\mathbb{F}_2^k \times 0_{n-k}) \cdot U$$

$$s(E) = (S_i)_{1 \leq i \leq n-k}$$

$$d(C) = \min \{|(L, 0_{n-k}) \cdot U| : L \neq 0\}$$
## Analogies

<table>
<thead>
<tr>
<th></th>
<th>Linear codes</th>
<th>Stabilizer codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>encoding matrix</td>
<td>$U = \begin{pmatrix} G \ (H^{-1})^T \end{pmatrix}$</td>
<td>symplectic matrix of size $2n$.</td>
</tr>
<tr>
<td>code</td>
<td>$C = (\mathbb{F}<em>2^k \times 0</em>{n-k}) \cdot U$</td>
<td>$C = (\mathbb{F}_4^k \times {0, 1}^{n-k}) \cdot U$</td>
</tr>
<tr>
<td>harmless errors</td>
<td>$C_0 = {0_n}$</td>
<td>$C_0 = ({0_k} \times {0, 1}^{n-k}) \cdot U$</td>
</tr>
<tr>
<td>min. distance</td>
<td>$\min {</td>
<td>c</td>
</tr>
<tr>
<td>syndrome</td>
<td>$s(E) = (S_i)_{1 \leq i \leq n-k}$</td>
<td>$s(E) = (\text{tr}S_i)_{1 \leq i \leq n-k}$</td>
</tr>
</tbody>
</table>
Concatenation of codes

$C_1$, $[[k_1 + r_1, k_1]]$-code with encoding $U_1$, 
$C_2$, $[[k_1 + r_1 + r_2, k_1 + r_1]]$-code with encoding $U_2$.

$\mathbb{C}^{2^{k_1}} \otimes |0_{r_1}\rangle \otimes |0_{r_2}\rangle \xrightarrow{U_1} \mathbb{C}^{2^{k_1+r_1}} \otimes |0_{r_2}\rangle \xrightarrow{U_\pi} \mathbb{C}^{2^{k_1+r_1}} \otimes |0_{r_2}\rangle \xrightarrow{U_2} \mathbb{C}^{2^{k_1+r_1+r_2}}$

corresponds to in the discrete setting

$L_1, ..., L_{k_1}, S_1, ..., S_{r_1}, S'_1, ..., S'_{r_2}$ \xrightarrow{U_1} $L'_1, ..., L'_{k_1+r_1}, S'_1, ..., S'_{r_2}$ \xrightarrow{U_\pi} $L'_{\pi(1)}, ..., L'_{\pi(k_1+r_1)}, S'_1, ..., S'_{r_2}$ \xrightarrow{U_2} $E_1, ..., E_{k_1+r_1+r_2}$
The problem

Assume that there exists for the second code a bound $D$ such that for each $i \in \{1, \ldots, k_1 + r_1\}$ and every $\gamma \neq 0$ in $\mathbb{F}_4$ there exists a choice for the $S_j'$’s in $\mathbb{F}_2$ such that

$$\left| \begin{array}{cc}
i-1 \text{ times} & k_1 + r_1 - i \text{ times} \\ (0 \ldots 0, \gamma, 0 \ldots 0, S_1', \ldots S_{r_2}')U_2 \end{array} \right| \leq D$$

then if the minimum distance of the first code is $d$ the minimum distance of the concatenated code is upper bounded by $dD$.
The problem (II)

\[ L_1, \ldots, L_{k_1}, S_1, \ldots, S_{r_1}, S'_1, \ldots, S'_{r_2} \]

with \( |L'_1, \ldots, L'_{k_1+r_1}| \)

for each of the \( L'_{\pi(i)} \neq 0 \) consider the corresponding \( S'_1 \ldots S'_{r_2} \)

and sum them to obtain

\[ U_1 \rightarrow L'_1, \ldots, L'_{k_1+r_1}, S'_1, \ldots, S'_{r_2} \]

\[ U_\pi \rightarrow L'_{\pi(1)}, \ldots, L'_{\pi(k_1+r_1)}, S'_1, \ldots, S'_{r_2} \]

\[ U_2 \rightarrow E_1, \ldots, E_{k_1+r_1+r_2} \]

with \( |E_1 \ldots E_{k_1+r_1+r_2}| \)

\[ \leq dD \]
When the second code is a juxtaposition of small codes

$U$ Clifford transformation on $n$ qubits, $D \leq n$.  

*stabilizer*
When the encoder is convolutional

\[ D \leq \frac{24}{32} \]
4. Quantum serial turbo-codes

Choose $\mathcal{U}_1$ and $\mathcal{U}_2$ as convolutional encoders.

[Kahale-Urbanke] In the classical case, by an averaging argument, if the free distance of $\mathcal{C}_1$ is $d_1$ and if $\mathcal{U}_2$ is a non-catastrophic and recursive encoder, then the minimum distance of the resulting code is typically of order $\Theta \left( n \frac{d_1-2}{d_1} \right)$.

Generalizes easily to the quantum setting.
Quantum convolutional codes

- Choose an encoding matrix $U$ over $n + m$ qubits.
- The encoding matrix of the convolutional code is defined by

$$U_1 \rightarrow n + m U_{n+1} \rightarrow 2n + m \cdots U_{n(i-1)+1} \rightarrow ni + m \cdots,$$

where

$$(P_1, \ldots,) U_{a+1} \rightarrow a + n + m = (P'_1, \ldots,)$$

with

$$P'_i = P_i \text{ for } i \leq a \text{ or } i > a + n + m$$

$$(P'_a+1, \ldots, P'_a+n+m) = (P_a+1, \ldots, P_a+n+m) \cdot U.$$
Quantum convolutional codes

for an \([\lbrack n, k \rbrack]\) convolutional encoder of time duration \(N\)

\[
(S_0, L_1, S_1, \ldots, L_i, S_i, \ldots, L_N, S_N) \xrightarrow{\text{conv. encoder}} P = (P_1, P_2, \ldots, P_N)
\]

with \(S_0 \in \mathbb{F}_4^m, L_i \in \mathbb{F}_4^k, S_i \in \mathbb{F}_4^{n-k}\), for \(1 \leq i \leq N\), \(P_i \in \mathbb{F}_4^n\), for \(1 \leq i < N\) and \(P_N \in \mathbb{F}_4^{n+m}\).

\[
(S_0, L_1, S_1)U = (P_1, M_1)
\]

\[
(M_{i-1}, L_i, S_i)U = (P_i, M_i) \text{ and}
\]

\[
(M_{N-1}, L_N, S_N)U = P_N
\]

\(M_i \in \mathbb{F}_4^m\) for \(i \in \{1, \ldots, N - 1\}\)
State diagram

- Vertex set: $\mathbb{F}_4^m$.

- Labelled edge from $M$ to $M'$ with labels $(L, P) \in \mathbb{F}_4^k \times \mathbb{F}_4^n$ if there exists $S \in \mathbb{F}_2^{n-k}$ such that

$$(M, L, S)U = (P, M').$$
Catastrophic and recursive encoders

\[(S_0, L_1, S_1, \ldots, L_i, S_i, \ldots) \xrightarrow{\text{conv. encoder}} P = (P_1, P_2, \ldots, ) \text{ with} \]
\[S_0 \in \mathbb{F}_2^m, S_i \in \mathbb{F}_2^{m-k} \quad \text{for } i \geq 1 \]
\[L \overset{\text{def}}{=} L_1, L_2, \ldots, \]

- **Non-catastrophic encoder**: \(\text{supp}(P) \text{ finite } \Rightarrow \text{supp}(L) \text{ finite.} \)
- **Recursive encoder**: \(|L| = 1 \Rightarrow \text{supp}(P) \text{ infinite.} \)
Bad news...

Theorem 1. [Poulin-Tillich-Ollivier-07] There are no encoders which are at the same time non-catastrophic and recursive.

Remote consequence of the fact that $U$ is a symplectic matrix + the fact that the $S_i$ might be chosen different from 0.
Non catastrophic or recursive encoders?

- Non-catastrophic and non-recursive encoders:
  - ⇒ Constant minimum distance...
  - Might be interesting up to moderate blocklength.

- Catastrophic and recursive encoders
  - Iterative decoding does not converge (the scheme has to be modified).
  - The minimum distance might be unbounded.
An example at rate $\frac{1}{4}$, $m = 4$, and with non-catastrophic non-recursive encoders.