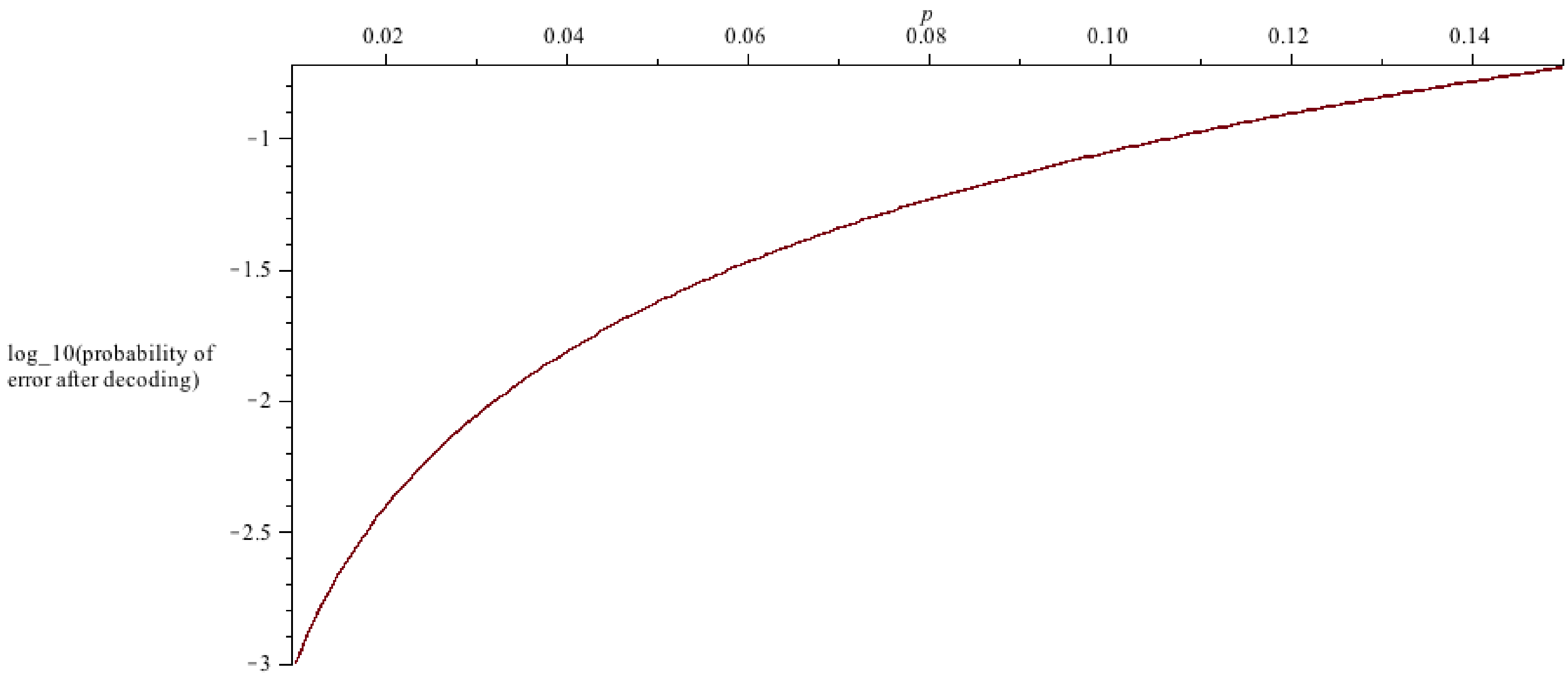
Turning error-reducing quantum turbo codes into error-correcting codes

Mamdouh Abbara (MEc), Iryna Andriyanova (ENSEA),
Jean-Pierre Tillich (INRIA)

QEC14

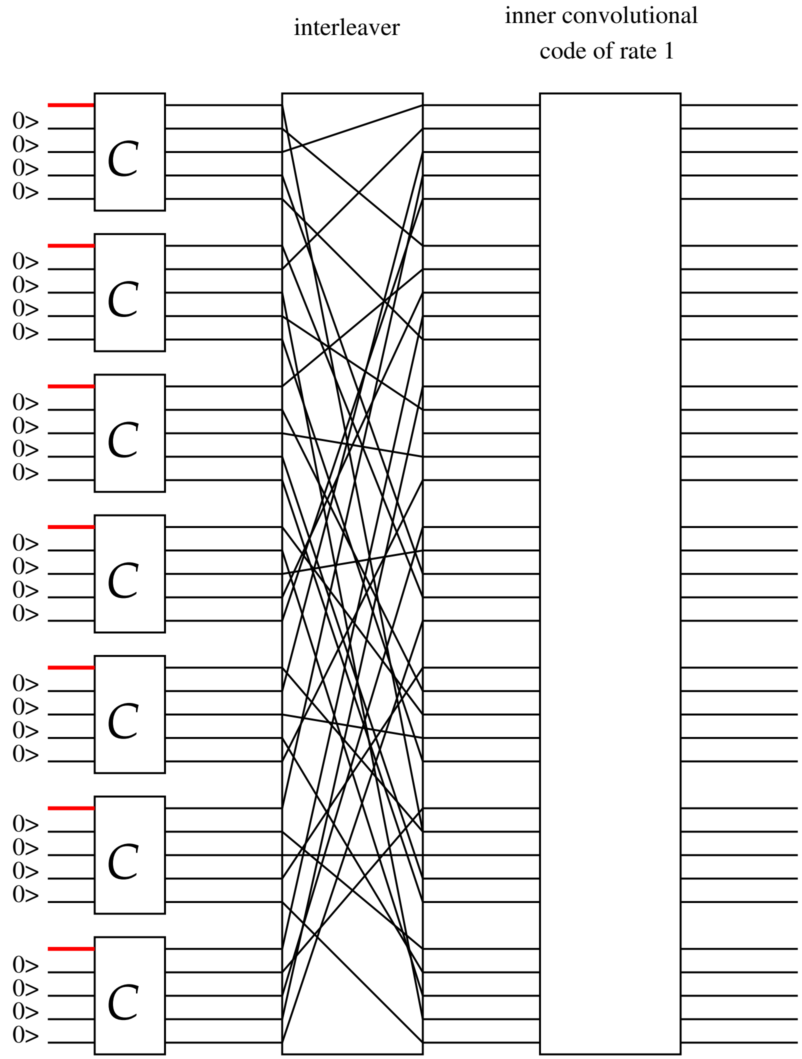
December the 17th, 2014

The $5-$qubit code



Probability of error after decoding the 5-qubit code

An alternative strategy for concatenation

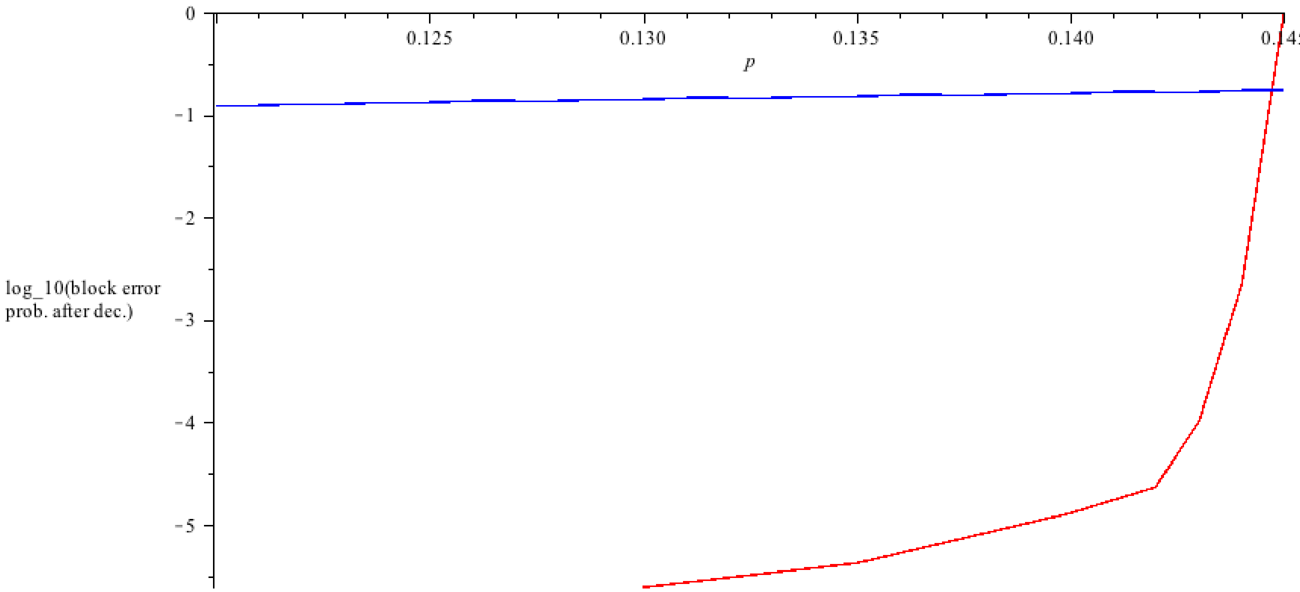


The message of this talk

- It is possible to concatenate with a rate 1 code (so no protection against errors at all...) and still achieve something nontrivial when the rate 1 code is a convolutional code.

Improving the $5-$qubit code

FIGURE 1: Probability of error after decoding



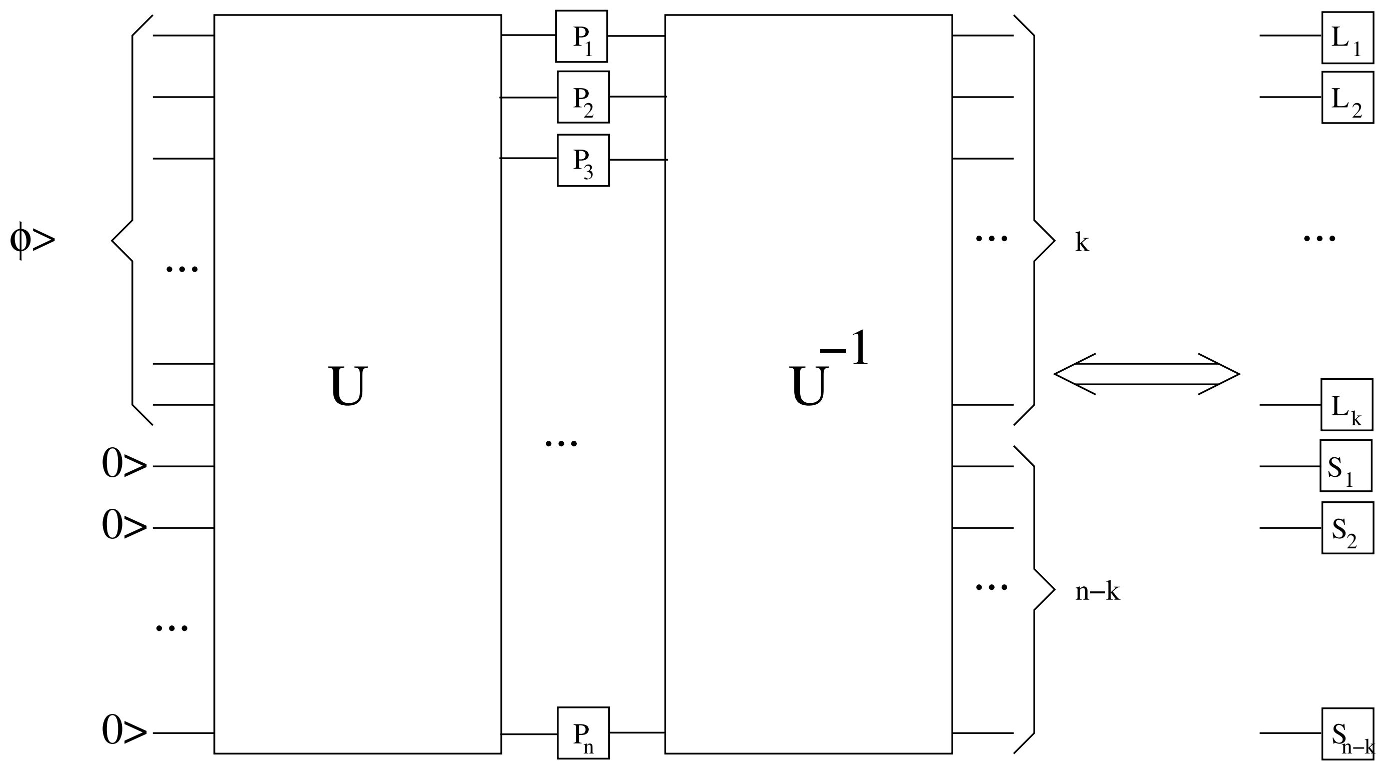
- complexity of encoding $\approx$ complexity of encoding a 5-qubit code
- Rate $\frac{1}{5} \to \frac{1}{8}$
- same complexity of decoding as the 5-qubit code
- modified quantum turbo-code construction

serial quantum turbo-codes

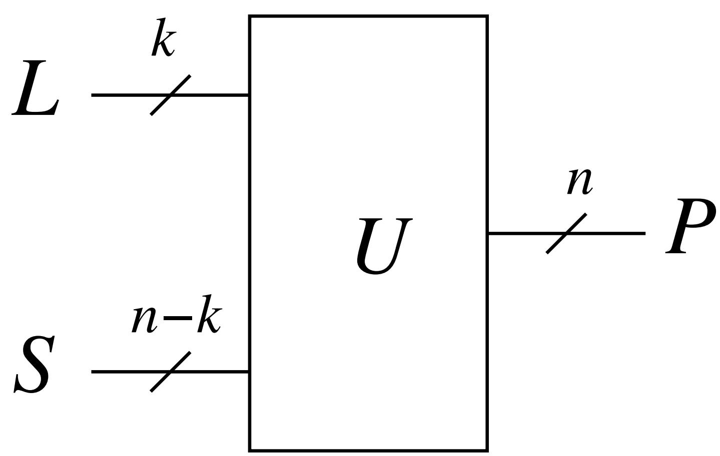
- as for quantum LDPC codes it is possible to build such codes and decode them with iterative decoding algorithms.
- freedom to introduce randomness in the construction what we do not have for quantum LDPC codes.
- much simpler to construct.
- but there are also some problems related to encoding issues...

2. Concatenation of codes

– $\mathcal{P}_n$ Pauli group over n quits
– Clifford transformation U : $U^\dagger \mathcal{P}_n U \in \mathcal{P}_n$



- Physical error $P = P_1 P_2 \dots P_n$
- Logical error,syndrome $LS = \underbrace{L_1 L_2 \dots L_k}_{\text{logical error}} \underbrace{S_1 \dots S_{n-k}}_{\text{syndrome}} = U^\dagger P U$



Stabilizer, Normalizer

- Stabilizer set $\mathcal{S}$ corresponds to $L = I \ldots I$, $S \in \{I, Z\}^{n-k}$:

$$\mathcal{S} = \left\{ \mathcal{U}(\underbrace{I \ldots I}_{k} S)\mathcal{U}^{\dagger}, S \in \{I, Z\}^{n-k} \right\}$$

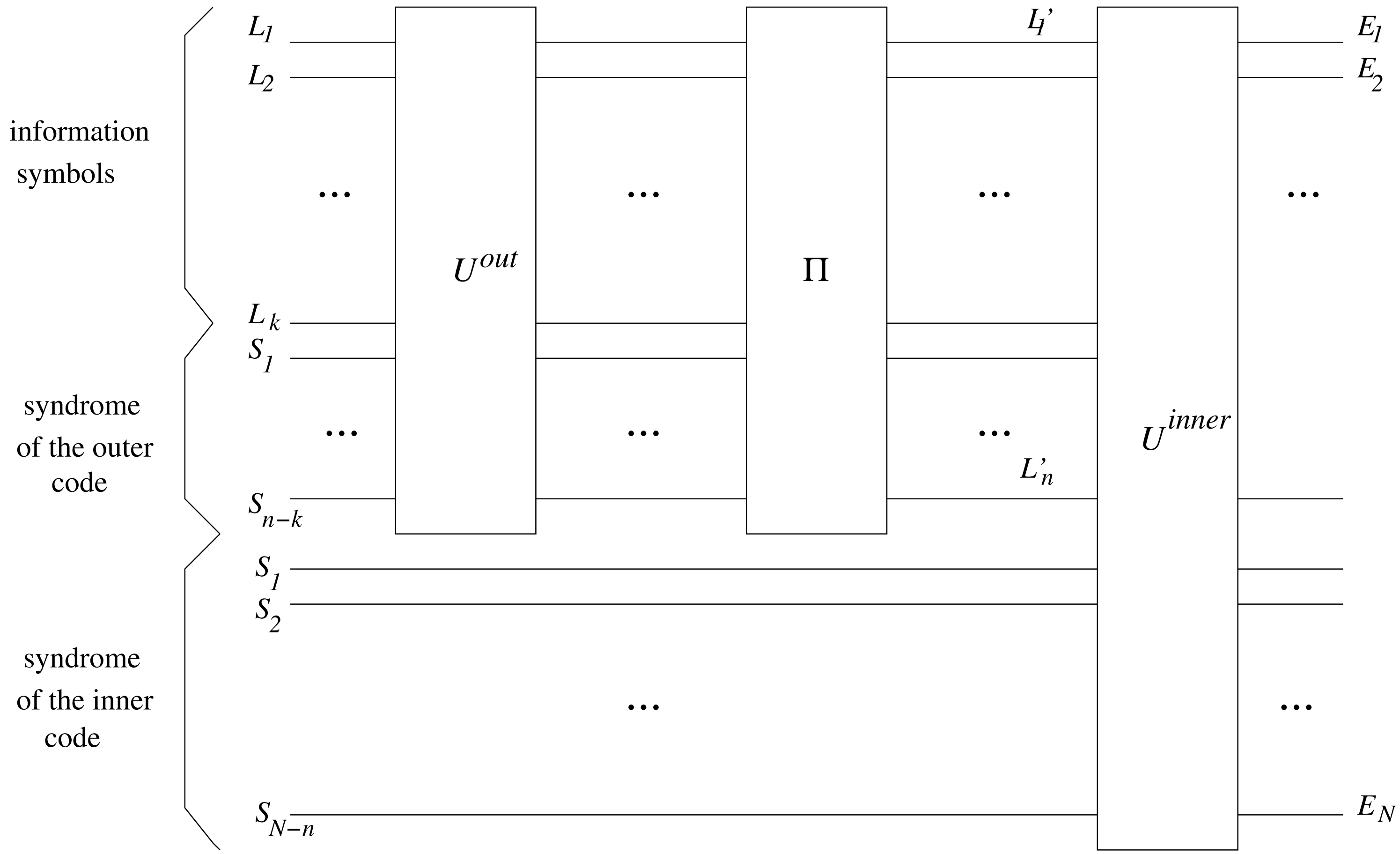
- Normalizer set $\mathcal{N}$ corresponds to $S \in \{I, Z\}^{n-k}$.

$$\mathcal{N} = \{\mathcal{U}(L, S)\mathcal{U}^{\dagger}, S \in \{I, Z\}^{n-k}\}$$

- Quantum minimum distance

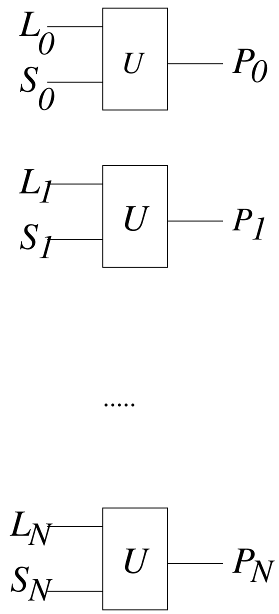
$$\begin{aligned} d_{\text{quantum}} &= \min\{|P| \in \mathcal{N} \setminus \mathcal{S}\} \\ d_{\text{classical}} &= \min\{|P| \in \mathcal{N} \setminus \{I \ldots I\}\} \end{aligned}$$

Serial concatenation of codes



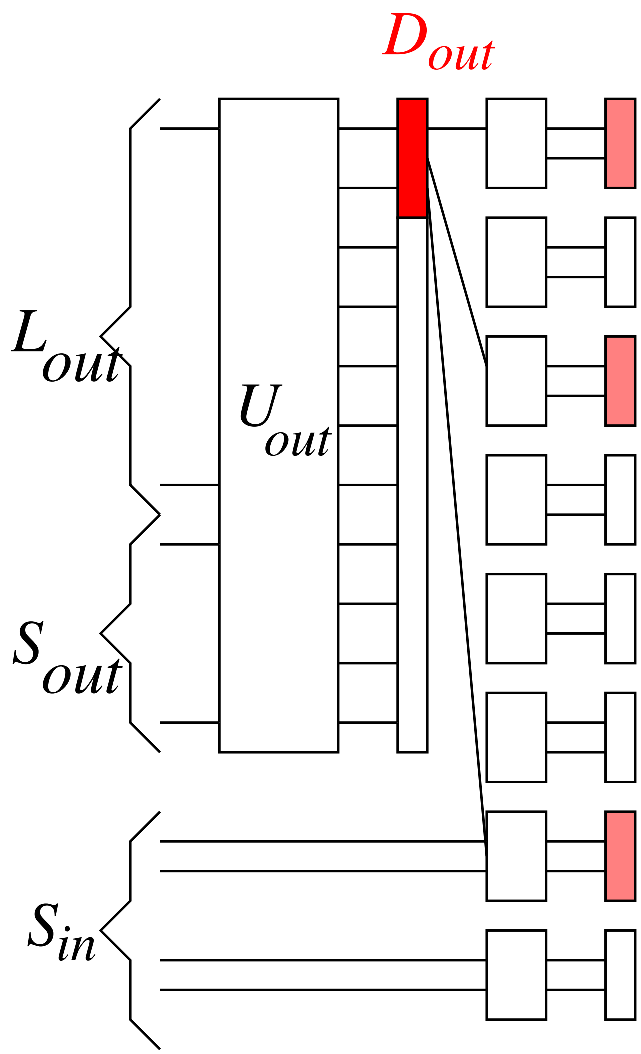
3. Minimum Distance Properties

When the inner code is a juxtaposition of small codes



U Clifford transformation on n qubits, $D_{\text{in}} \leq n$,

$$D_{\text{cont}} \leq D_{\text{out}} n.$$



$$D_{\text{con}} \le D_{\text{out}} n.$$

The problem (I)

$$L_1 \ldots L_{k_1} \underbrace{S_1 \ldots S_{r_1}}_{S_{\text{out}}} \underbrace{S'_1 \ldots S'_{r_2}}_{S_{\text{in}}} \xrightarrow{U_{\text{out}}} L'_1, \ldots, L'_{k_1+r_1} \underbrace{S'_1, \ldots, S'_{r_2}}_{S_{\text{in}}}$$

$$\xrightarrow{\Pi} L'_{\pi(1)}, \ldots, L'_{\pi(k_1+r_1)}, S'_1, \ldots, S'_{r_2}$$

$$\xrightarrow{U_{\text{in}}} P_1, \ldots, P_{k_1+r_1+r_2}$$

The problem (II)

Assume that there exists for the inner code a bound D such that for each $i \in \{1, \dots, k_1 + r_1\}$ and every $P \in \{X, Y, Z\}$ there exists a choice for the S'_j's in $\{I, Z\}$ such that

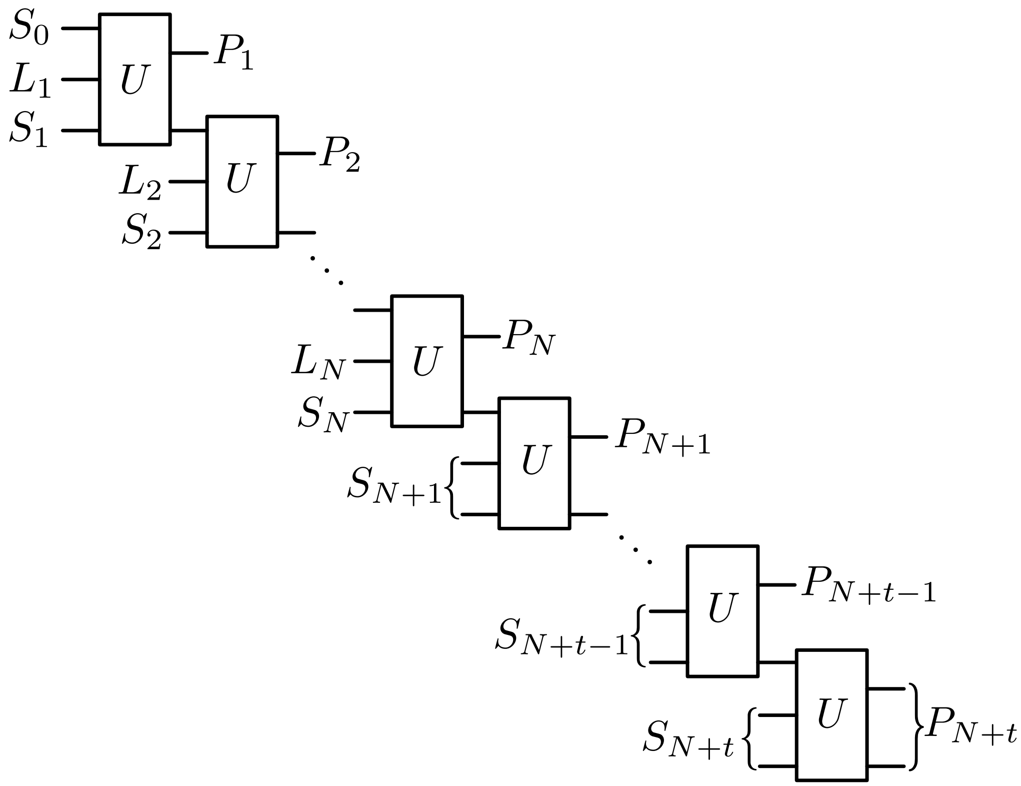
$$\left| U_{\text{in}}(\overbrace{I \dots I}^{i-1 \text{ times}} \; P \; \overbrace{I \dots I}^{k_1+r_1-i \text{ times}} \; S'_1, \dots S'_{r_2}) U_{\text{in}}^{\dagger} \right| \leq D$$

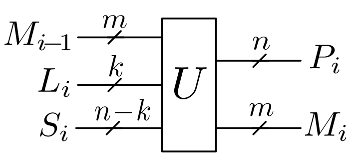
then if the minimum distance of the outer code is D_{out} the minimum distance of the concatenated code is upper bounded by $D_{\text{out}} D$

The problem(III)

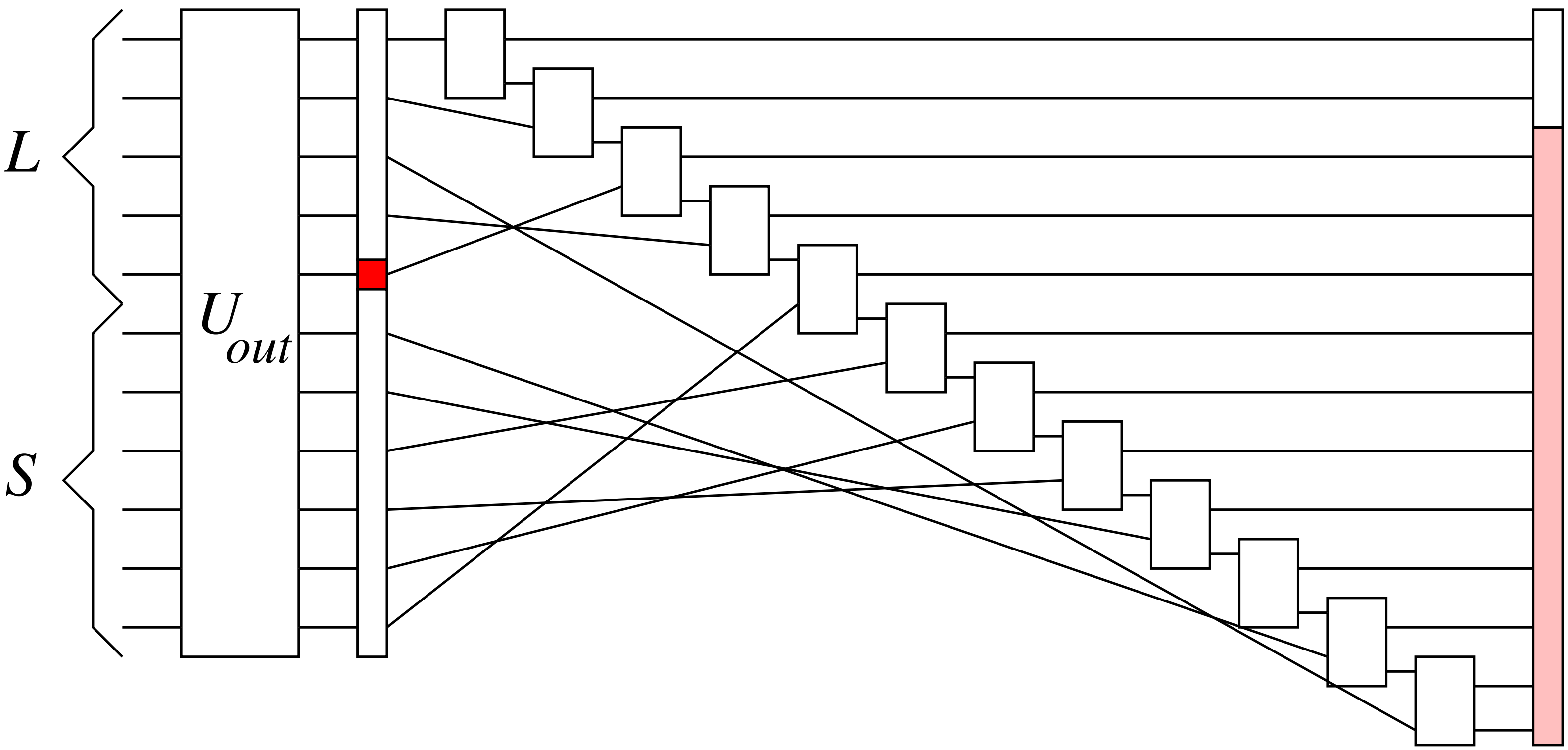
$$\begin{array}{rcl}
L_1 \ldots L_{k_1} \underbrace{S_1 \ldots S_{r_1}}_{S_{\text{out}}} \underbrace{S'_1 \ldots S'_{r_2}}_{S_{\text{in}}} & \xrightarrow{U_{\text{out}}} & L'_1, \ldots, L'_{k_1+r_1} \underbrace{S'_1, \ldots, S'_{r_2}}_{S_{\text{in}}} \\
\text{with } \left|L'_1, \ldots, L'_{k_1+r_1}\right| & = & D_{\text{out}} \\
 & \xrightarrow{\Pi} & L'_{\pi(1)}, \ldots, L'_{\pi(k_1+r_1)}, S'_1, \ldots, S'_{r_2} \\
\text{for each of the } L'_{\pi(i)} \neq I & \text{consider} & \text{the corresponding } S'^{i}_1 \ldots S'^{i}_{r_2} \\
\text{and mutiply them to obtain} & & S'_1, \ldots, S'_{r_2} \\
 & \xrightarrow{U_{\text{in}}} & P_1, \ldots, P_{k_1+r_1+r_2} \\
\text{with } |P_1 \ldots P_{k_1+r_1+r_2}| & \leq & D_{\text{out}} D
\end{array}$$

When the inner encoder is convolutional





$$D_{\text{in}} = O(1) \quad D_{\text{con}} \leq \quad ?$$



L
S
U_{out}

Classical setting

- Choose U_{out} and U_{in} as (classical) convolutional encoders.
- [Kahale-Urbanke-ISIT 1998] In the classical case, by an averaging argument, if the free distance of $\mathscr{C}_{\text{out}}$ is d_{out} and if U_{in} is a non-catastrophic and recursive encoder, then the minimum distance of the resulting code is typically of order $\Theta\left(N^{\frac{d_{\text{out}}-2}{d_{\text{out}}}}\right)$.
- Generalizes easily to the quantum setting ?

A first problem

Theorem 1. [Poulin-Tillich-Ollivier-ISIT 2008] *There are no quantum convolutional encoders which are at the same time non-catastrophic and recursive.*

Catastrophic/recursive

$$
\begin{array}{rcl}
(S_0, L_1, S_1, \dots, L_i, S_i, \dots) & \overset{\text{conv. encoder}}{\longrightarrow} & P = (P_1, P_2, \dots,) \text{ with} \\
S_0 \in \{I, Z\}^m, S_i \in \{I, Z\}^{n-k} & & \text{for } i \geq 1 \\
L & \overset{\text{def}}{=} & L_1, L_2, \dots,
\end{array}
$$

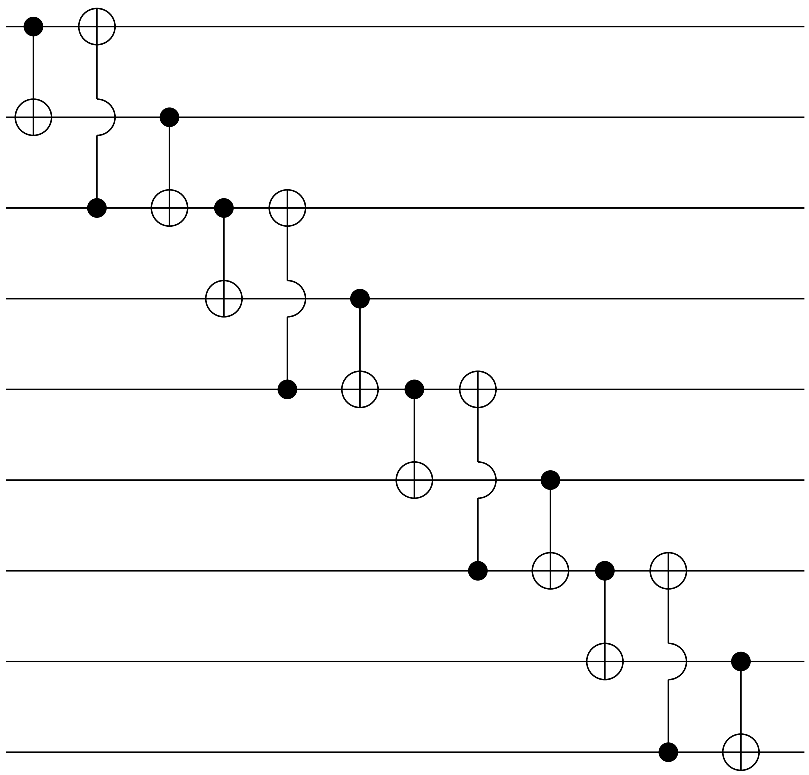
- Non-catastrophic encoder : supp(P) finite $\Rightarrow$ supp(L) finite.
- Recursive encoder : $|L| = 1 \Rightarrow$ supp(P) infinite.

A crucial argument used in the classical setting

Consider convolutional encoders for which

$$|L| \leq |P|$$

A quantum convolutional encoder that does the job



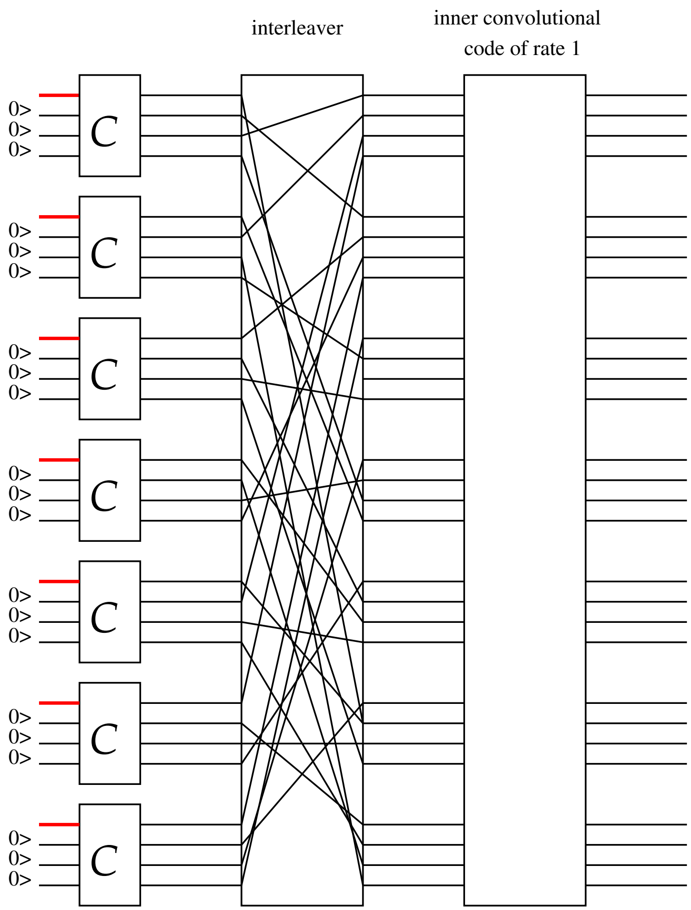
A theorem

Theorem 2. [Abbara-Tillich - ITW 2011] *If the inner code is the aforementioned convolutional code of rate* 1 *and the outer code is a juxtaposition of copies of a quantum code of classical minimum distance* $d_{\text{classical}}$ *and quantum minimum distance* d_{quantum}*, then with probability* $\to 1$ *as the length* N *of the inner code* $\to \infty$ *the minimum distance* D_{con} *of the concatenated scheme satisfies*

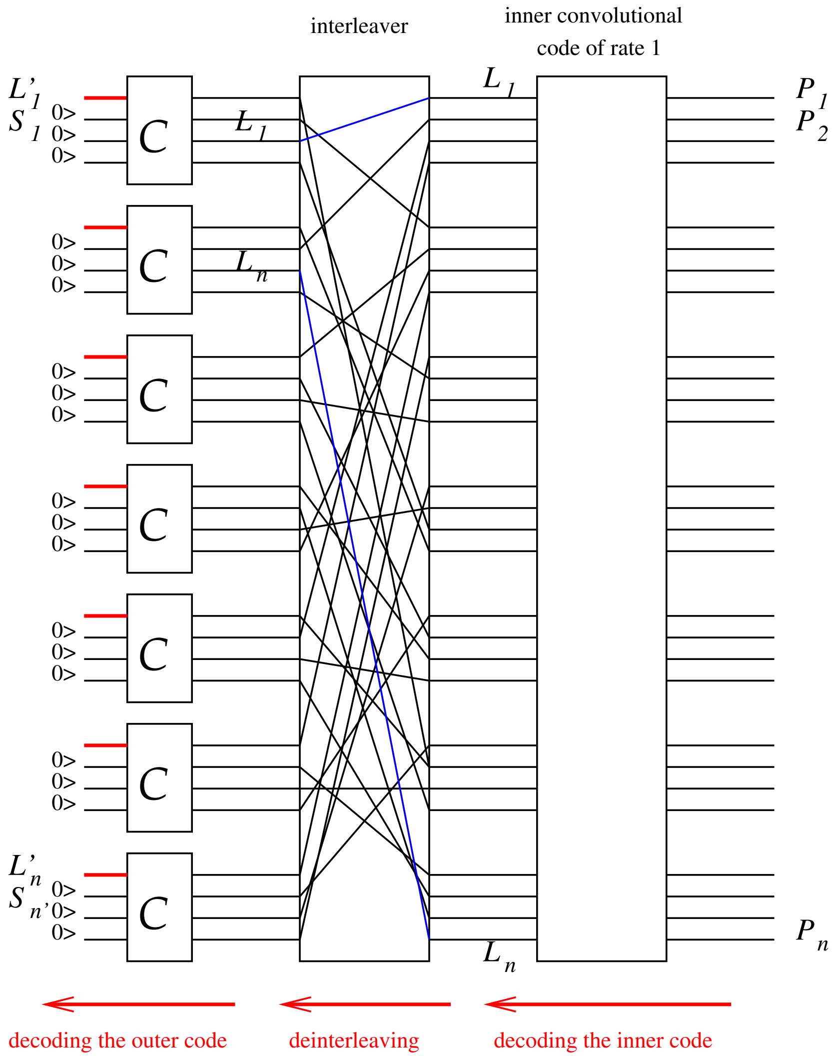
- $D_{\text{con}} = \Omega\left(N^{\frac{d_{\text{classical}}-2}{d_{\text{classical}}}}\right)$ *if* $d_{\text{classical}} > 2$
- $D_{\text{con}} = \Omega\left(\frac{\log N}{\log \log N}\right)$ *if* $d_{\text{classical}} = 2$ *and* $d_{\text{quantum}} \geq 3$.

The construction

A first attempt

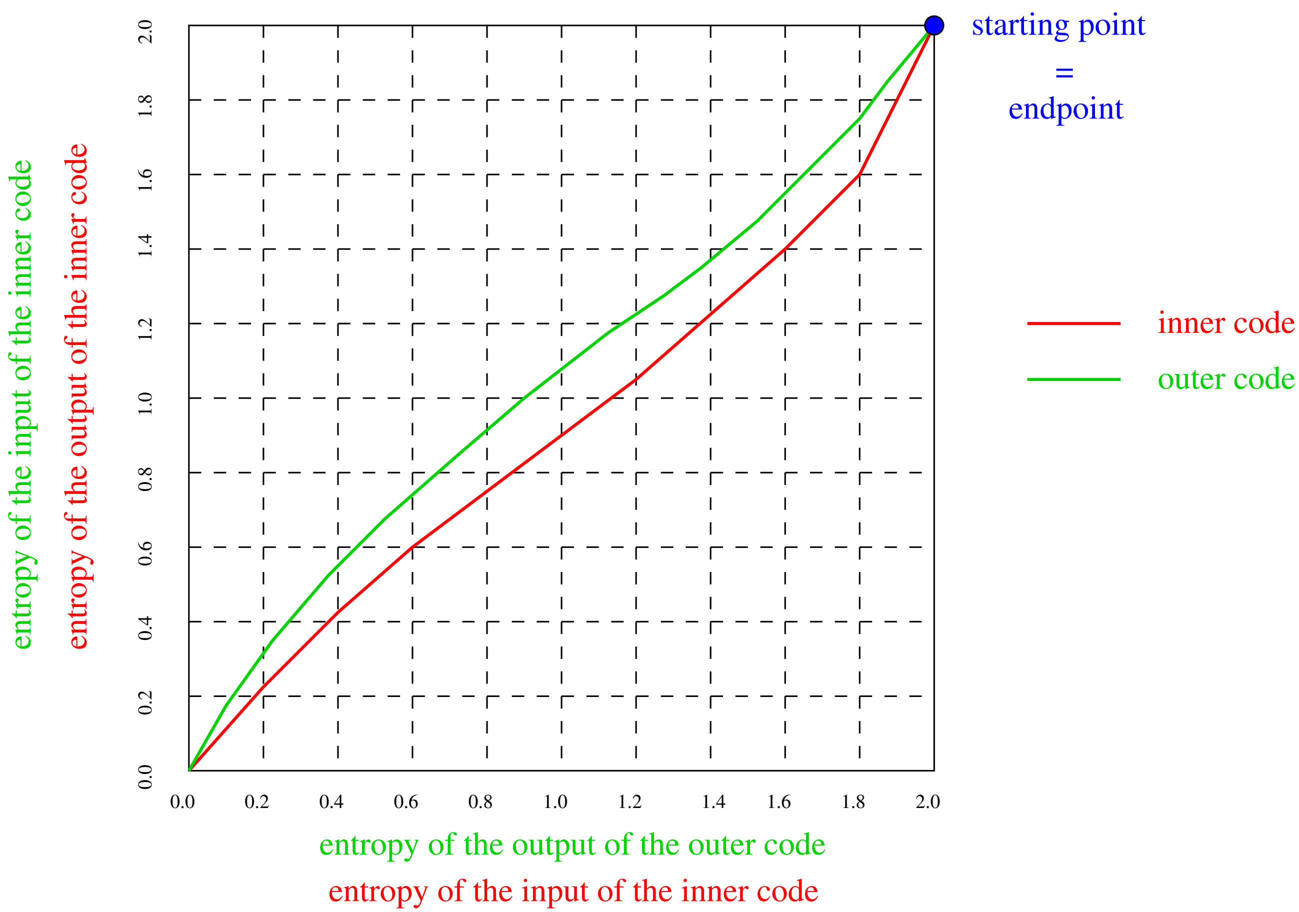


Decoding



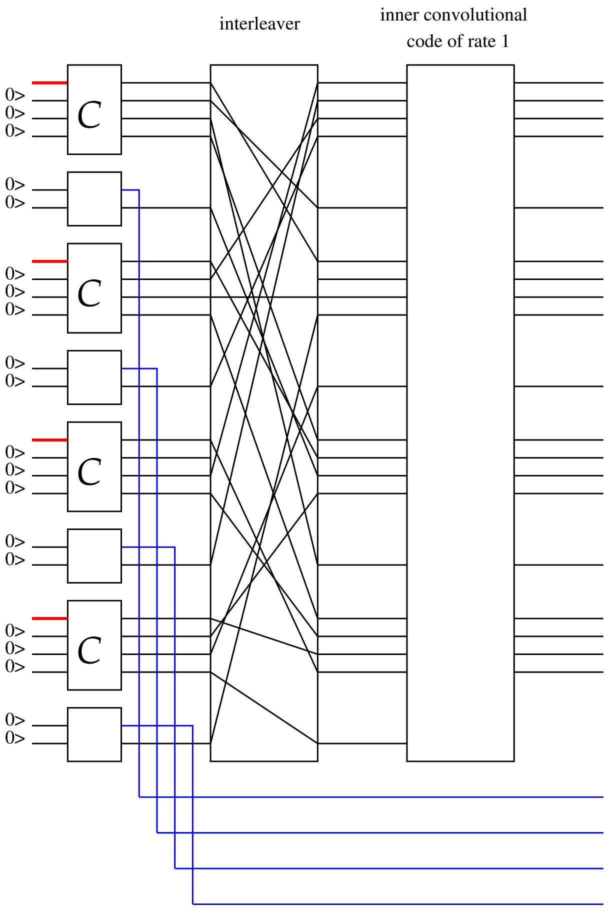
interleaver
inner convolutional code of rate 1
L'1
S1
0>
C
L1
Ln
L'n
Sn'
P1
P2
Pn
decoding the outer code
deinterleaving
decoding the inner code

The problem

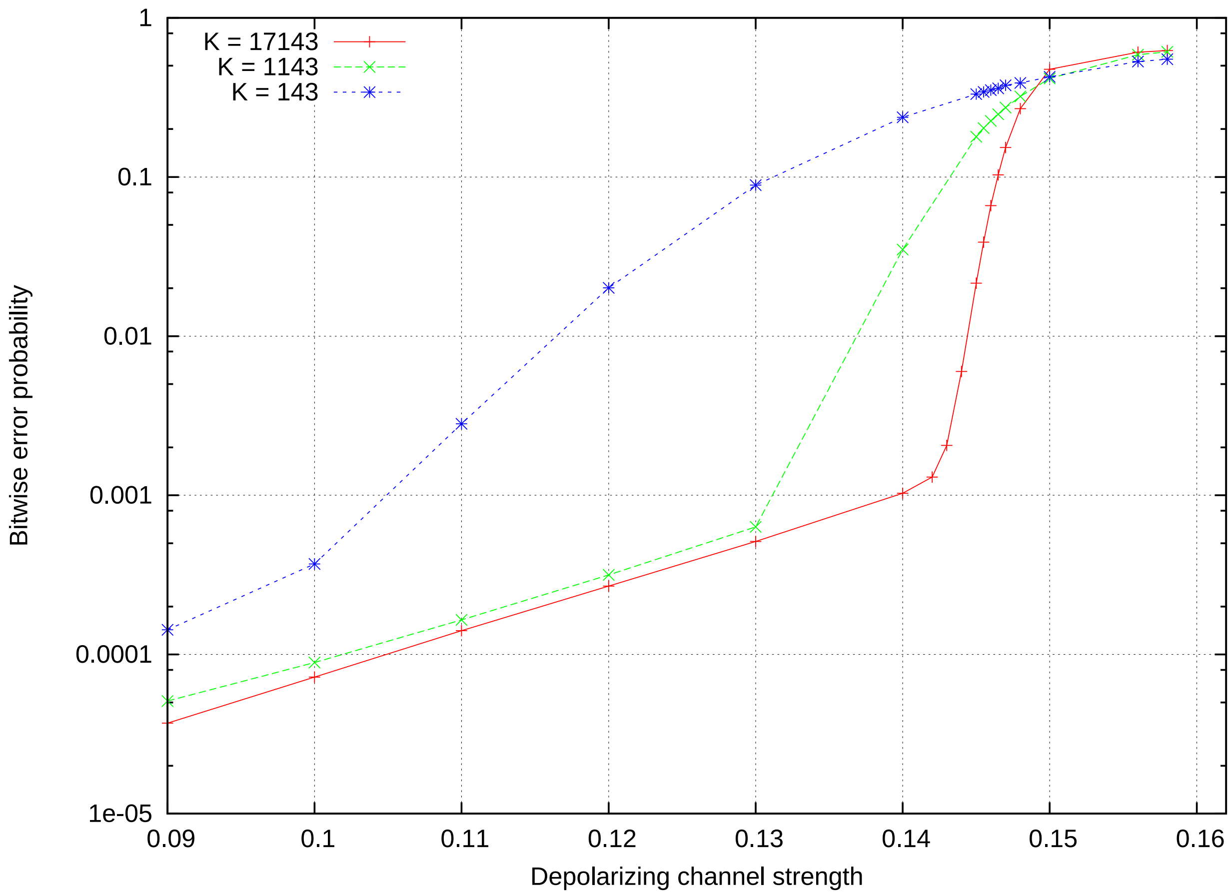


starting point
=
endpoint
inner code
outer code
entropy of the input of the inner code
entropy of the output of the inner code
entropy of the output of the outer code
entropy of the input of the inner code
0.0
0.2
0.4
0.6
0.8
1.0
1.2
1.4
1.6
1.8
2.0

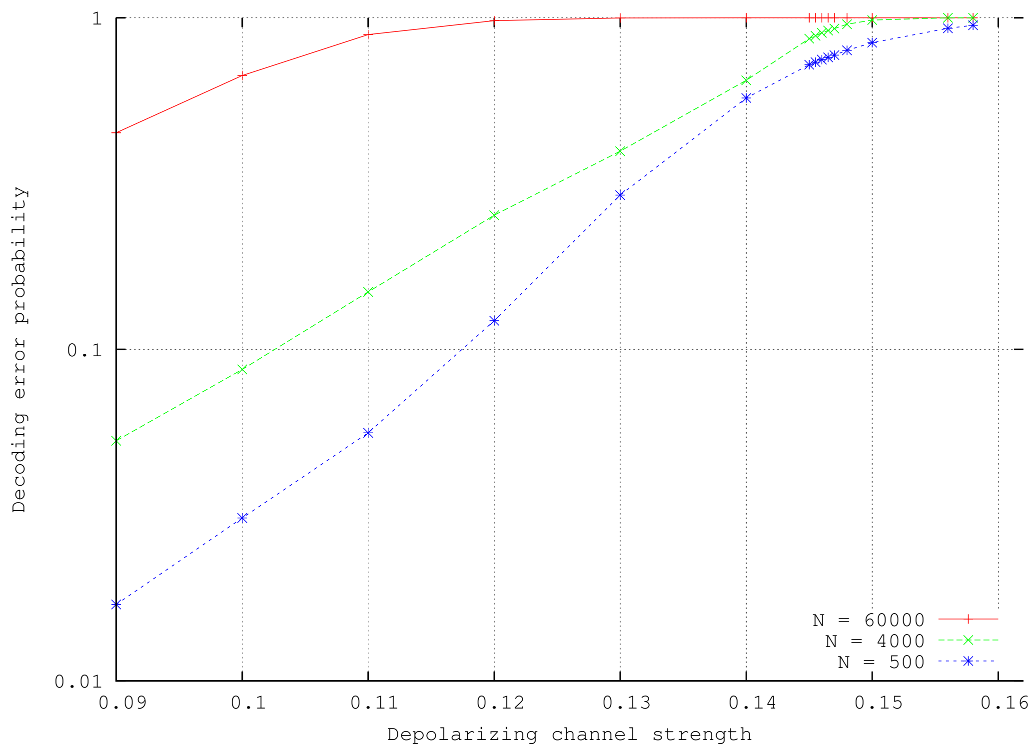
The modified construction



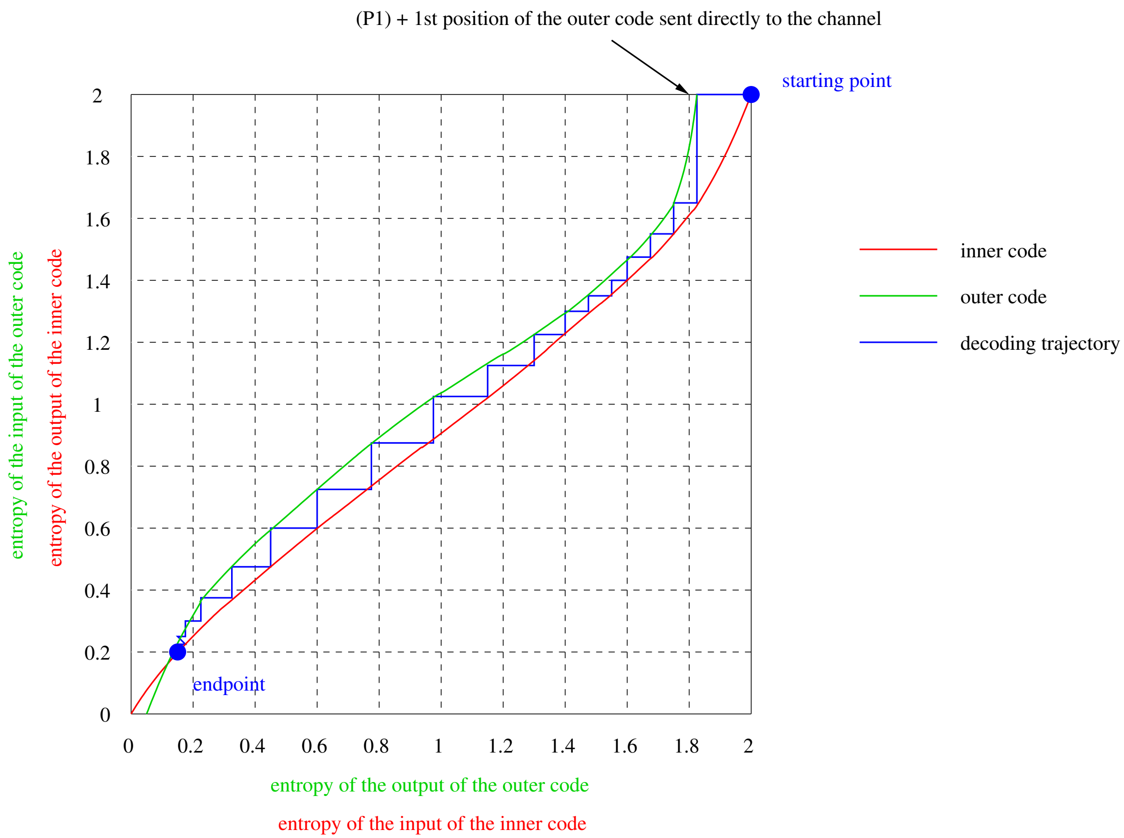
QuBit-error probability after decoding



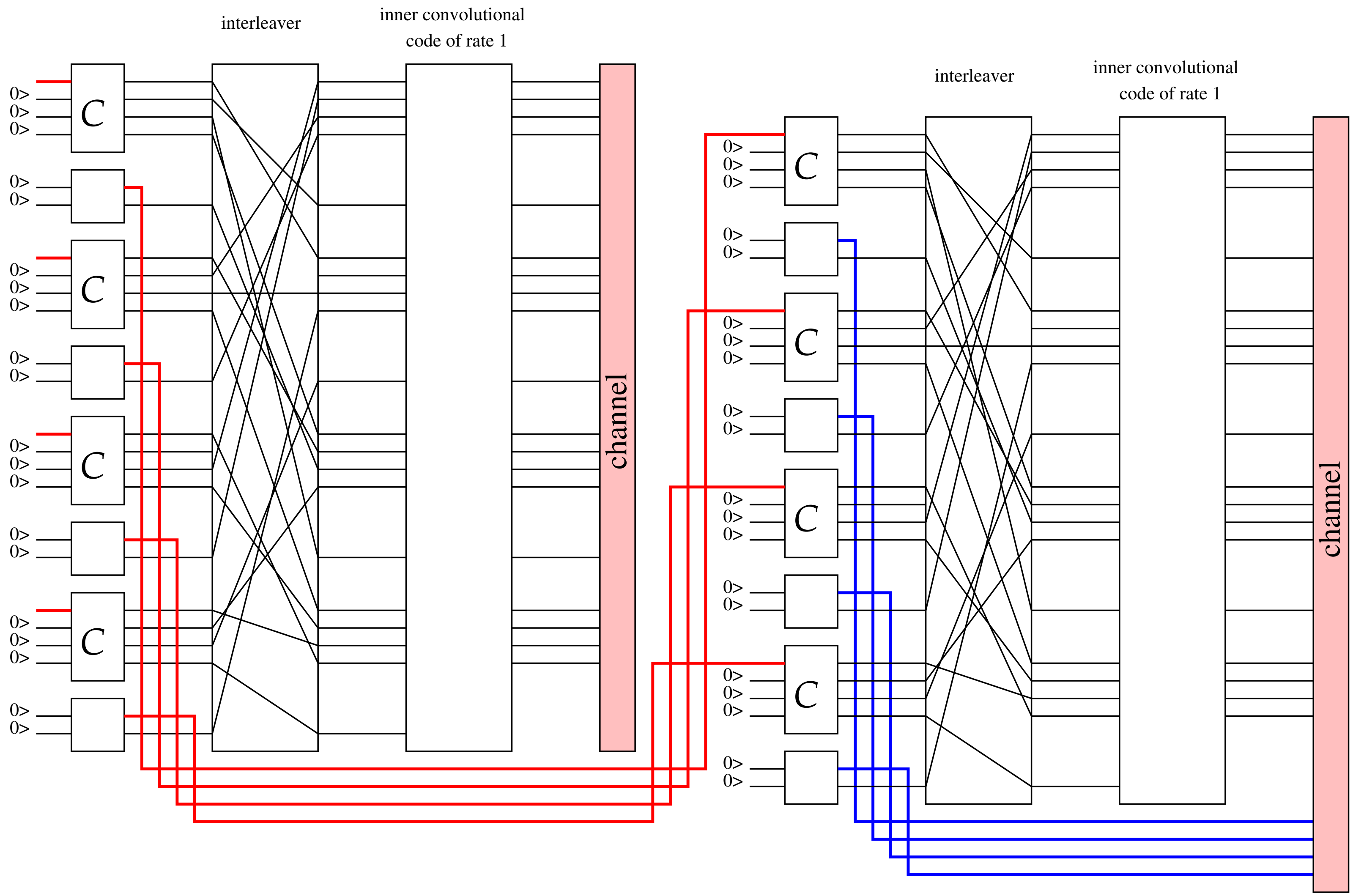
Probability of error per block



Entropy evolution during decoding



5. Going further : a multilevel construction



Analysis on the erasure channel

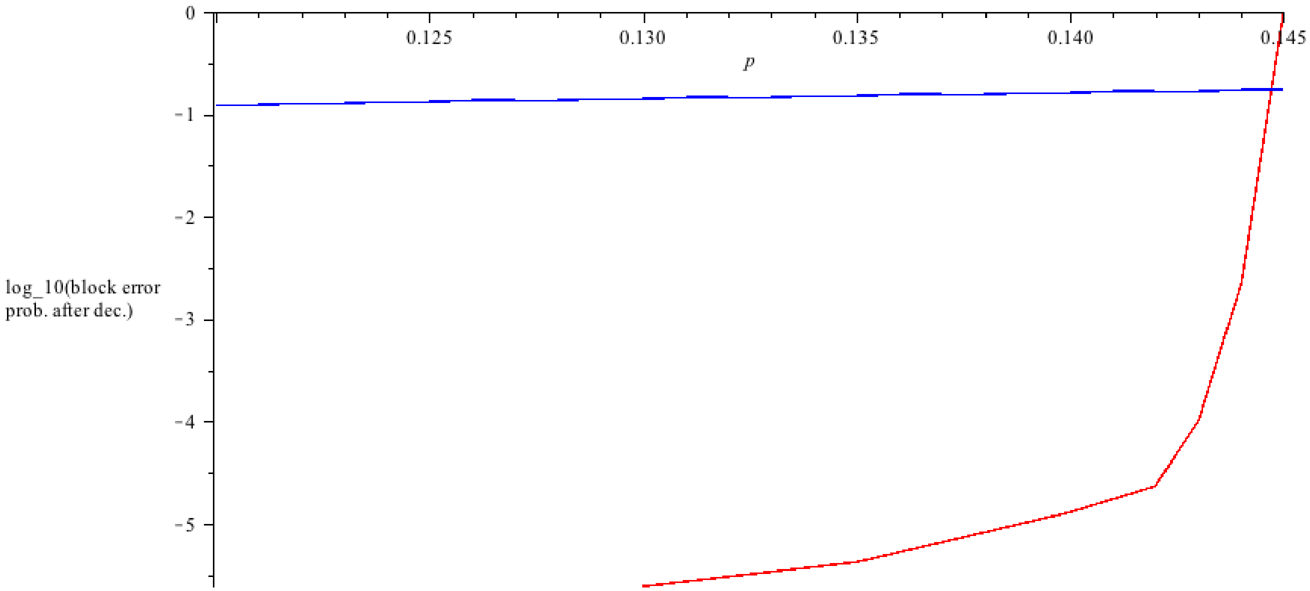
Theorem 3. *Let t be the number of stages of the concatenated construction where we assume that the underlying block code C is of minimum distance 3. Then the probability p_t that a logical qubit stays erased after transmission of the encoded words over an erasure channel of erasure probability p is given by*

$$p_t = O\left(p^{3^{t+1}+3^t-3}\right)$$

t	1	2	3
p_t	$O(p^9)$	$O(p^{33})$	$O(p^{105})$

Results

FIGURE 2: Probability of error after decoding/comparison with the 5-qubit code



Summary

Theorem 4. [Poulin-Tillich-Ollivier-08] *There are no quantum convolutional encoders which are at the same time non-catastrophic and recursive.*

Summary/Conclusion

- Non-catastrophic and non-recursive encoders**[Poulin-Tillich-Ollivier-09]** :
  - $\Rightarrow$ 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.

The work presented here : exploring the option catastrophic and recursive encoder.