Quantum Serial Turbo-codes

David Poulin
Center for the Physics of Information
California Institute of Technology
Pasadena, CA 91125, USA
Email: dpoulin@ist.caltech.edu

Jean-Pierre Tillich
INRIA, Equipe SECRET
Domaine de Voluceau BP 105
F-78153 Le Chesnay cedex, France
Email: jean-pierre.tillich@inria.fr

Harold Ollivier
Perimeter Institute for Theoretical Physics
Waterloo, ON, N2J 2W9, Canada
Email: harold.ollivier@industrie.gouv.fr

Abstract— **We present a theory of quantum serial turbo-codes and study their performance numerically on a depolarization channel. These codes can be considered as a generalization of classical serial turbo-codes. As their classical cousins, they can be iteratively decoded and with well chosen constituent convolutional codes, we observe an important reduction of the word error rate as the number of encoded qubits increases.**

Our construction offers several advantages over quantum LDPC codes. First, the Tanner graph used for decoding can be chosen to be free of 4-cycles that deteriorate the performances of iterative decoding. Secondly, the iterative decoder makes explicit use of the code's degeneracy. Finally, there is complete freedom in the code design in terms of length, rate, memory size, and interleaver choice.

We address two issues related to the encoding of convolutional codes that are directly relevant for turbo-codes, namely the character of being recursive and non-catastrophic. We define a quantum analogue of a state diagram that provides an efficient way to verify these properties on a given quantum convolutional encoder. Unfortunately, we also prove that all recursive quantum convolutional encoder have catastrophic error propagation. In our constructions, the convolutional codes have thus been chosen to be non-catastrophic and non-recursive. While the resulting families of turbo-codes have bounded minimum distance, from a pragmatic point of view the effective minimum distances of the codes that we have simulated are large enough for not degrading iterative decoding performance up to reasonable word error rates and block sizes.

I. Introduction

Turbo-codes [1], LDPC codes [8] and their variants are one of the most satisfying answer to the problem of devising codes promised by Shannon's theorem. They display outstanding performances for a large class of error models with a decoding algorithm of reasonable complexity. Generalizing these codes to the quantum setting seems a promising way to efficiently approach the quantum capacity, and quantum generalizations of LDPC codes have indeed been proposed in [14]. However all these attempts to obtain such quantum analogues [3], [11], [13], [11] have not yielded results as spectacular as their classical counterpart.

This is due to several reasons. First there are issues with the code design. Due to the orthogonality constraints imposed on the parity-check matrix, it is much harder to construct quantum LDPC codes than classical ones. In particular, constructing the code at random will certainly not do. In fact, it is still unknown whether there exist families of quantum LDPC codes with non-vanishing rate and unbounded minimum distance and all known constructions seem to suffer from a poor minimum distance for reasons which are not always fully understood. Second, there are issues with the decoder. The Tanner graph associated to a quantum LDPC code necessarily contains many 4-cycles which are well known for their negative effect on the performances of iterative decoding. Moreover, quantum LDPC codes are by definition highly degenerate but their decoder does not exploit this property, rather it is impaired by it [18].

On the other hand, generalizing turbo-codes to the quantum setting first requires a quantum analogue of convolutional codes. These have been introduced in [6], [15], [16] and followed by further investigations [7], [10]. Quantum turbo-codes can be obtained from the interleaved serial concatenation of convolutional codes. This idea was first introduced in [17]. There, it was shown that, on memoryless Pauli channels, quantum turbo-codes can be decoded similarly to classical serial turbo-codes. One of the motivation behind this work was to overcome some of the problems faced by quantum LDPC codes. For instance, graphical representations of serial quantum turbo-codes do not necessarily contain 4-cycles. Moreover, there is complete freedom in the code parameters. Both of these points are related to the fact that there are basically no restrictions on the choice of the interleaver used in the concatenation. Another advantage over LDPC codes is that the decoder makes explicit use of the coset structure associated to degenerate errors.

Despite these features, the iterative decoding performance of the turbo-code considered in [17] was quite poor, much poorer in fact that results obtained from quantum LDPC codes. The purpose of the present article is to suggest much better turbo-codes than the one proposed there, and, most importantly, to address the issue of catastrophic error propagation for recursive quantum convolutional encoders. Non-catastrophic and recursive convolutional encoders are responsible for the great success of parallel and serial classical turbo-codes. In a serial concatenation scheme, an inner convolutional code that is recursive yields turbo-code families with unbounded minimum distance [12], while non-catastrophic error propagation is necessary for iterative decoding convergence. The last point can be circumvented in several ways (by doping for instance, see [2]) and some of these tricks can be adapted to the quantum setting, but are beyond the scope of this paper.

The proof [12] that serial turbo-codes have unbounded minimal-distance carries almost verbatim to the quantum setting. Thus, it is possible to design quantum turbo-codes with polynomially large minimal distances. However, we will demonstrate that all recursive quantum convolutional encoders have catastrophic error propagation. This phenomenon is related to the orthogonality constraints which appear in the quantum setting and to the fact that quantum codes are in a sense coset codes. As a consequence, such encoders are not suitable for (standard) serial turbo-code schemes.

In our constructions, the convolutional codes are therefore chosen to be non-catastrophic and non-recursive. The resulting families of turbo-codes have bounded minimum distance. Despite these limitations, from a pragmatic point of view, the minimum distances of the codes that we have simulated are large enough not to degrade the iterative decoding performance up to moderate word error rates ($10^{-3}-10^{-5}$) and block sizes (10^2-10^4).

II. Stabilizer codes

Like the vast majority of quantum codes, quantum turbo-codes are stabilizer codes [4], [9]. However, we will not restrict them to the CSS family [5], [20]. Due to their particular nature, we find it appropriate to define these codes in terms of their encoding matrix rather than their stabilizer group. Although somehow uncommon, this approach is completely equivalent to the usual stabilizer-based description. In this section, we briefly recall some basic facts about stabilizer codes, putting emphasis on the encoder. More details about this can be found in [19].

A quantum error correcting code protecting a system of k qubits by embedding it in a larger system of n qubits is a 2^k dimensional subspace $\mathscr{C}$ of $\mathbb{C}^{2^n}$. We say that it is a quantum code of length n and rate $\frac{k}{n}$. An encoding for a quantum code $\mathscr{C}$ is in general a unitary transformation $\mathcal{V}:\mathbb{C}^{2^n}\rightarrow\mathbb{C}^{2^n}$ such that:

$$\mathscr{C}=\left\{|\overline{\psi}\rangle=\mathcal{V}(|\psi\rangle\otimes|0_{n-k}\rangle)\mid|\psi\rangle\in\mathbb{C}^{2^k}\right\}. \qquad (1)$$

Stabilizer codes arise by choosing $\mathcal{V}$ from a subgroup of the unitary group over $\mathbb{C}^{2^n}$ called the Clifford group.

Recall that the Pauli group is defined with the help of the three Pauli matrices

$$\mathcal{X}=\begin{pmatrix}0&1\\1&0\end{pmatrix},\ \mathcal{Y}=\begin{pmatrix}0&-i\\i&0\end{pmatrix},\ \mathcal{Z}=\begin{pmatrix}1&0\\0&-1\end{pmatrix}.$$

These matrices anti-commute with each other. The Pauli group $\mathscr{G}_n$ over n qubits is obtained by

$$\mathscr{G}_n \quad = \quad \{\epsilon\mathcal{P}_1\otimes\cdots\otimes\mathcal{P}_n|\epsilon\in\{\pm1,\pm i\},\mathcal{P}_i\in\{\mathcal{I},\mathcal{X},\mathcal{Y},\mathcal{Z}\}\},$$

where $\mathcal{I}$ denotes the 2×2 identity matrix. The n-qubit Clifford group is the subgroup of the unitary group on $\mathbb{C}^{2^n}$ that leaves the Pauli group over n qubits globally invariant by conjugation.

In quantum mechanics two states are physically indistinguishable if they differ by a multiplicative constant. This motivates the definition of another group, called the effective Pauli group G_n, obtained by taking the quotient of $\mathscr{G}_n$ by $\{\pm\mathcal{I},\pm i\mathcal{I}\}$. This group is Abelian and is isomorphic to $\mathbb{F}_2^{2n}$. It will be convenient to bring in the following homorphism from $\mathscr{G}_n$ to $\mathbb{F}_2^{2n}$.

Notation 1: Let ϕ be the homorphism from $\mathscr{G}_n$ to $\mathbb{F}_2^{2n}$ consisting in associating to a Pauli group element $\epsilon\mathcal{P}_1\otimes\cdots\otimes\mathcal{P}_n$ the $2n$ bit string $\psi(\mathcal{P}_1):\cdots:\psi(\mathcal{P}_n)$ with $\psi(\mathcal{I})=00,\psi(\mathcal{X})=10,\psi(\mathcal{Z})=01,\psi(\mathcal{Y})=11$.

We use here the notation

Notation 2: For an n-tuple $a\in\mathscr{A}^n$ and an m-tuple $b\in\mathscr{A}^m$ over some alphabet $\mathscr{A}$, we denote by $a:b$ the $n+m$-tuple formed by the concatenation of a followed by b.

The commutation relations on $\mathscr{G}_n$ are encoded in G_n by symplectic product $\star:G_n\times G_n\rightarrow\mathbb{F}_2$ between elements of the effective Pauli group, that is defined by its action on $\mathbb{F}_2^{2n}$ by $P\star Q=P\Lambda_nQ^T$, where $\Lambda_n\triangleq\mathbb{1}_n\otimes\mathcal{X}$. An n-qubit symplectic transformation V is a $2n\times2n$ matrix on $\mathbb{F}_2$ which preserves the symplectic product, i.e. $V\Lambda_nV^T=\Lambda_n$.

The adjoint action of the Clifford group on the Pauli group induces a linear action on $\mathbb{F}_2^{2n}$. This action is specified by a symplectic matrix V over $\mathbb{F}_2$ of size $2n$ which satisfies $\phi(\mathcal{P})V=\phi(\mathcal{V}\mathcal{P}\mathcal{V}^\dagger)$ for any Pauli group element $\mathcal{P}$. The matrix V over $\mathbb{F}_2^{2n}$ associated to a Clifford encoding $\mathcal{V}$ of a code $\mathscr{C}$ (c.f. Eq. (1)) is called the *encoding matrix over* $\mathbb{F}_2$. Note that any symplectic matrix V is the encoding matrix associated to a Clifford transformation $\mathcal{V}$ defining a code $\mathscr{C}$ via Eq. (1). It is readily verified that the rows of V, denoted by V_i $i=1,2,\ldots,2n$, are given by $V_{2i-1}=\phi(\mathcal{V}\mathcal{X}_i\mathcal{V}^\dagger)$, $V_{2i}=\phi(\mathcal{V}\mathcal{Z}_i\mathcal{V}^\dagger)$, where

$$\mathcal{X}_i\triangleq\overbrace{\mathcal{I}\otimes\cdots\otimes\mathcal{I}}^{i-1\text{ times}}\otimes\mathcal{X}\otimes\overbrace{\mathcal{I}\otimes\cdots\otimes\mathcal{I}}^{n-i\text{ times}},$$
$$\mathcal{Z}_i\triangleq\overbrace{\mathcal{I}\otimes\cdots\otimes\mathcal{I}}^{i-1\text{ times}}\otimes\mathcal{Z}\otimes\overbrace{\mathcal{I}\otimes\cdots\otimes\mathcal{I}}^{n-i\text{ times}}.$$

Note that any state in $\mathscr{C}$ is invariant by $\mathcal{V}\mathcal{Z}_i\mathcal{V}^\dagger$ for $i>k$ and that these Pauli operators commute and define an Abelian group of size 2^{n-k}. Conversely, it can be checked that a stabilizer code of length n and rate $\frac{k}{n}$ is equivalently defined by a set of $n-k$ independent generators of order 2 of an Abelian subgroup of the Pauli group which leave the code space pointwise fixed. Applying ϕ to such generators yields an analogue of the parity-check matrix of a linear code. More formally

Fact 1: A quantum parity-check matrix H is any matrix over $\mathbb{F}_2$ whose rows are linearly independent and orthogonal with respect to the symplectic inner product.

For a given stabilizer code $\mathscr{C}$, it can be checked that there is a unique subset $\mathscr{S}$ of the indices of therows of the encoding matrix V that form its parity-check matrix : they are given by $\{2k+2,2k+4,\ldots,2n\}$ (this follows from the previous remark about the action of the $\mathcal{V}\mathcal{Z}_i\mathcal{V}^\dagger$'s). We call the elements of $\mathscr{S}$ the *stabilizer positions* of the encoder. In general, these positions are derived from the qubit positions corresponding to the $|0_{n-k}\rangle$ state used for encoding. For reasons that will become apparent later, we refer to $\mathscr{T}=\{2k+1,2k+3,\ldots,2n-1\}$ as the *syndrome positions* and finally $\mathscr{L}=\{1,2,3,\ldots2k\}$ as the *logical positions* of the encoder.

Although they can correct more general type of errors, stabilizer codes are tailored to correct a discrete error model which consists only of Pauli errors. This includes for example the important depolarizing channel, which is a generalization of the binary symmetric channel.

Definition 1 (Depolarizing channel): The depolarizing channel on n qubits of error probability p picks up an element $E \in G_n$ where the coordinates E_i of E are chosen independently of each other and $\mathbf{P}(E_i = 00) = 1-p$,$\mathbf{P}(E_i = 01) = \mathbf{P}(E_i = 10) = \mathbf{P}(E_i = 11) = \frac{p}{3}$.

There is a quantum measurement associated to any parity-check matrix for the stabilizer code which reveals information about the error that has affected the quantum system. Its outcome is an element of $\mathbb{F}_2^{n-k}$ defined by

Definition 2 (error syndrome): The error syndrome associated to an error $E \in G_n$ with respect to a parity-check matrix H with rows $H_1, \dots, H_{n-k}$ is the binary vector

$$s(E) \triangleq (E \star H_i)_{1 \leq i \leq n-k}.$$

The normalizer code is then defined as

Definition 3 (normalizer code): The group C of elements of zero syndrome is the normalizer code. Elements of C are called codewords.

To summarize these definitions, write for any $P \in G_n$ $Q \triangleq PV^{-1}$ and for $\mathscr{A} \subset \{1, 2, \dots 2n\}$ let $Q_{\mathscr{A}}$ denote the substring of Q. Let us call $Q_{\mathscr{L}}$ the *logical component* of P. The logical component plays a role analogous to the information sequence of a codeword in the classical setting. It can be verified that:
(i) P is a codeword if and only if $Q_{\mathscr{T}} = 0_{n-k}$,
(ii) the syndrome $s(P)$ is given by $Q_{\mathscr{T}}$,
(ii) elements of the stabilizer group are codewords with all zero logical component, i.e. they have $Q_{\mathscr{T}} = 0_{n-k}$ and $Q_{\mathscr{L}} = 0_k$.

The fact that all states in the code $\mathscr{C}$ are invariant by the stabilizer group G itself (generated by the rows of $H = V_{\mathscr{S}}$), has important consequences that distinguish quantum codes from classical codes beyond the stringent orthogonality constraint imposed on their parity-check matrix. The decoding problem in the quantum setting for a stabilizer code does not consist of finding the most likely error satisfying the measured syndrome, but consists instead of finding the *most likely coset* of the stabilizer group:

Definition 4 (Maximum-likelihood decoding): Maximum likelihood decoding of a stabilizer code of length n, rate $\frac{k}{n}$ with stabilizer group G consists in finding for a given syndrome $\sigma \in \mathbb{F}_2^{n-k}$ and an error model on G_n specified by a probability distribution $\mathbf{P}$, the coset $E + G$ such that $s(E) = \sigma$ which maximizes $\mathbf{P}(E+G) = \sum_{F \in G} \mathbf{P}(E+F)$.

For a classical linear code the minimum distance of the code is equal to the minimum weight of a nonzero error of zero syndrome. The minimum distance of stabilizer codes is defined by

Definition 5 (minimum distance): The minimum distance of a stabilizer code is the minimum weight of an error in G_n with zero syndrome which does not belong to the stabilizer group.

We use here the following definition for the weight

Definition 6 (weight): The weight of an element of G_n is the number of locations where it differs from the identity, where we view now an element in G_n as an n-tuple of elements in $\{\mathcal{I}, \mathcal{X}, \mathcal{Y}; \mathcal{Z}\}$.

A stabilizer code of minimum distance d can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors by choosing the error of minimum weight satisfying the syndrome. Stabilizer codes for which the stabilizer group contains elements of weight smaller than the minimum weight are said to be *degenerate*. This is typically the case for quantum LDPC codes which are defined to be stabilizer codes which admit a sparse parity-check matrix. Quantum turbo-codes also have some sparse stabilizers, and so will typically be degenerate.

III. Quantum turbo-codes

In this section, we describe quantum turbo-codes obtained from interleaved serial concatenation of quantum convolutional codes. This first requires the definition of quantum convolutional codes. We will define them through their encoding matrix rather than through their parity-check matrix as in [7], [10]: this allows to define in a natural way the state diagram and is also quite helpful for describing the decoding algorithm [19].

A. Quantum convolutional codes

Formally, we define a quantum convolutional code as follows.

Definition 7 (Quantum convolutional encoder): Let n, k, m, and t be integers defining the parameters of the code, and N the duration of the encoding. Let U be an $(n+m)$-qubit symplectic matrix called the seed transformation. The encoding matrix V of the quantum convolutional encoder is a symplectic matrix over $m + n(N+t)$ qubits given by

$$V \quad = \quad \prod_{i=1}^{N+t} U_{[(i-1)n+1..in+m]}$$

where $[a..b]$ stands for the integer interval $\{a, a+1, \dots, b\}$ and where $U_{[(i-1)n+1..in+m]}$ acts on an element $(P_1, \dots, P_{m+n(N+t)}) \in G_{m+n(N+t)}$ such that its image $(P'_1, \dots, P'_{m+n(N+t)})$ satisfies: $(P'_{(i-1)n+1}, \dots, P'_{in+m}) = (P_{(i-1)n+1}, \dots, P_{in+m})U$ and all other P_i are given by $P'_i = P_i$. The logical, syndrome, and stabilizer positions are respectively given by $\mathscr{L} = \{(i-1)2n + j | i = [1..N], j = [1..2k]\}$, $\mathscr{T} = \{(i-1)2n + 2k + 2j - 1 | i = [1..N], j = [1..n-k]\} \cup \{2k + i | i \in [1..m]\} \cup \{2m + 2Nn + 2j - 1 | j \in [1..nt]\}$, and $\mathscr{S} = \{i + 1 | i \in \mathscr{T}\}$.

We will now define some properties of convolutional codes that will play important roles in the analysis of the performance of turbo codes. Most of these definitions rely on the the state diagram of a convolutional code, which is defined similarly as in the classical case.

Definition 8 (State diagram): The state diagram of an encoder with seed transformation U and parameters (n, k, m) is a directed multigraph with 4^m vertices called *memory-states*, each labeled by an $M \in G_m$. Two vertices M and M' are linked by an edge $M \to M'$ with label (L, P) if and only if there exists $L \in \mathbb{F}_2^{2k}$, $P \in \mathbb{F}_2^{2n}$ and an $S \in \{00, 01\}^{n-k}$ such that

$$P : M' = (M : L : S)U. \qquad (2)$$

The labels L and P are referred to as the logical label and physical label of the edge respectively.

The state diagram is a very handy tool for analyzing the properties of the convolutional encoder, and also for defining some of its essential features, such as being recursive and non catastrophic. For instance, similarly to the classical case

Definition 9 (Non-catastrophic encoder): An encoder is *non-catastrophic* if and only if the only cycles in its state diagram with zero physical label have zero logical label.

We note that this definition is slightly weaker to the one introduced in [15] which required that for the infinite convolutional encoder, there is no error affection a finite number of qubits that propagate under V^{-1} to an infinite number of qubits. Nonetheless, the current definition is a natural generalization of the classical one and is sufficient to ensure good iterative decoding performances.

Again as in the classical case, a convolutional encoder is recursive if and only if for the infinite convolutional encoder no codeword with logical weight 1 has finite support. The logical weight of a Pauli group element refers here to the weight of its logical component. The difference between the quantum setting and the classical setting is the fact that in the classical case there is only one codeword corresponding to a given logical (*i.e.* information) input, whereas there is a whole coset in the quantum case. This reflects in the fact that there are infinitely many paths in the state diagram which have the same logical labels. This definition of being recursive can be verified with the state diagram by bringing in the following definition.

Definition 10 (Admissible path): A path in the state diagram is *admissible* if and only if its first edge is not part of a zero physical-weight cycle.

The previous definition is then equivalent to

Definition 11 (Recursive encoder): A recursive encoder is such that any admissible path with logical weight 1 starting from a vertex belonging to a zero-physical weight loop does not contain a zero-physical weight loop.

B. Interleaved serial concatenation

Quantum turbo-codes are obtained from a particular form of interleaved concatenation of quantum convolutional codes. Interleaving is slightly more complex in the quantum setting since in addition to permuting the qubits it is also possible to perform a Clifford transformation on each qubit which amounts to permute the three Pauli matrices. More precisely:

Definition 12 (Quantum interleaver): A *quantum interleaver* Π of size N is an N-qubit symplectic transformation which acts as follows on G_N :

$$(P_1, \ldots, P_N) \mapsto (R_1(P_{\pi(1)}), \ldots, R_N(P_{\pi(N)}))$$

where π is a fixed permutation of $\{1, \ldots, N\}$ and $R_1, \ldots, R_N$ act on G_1 by fixing 00 and permuting $01, 10$, and 11.

An interleaved serial concatenation of two quantum encoders has three basic components:

1) An *outer code* encoding k^{Out} qubits by embedding them in a register of n^{Out} qubits, with encoding matrix V^{Out},
2) An *inner code* encoding k^{In} qubits by embedding them in a register of n^{In} qubits, with encoding matrix V^{Out} and which is such that $k^{\text{In}} = n^{\text{Out}}$,
3) A *quantum interleaver* Π of size $N = n^{\text{Out}} = k^{\text{In}}$.

The resulting *encoding matrix of the interleaved concatenated code* is a symplectic matrix V acting on $G_{n^{\text{In}}}$ such that

$$V = V'^{\text{Out}} \Pi' V^{\text{In}},$$

with the action of V'^{Out} and Π' on $G_{n^{\text{In}}}$ being defined by

$$(L : S^{\text{Out}} : S^{\text{In}})V'^{\text{Out}} = ((L : S^{\text{Out}})V^{\text{Out}} : S^{\text{In}}) \qquad (3)$$

for $(L : S^{\text{Out}} : S^{\text{In}}) \in G_{k^{\text{Out}}} \times G_{n^{\text{Out}}-k^{\text{Out}}} \times G_{n^{\text{In}}-k^{\text{In}}}$, and

$$(L' : S^{\text{In}})\Pi' = (L'\Pi : S^{\text{In}}) \qquad (4)$$

for $L' \in G_{n^{\text{Out}}}$. The rate of the concatenated code is equal to $\frac{k^{\text{Out}}}{n^{\text{In}}} = \frac{k^{\text{Out}}}{n^{\text{Out}}} \frac{k^{\text{In}}}{n^{\text{In}}}$, that is the product of the rates of the inner code and the outer code.

A serial quantum turbo-code is obtained from this interleaved concatenation scheme by choosing V^{Out} and V^{In} as quantum convolutional encoders.

C. Recursive convolutional encoders are catastrophic

In the classical setting, non-catastrophic and recursive convolutional encoders are of particular interest. When used as the inner encoders of a concatenated coding scheme, the resulting codes have a minimal distance that grows polynomially with their length and offer good iterative decoding performances. More precisely, random serial turbo-codes have a minimum distance which is typically of order $N^{\frac{d_*^{\text{Out}}-2}{d_*^{\text{Out}}}}$ when the inner encoder is recursive, where N is the length of the concatenated code and d_*^{Out} the free distance of the outer code [12]. That the encoder be non-catastrophic is important to obtain good iterative decoding performances.

This result and its proof would carry over the quantum setting almost verbatim with our definition of recursive encoders. The quantum case is slightly more subtle due to the coset structure of the code. Unfortunately, such encoders do not exist:

Theorem 1: Quantum convolutional recursive encoders are catastrophic.

This result is perhaps surprising since the notions of catastrophic and recursive are quite distinct in the classical setting. Nonetheless, the stringent symplectic constraints imposed to the seed transformation U gives rises to a conflicting relation between them. The proof of Theorem 1 is too long to be included here and can be found in [19].

IV. Results

The convolutional codes we used for our construction of turbo-codes are for the most part generated at random. That is, we first generate a random seed transformation U of desired dimensions. Using its state diagram, we then test whether the corresponding encoder is catastrophic, and if so we reject it and start over. Non-catastrophicity is the only criterion that we systematically imposed.

As a first sieve among the randomly generated non-catastrophic seed transformations, we can study their distance spectrums and make some heuristic test based on it. An example of a good seed transformation obtained from this procedure is $U_{(2,1,4)} = \{610, 3323, 760, 1591, 2500, 942, 2290, 794, 1535, 2202, 2859, 809\}$ where the binary symplectic encoding matrix is specified by its list of rows and each row is given by the integer corresponding to the binary entry. The subscripts on the encoder specify its parameters (n, k, m). Let us denote by d_1 the minimum weight of a codeword of the infinite convolutional code of logical weight 1 and d_* the same minimum weight but without any constraint on the logical weight. For our code $d_1 = 8$ and $d_* = 6$. It can easily be seen that the minimum distance of a turbo-code obtained from the concatenation of two convolutional codes is no greater than $d_*^{\mathrm{Out}} d_1^{\mathrm{In}}$. Therefore the codes obtained from the concatenation of $U_{(2,1,4)}$ with itself have minimum distance at most $8 \times 6 = 48$.

The serial turbo-codes that we have presented here can be decoded similarly to classical serial turbo-codes. The decoding algorithm is presented in detail in [19]. We have performed numerical simulations of these codes on the depolarizing channel for different lengths and for randomly chosen interleavers. The WERs as a function of the depolarizing probability p is shown on Fig.1. Perhaps the most striking features of those curves is the existence of a pseudo-threshold value of p below which the WER *decreases* as the number of encoded qubits is increased. Since the codes have a bounded minimal distance, this is not a true threshold in the sense that as we keep increasing the number of encoded qubits, the WER should start to increase. However, we see that for modest sizes N_L of up to 1000, this effect is not observed. These values should be compared with the hashing bound, whose value is approximately 0.12689 for rate $\frac{1}{4}$. We can also compare with the results obtained from LDPC codes in [14, Figure 10] by evaluating the depolarizing probability p at which the WER drops below 10^{-4}. For a rate $\frac{1}{4}$, this threshold was achieved at $p_{th} \approx 0.033$ (note the convention $f_m = \frac{2}{3}p$) for LDPC codes while the turbo-code shown at Fig. 1 has $p_{th} \approx 0.048$. It should also be noted that this improved threshold is achieved with a smaller block size than that used for the LDPC in [14]; a larger block should further improve this result.

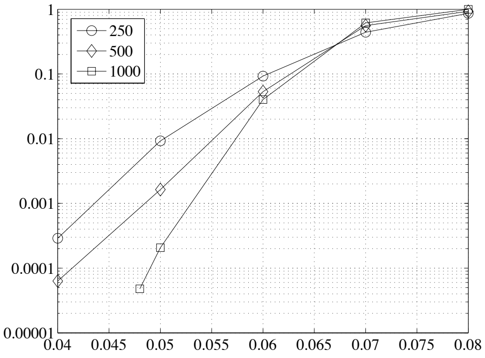

Fig. 1. WER *vs* depolarizing probability p for the quantum turbo-code obtained from the concatenation of the convolutional code with seed transformation $U_{(2,1,4)}$ with itself, for different number of encoded qubits N_L. Each constituent convolutional code has $m = 4$ qubits of memory and has rate $\frac{1}{2}$, so the rate of the turbo code is $\frac{1}{4}$.

References

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding," in *ICC'93*, Genève, Switzerland, May 1993, pp. 1064–1070.

[2] S. ten Brink, "Designing iterative decoding schemes with the extrinsic information transfer chart," *AEU Int. J. Electron. Commun.*, vol. 54, no. 6, p. 389, 2000.

[3] T. Camara, H. Ollivier, and J.-P. Tillich, "A class of quantum LDPC codes: construction and performances under iterative decoding," in *Proceedings of ISIT 2007*. Nice: IEEE, June 2007, pp. 811–815.

[4] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, pp. 405–408, 1997.

[5] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, 1996.

[6] H. F. Chau, "Quantum convolutional correcting codes," *Phys. Rev. A*, vol. 58, pp. 905–909, 1998.

[7] J. G. D. Forney, M. Grassl, and S. Guha, "Convolutional and tail-biting quantum error-correcting codes," *IEEE Transactions on Information Theory*, vol. 53, no. 3, pp. 865–880, 2007.

[8] R. G. Gallager, *Low Density Parity Check Codes*. Cambridge, Massachusetts: M.I.T. Press, 1963.

[9] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Institute of Technology, Pasadena, CA, 1997.

[10] M. Grassl and M. Rötteler, "Non-catastrophic encoders and encoder inverses for quantum convolutional codes," in *Proceedings of ISIT 2006*. IEEE, July 2006, pp. 1109–1113.

[11] M. Hagiwara and H. Imai, "Quantum quasi-cyclic LDPC codes," in *Proceedings of ISIT 2007*. Nice: IEEE, June 2007, pp. 806–811.

[12] N. Kahale and R. Urbanke, "On the minimum distance of parallel and serially concatenated codes," in *Proc. IEEE Int. Symp. Info. Theo. (ISIT'98)*, 1998, p. 31.

[13] H. Lou and J. Garcia-Frias, "On the application of error-correcting codes with low-density generator matrix over different quantum channels," in *Proceedings of Turbo-coding 2006*, Munich, April 2006.

[14] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, "Sparse graph codes for quantum error-correction," *IEEE Trans. Info. Theor.*, vol. 50, no. 10, pp. 2315–2330, 2004.

[15] H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Phys. Rev. Lett.*, vol. 91, no. 17, p. 177902, 2003.

[16] ——, "Quantum convolutional codes: fundamentals," 2004. [Online]. Available: http://arxiv.org/quant-ph/0401134

[17] H. Ollivier and J.-P. Tillich, "Interleaved serial concatenation of quantum convolutional codes: gate implementation and iterative error estimation algorithm," in *Proceedings of the 26th Symposium on Information Theory in the Benelux*, Brussels, Belgium, 2005, p. 149.

[18] D. Poulin and Y. Chung, "On the iterative decoding of sparse quantum codes," 2008. [Online]. Available: http://arxiv.org/0801:1241

[19] D. Poulin, J.-P. Tillich, and H. Ollivier, "Quantum serial turbo-codes," 2007. [Online]. Available: http://arxiv.org/0712.2888

[20] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, p. 793, 1996.