Entanglement boosts quantum turbo codes

Mark M. Wilde
School of Computer Science
McGill University
Montreal, Quebec, Canada H3A 2A7
Email: mwilde@cs.mcgill.ca

Min-Hsiu Hsieh
Statistical Laboratory
University of Cambridge
Cambridge, United Kingdom CB3 0WB
Email: minhsiuh@gmail.com

***Abstract*—One of the unexpected breakdowns in the existing theory of quantum serial turbo coding is that a quantum convolutional encoder cannot simultaneously be recursive and non-catastrophic. These properties are essential for a quantum turbo code to have an unbounded minimum distance and for its iterative decoding algorithm to converge, respectively. Here, we show that the entanglement-assisted paradigm gives a theoretical and simulated "turbo boost" to these codes, in the sense that an entanglement-assisted quantum (EAQ) convolutional encoder can possess both of the aforementioned desirable properties, and simulation results indicate that entanglement-assisted turbo codes can operate reliably in a noise regime 5.5 dB beyond that of standard quantum turbo codes. Entanglement is *the* resource that enables a convolutional encoder to satisfy both properties because an encoder acting on only information qubits, classical bits, gauge qubits, and ancilla qubits cannot simultaneously satisfy them. Simulation results demonstrate that interleaved serial concatenation of EAQ convolutional encoders leads to a powerful code construction with excellent performance on a memoryless depolarizing channel.**

I. Introduction

Classical turbo codes represent one of the great successes of the modern coding era [1], [2]. These near Shannon-limit codes have efficient encodings, they offer astounding performance on memoryless channels, and their iterative decoding algorithm quickly converges to an accurate error estimate. They are probabilistic codes, meaning that they possess sufficient structure to ensure efficient encoding and decoding, yet they have enough randomness to allow for analysis of their performance with the probabilistic method [2].

The theory of quantum turbo codes is much younger than its classical counterpart [3], [4]. Poulin *et al*. set this theory on a firm foundation [4] in an attempt to construct explicit quantum codes that come close to achieving the quantum capacity of a quantum channel [5]. The structure of a quantum serial turbo code is similar to its classical counterpart—one quantum convolutional encoder [6] followed by a quantum interleaver and another quantum convolutional encoder. The encoder "closer to the channel" is the inner encoder, and the one "farther from the channel" is the outer encoder.

Despite Poulin *et al*.'s success in providing a solid theoretical construction, this theory had an unexpected breakdown. They found that quantum convolutional encoders cannot be simultaneously non-catastrophic and recursive, two desirable properties that can hold simultaneously for classical convolutional encoders and are the reason underpinning the high performance of classical turbo codes [2]. These two respective properties ensure that an iterative decoder performs well in estimating errors and that the turbo code has an unbounded minimum distance growing almost linearly with the length of the code [7], [8]. Quantum convolutional encoders cannot have these properties simultaneously, essentially because stabilizer operators must satisfy stringent commutativity constraints in order to form a valid quantum code (see Theorem 1 of Ref. [4]). Thus, the existing quantum turbo codes with non-catastrophic constituent quantum convolutional encoders do not have unbounded minimum distance, but Poulin *et al*. conducted numerical simulations and showed that performance of their quantum turbo codes appears to be good in practice.

The breakdown in the quantum turbo coding theory has led researchers to ponder if some modification of the quantum turbo code construction could have unbounded minimum distance with the iterative decoding algorithm converging. One possibility is simply to change the paradigm for quantum error correction, by allowing the sender and the receiver access to shared entanglement before communication begins. This paradigm is known as the "entanglement-assisted" setting, and it simplifies the theory of quantum error correction [9].

In this work, we show that entanglement gives a theoretical and practical boost to quantum turbo codes [10]. Specifically, after the review in the next section, Section III gives an example of an EAQ convolutional encoder that can simultaneously be recursive and non-catastrophic. A "quantized" version of the result in Ref. [7] then implies that a quantum serial turbo code employing such an encoder along with another non-catastrophic encoder has an unbounded minimum distance [8], and non-catastrophicity implies that it has good iterative decoding performance. Section IV overviews how an EAQ turbo code operates, and Section V discusses the results of our simulations of EAQ turbo codes. Section VI shows that entanglement is the unique resource that enables EAQ convolutional encoders to be recursive and non-catastrophic—encoders acting on information qubits, ancillas, gauge qubits, and classical bits cannot have both properties. We end the paper with some open questions.

II. EAQ convolutional codes

An EAQ convolutional code is a particular type of EAQ code that has a convolutional structure. We adopt the approach of Poulin *et al*. [4] which in turn heavily borrows from ideas

978-1-4577-0595-3/11/$26.00 ©2011 IEEE

in classical convolutional coding [11]. We begin with a seed transformation and determine its state diagram, which yields important properties of the encoder.

An EAQ convolutional encoder is a "Clifford group" unitary U that acts on m memory qubits, k information qubits, a ancilla qubits, and c halves of ebits to produce a set of m memory qubits and n channel qubits, where $n = k + a + c$. The transformation that it induces on binary representations of Pauli operators [4] acting on these registers is as follows:

$$(M' : P) = (M : L : S : E)U,$$

where M' acts on m output memory qubits, P acts on n output physical qubits, M acts on m input memory qubits, L acts on k information qubits, S acts on a ancilla qubits, and E acts on c halves of ebits (see Ref. [10] for more details). Although the quantum states in these registers can be continuous in nature, the act of syndrome measurement discretizes the errors acting on them, and the above classical representation is useful for analysis of the code's properties and the flow of the logical operators through the encoder.

The overall encoding operation is the transformation induced by repeated application of the above seed transformation to a quantum data stream broken up into periodic blocks of information qubits, ancilla qubits, and halves of ebits while feeding the output memory qubits of one transformation as the input memory qubits of the next (see Figure 6 of Ref. [4] for a visual aid). The advantage of a quantum convolutional encoder is that the complexity of the overall encoding scales only linearly with the length of the code for a fixed memory size, while the decoding complexity scales linearly with the length of the code by employing a local maximum likelihood decoder combined with a belief propagation algorithm [4]. The quantum communication rate of the code is essentially k/n while the entanglement consumption rate is c/n, if the length of the code becomes large compared to n.

1) State Diagram: The state diagram of an EAQ convolutional encoder is the most important tool for analyzing its properties, and it is the formal "quantization" of a classical convolutional encoder's state diagram [11]. It examines the flow of the logical operators through the encoder with a finite-state machine approach, and this representation is important for analyzing both its distance and its performance under the iterative decoding algorithm of Ref. [4]. The *state diagram* is a directed multigraph with 4^m vertices that we think of as memory states. We label each memory state with an m-qubit Pauli operator M. We connect two vertices with a directed edge from $M \to M'$, labeled as (L, P), if there exists a k-qubit Pauli operator L, an n-qubit Pauli operator P, and an a-qubit Pauli operator $S^z \in \{I, Z\}^a$ such that

$$(M' : P) = (M : L : S^z : I_c)U, \tag{1}$$

where I_c is the identity acting on c qubits. We refer to the labels L and P of an edge as the respective logical and physical label.

As an example, consider the transformation depicted in Figure 1. It acts on one memory qubit, one information qubit,

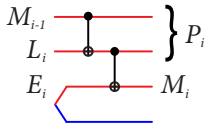

Fig. 1. (Color online) Seed transformation for an $n = 2$, $k = 1$, $c = 1$, $m = 1$ EAQ convolutional code.

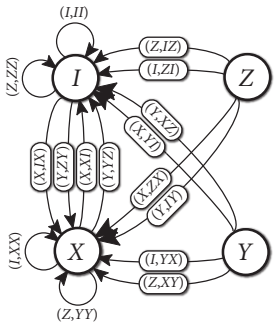

Fig. 2. The state diagram corresponding to the seed transformation in Figure 1. The state diagram allows us to check that the encoder is non-catastrophic and non-recursive.

and one half of an ebit to produce two channel qubits and one memory qubit. Figure 2 illustrates the state diagram corresponding to this transformation. There are four memory states because there is only one memory qubit, and there are 16 edges because there are four memory states and four logical operators for one information qubit and one ebit.

2) Non-catastrophicity: We now recall the definition of non-catastrophicity in Ref. [4], which is the formal "quantization" of the definition in Section IX of Ref. [11]. The definition from Ref. [4] is the same for an EAQ convolutional encoder because it depends on the iterative decoding algorithm used to decode the code, and we can exploit the same iterative decoding algorithm as in Ref. [4] to decode EAQ convolutional codes. A *path* through the state diagram is a sequence $M_1, \ldots, M_t$ of vertices such that $M_i \to M_{i+1}$ is an edge belonging to it. Each logical operator of the code corresponds to a path in the state diagram, with the sequence of vertices in the path being the states of memory traversed while encoding the logical operator. The physical and logical weights of a logical operator are equal to the sums of the corresponding weights of the edges traversed in a path that encodes the logical operator. A *zero physical-weight cycle* is a cycle in the state diagram such that all edges in the cycle have zero physical weight. Finally, an EAQ encoder acting on m memory qubits, k information qubits, a ancilla qubits, and c ebits is *non-catastrophic* if every zero physical-weight cycle in its state diagram has zero logical weight.

Observe that the state diagram in Figure 2 for the EAQ convolutional encoder does not feature a zero physical-weight cycle with non-zero logical weight. Thus, the encoder is non-catastrophic. This is in contrast to the case where the same encoding circuit acts on an ancilla qubit instead of half of

an ebit—in this case, the encoder is catastrophic [4]. This difference illustrates another intriguing departure from the classical theory of convolutional coding. *Non-catastrophicity in the quantum world is not only a property of the encoder, but it also depends on the resources available for encoding.*

3) Recursiveness: Recursiveness is another desirable property for an EAQ convolutional encoder when it is employed as the inner encoder of a quantum serial turbo code. This property ensures that a quantum serial turbo code on average has a distance growing near-linearly with the length of the code, and the proof of this statement [12], [8] is similar to the classical proof [7]. In short, an EAQ convolutional encoder is *quasi-recursive* if it transforms every weight-one Pauli operator X_i, Y_i, or Z_i to an infinite-weight Pauli operator [4]. It is *recursive* if, in addition to being quasi-recursive, every element in the logical cosets $C(X_i)$, $C(Y_i)$, and $C(Z_i)$ has infinite weight. This stringent requirement is necessary due to the coset structure of EAQ codes. One might think that quasi-recursiveness is sufficient for good performance, but our simulation results in Section V indicate that recursiveness is indeed necessary because a turbo code has a significant boost in performance if its inner encoder is recursive.

It seems like it would be demanding to determine if this condition holds for every possible input, but we can exploit the state diagram to check it. The algorithm for checking recursiveness is as follows. First, we define an *admissable path* to be a path in which its first edge is not part of a zero physical-weight cycle [4]. Now, consider any vertex belonging to a zero-physical weight loop and any admissable path beginning at this vertex with logical weight one. The encoder is *recursive* if all such paths do not contain a zero physical-weight loop [4]. The idea is that a weight-one logical operator is not enough to drive a recursive encoder to a memory state that is part of a zero-physical weight loop—the minimum weight of a logical operator that does so is two.

The example encoder in Figure 1 is not recursive. The only vertex in the state diagram in Figure 2 belonging to a zero physical-weight cycle is the vertex labeled I. If the logical input to the encoder is a Z operator followed by an infinite sequence of identity operators, the circuit outputs ZZ as the physical output, returns to the memory state I, and then outputs the identity for the rest of time. Thus, the response to this weight-one input is finite, and the circuit is non-recursive. Although this example is non-recursive, Section III details an example of an EAQ convolutional encoder that is both recursive and non-catastrophic (Ref. [10] has many other examples).

4) Distance Spectrum: We end this section by reviewing the performance measures from Ref. [4], which are also quantizations of the classical measures [11]. The *distance spectrum* $F(w)$ of an EAQ convolutional encoder is the number of admissable paths beginning and ending in memory states that are part of a zero physical-weight cycle, where the physical weight of each admissable path is w and the logical weight is greater than zero. The distance spectrum incorporates the translational invariance of a quantum convolutional code and gives an indication of its performance on a memoryless depolarizing channel. The *free distance* of an EAQ convolutional encoder is the smallest weight w for which $F(w) > 0$, and this parameter is one indicator of the performance of a quantum serial turbo code employing constituent convolutional encoders. Although one of the applications of our EAQ convolutional encoders are as the inner encoders in a quantum serial turbo coding scheme, we can also have them as outer encoders in a quantum serial turbo code and use the free distance to show that its minimum distance grows near-linearly when combined with a non-catastrophic, recursive inner encoder.

III. Example Encoder

One of our example EAQ convolutional encoders is the simplest example that is both recursive and non-catastrophic. It exploits one memory qubit and one ebit to encode one information qubit per frame. We discuss this example briefly and verify its non-catastrophicity and recursiveness.

The seed transformation for our example is as follows:

$$\begin{array}{ccc} Z & I & I \\ I & Z & I \\ I & I & Z \\ X & I & I \\ I & X & I \\ I & I & X \end{array} \rightarrow \begin{array}{ccc} Z & I & X \\ X & Z & Y \\ X & Y & Z \\ X & X & X \\ Y & I & Y \\ Y & X & Y \end{array}, \tag{2}$$

where the first input qubit is the memory qubit, the second input qubit is the information qubit, the third is Alice's half of the ebit, the first output qubit is the memory qubit, and the last two outputs are the physical qubits.

The seed transformation in (2) leads to the state diagram of Figure 3, by exploiting (1). We can readily check that the encoder is non-catastrophic and recursive by inspecting Figure 3. The only cycle with zero physical weight is the self-loop at the identity memory state with zero logical weight. The encoder is thus non-catastrophic. To verify recursiveness, note again that the only vertex belonging to a zero physical-weight cycle is the self-loop at the identity memory state. We now consider all weight-one admissable paths that begin in this state. If we input a logical X, we follow the edge (X, IY) to the Y memory state. Inputting the identity operator for the rest of time keeps us in the self-loop at memory state Y while still outputting non-zero physical weight operators. A similar analysis applies for the Y and Z logical operators, and the encoder is thus recursive.

IV. EAQ Turbo Codes

The construction of an EAQ serial turbo code is the same as that in Ref. [4] (see Figure 10 there), with the exception that we assume that Alice and Bob share entanglement in the form of ebits before encoding begins. Alice first encodes her stream of information qubits with the outer encoder, performs a quantum interleaver on all of the qubits, and then encodes the resulting stream with the inner encoder. The quantum communication rate of the resulting EAQ turbo code is $k^{\text{Out}}/n^{\text{In}} = (k^{\text{Out}}/n^{\text{Out}})(k^{\text{In}}/n^{\text{In}})$ where k^{Out} is the number

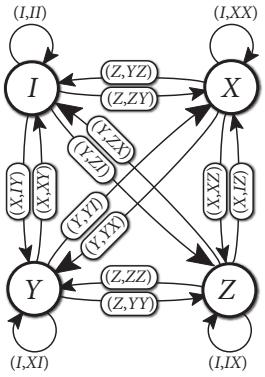

Fig. 3. The state diagram corresponding to the seed transformation in (2).

of information qubits encoded by the outer encoder, n^{Out} is the number of physical qubits output from the outer encoder, and a similar convention holds for k^{In}, n^{In}, and the inner encoder. In order for the qubits to match up properly, n^{Out} must be equal to k^{In}. The entanglement consumption rate of the code is $(c^{\text{Out}} + c^{\text{In}})/n^{\text{In}}$ where c^{Out} and c^{In} are the total number of ebits consumed by the outer and inner encoder, respectively.

V. Simulation Results

Our simulation results indicate that particular constructions of EA turbo codes have excellent performance on a memoryless depolarizing channel. In particular, we found two quantum convolutional encoders that are comparable to the first and third encoders of Poulin *et al*. [4]—they have the same number of memory qubits, information qubits, ancilla qubits, and a comparable distance spectrum. These encoders are non-catastrophic, and they become recursive after replacing all of the ancilla qubits with ebits. Additionally, the encoders with full entanglement assistance have a distance spectrum much improved over the unassisted encoders.

We constructed a quantum serial turbo code with these encoders and conducted four types of simulations: the first with the unassisted encoders, a second with full entanglement assistance, a third with the inner encoder assisted, and a fourth with the outer encoder assisted. Figure 4 plots the results of these simulations. The unassisted quantum turbo codes have performance similar to those of Poulin *et al*. in Ref. [4] (see Figure 4(a)). The encoders with full entanglement assistance have a tremendous boost in performance over the unassisted ones, in the sense that they can operate reliably in a noise regime several dB beyond the unassisted turbo codes (see Figure 4(b)). This boost is due to the improvement in the distance spectrum and is also due to the encoder becoming recursive. Also, these codes come close to achieving the entanglement-assisted hashing bound [13], which is the ultimate limit on their performance. The quantum turbo codes with inner encoder entanglement assistance have performance a few dB below the fully-assisted code (see Figure 4(c)), but one advantage of them is that other simulations indicate that they are more tolerant to noise on the ebits (see Figure 8 of Ref. [10]). The quantum turbo codes with outer encoder entanglement assistance have performance not far beyond that of the unassisted turbo codes (see Figure 4(d)). The hope for this last construction was that assisted outer encoders with an improved distance spectrum combined with unassisted inner encoders satisfying the weaker condition of quasi-recursiveness would be sufficient to have a marked improvement over the unassisted turbo codes, but our simulation results have shown that this intuition does not hold.

VI. Other Constructions

Poulin *et al*. suggest that subsystem convolutional codes might be "a concrete avenue" for circumventing the inability of a quantum convolutional encoder to be simultaneously recursive and non-catastrophic [4]. Such codes exploit a resource known as a "gauge" qubit that can add extra degeneracy beyond that available in a standard stabilizer code. Another variation is an encoder that encodes both classical bits and qubits, and we might wonder if these could be simultaneously recursive and non-catastrophic. Unfortunately, encoders that act on logical qubits, classical bits, ancilla qubits, and gauge qubits cannot possess both properties simultaneously, and this result follows as a corollary of Theorem 1 in Ref. [4]. This result implies that entanglement is *the* resource enabling a convolutional encoder to be both recursive and non-catastrophic (there are no other known local resources for quantum codes besides ancilla qubits, classical bits, and gauge qubits). The proof of this corollary follows by constructing the state diagram for a recursive encoder acting on memory qubits, information qubits, ancillas, classical bits, and gauge qubits and showing that it must be catastrophic [10].

VII. Conclusion

There are many questions to ask going forward from here. It would be interesting to explore the performance of the other suggested code structures in Ref. [10] to determine if they could come close to achieving the optimal rates from quantum Shannon theory [14]. For example, what is the best arrangement for a classically-enhanced EAQ code? Should we place classical bits in the inner or outer encoder? Are there better ways to use entanglement so that we increase error-correcting ability while reducing entanglement consumption?

We acknowledge T. Brun, H. Carteret, J. Florjanczyk, P. Hayden, D. Poulin, and J.-P. Tillich for useful discussions. M. M. Wilde acknowledges the MDEIE (Québec) PSR-SIIRI international collaboration grant. M.-H. Hsieh acknowledges the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement number 213681.

References

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," in *IEEE Int. Conf. Comm.*, vol. 2, Geneva, Switzerland, May 1993, pp. 1064–1070.

[2] S. Benedetto and G. Montorsi, "Unveiling turbo codes: Some results on parallel concatenated coding schemes," *IEEE Transactions on Information Theory*, vol. 42, no. 2, pp. 409–428, March 1996.

[3] H. Ollivier and J.-P. Tillich, "Trellises for stabilizer codes: Definition and uses," *Phys. Rev. A*, vol. 74, no. 3, p. 032304, September 2006.

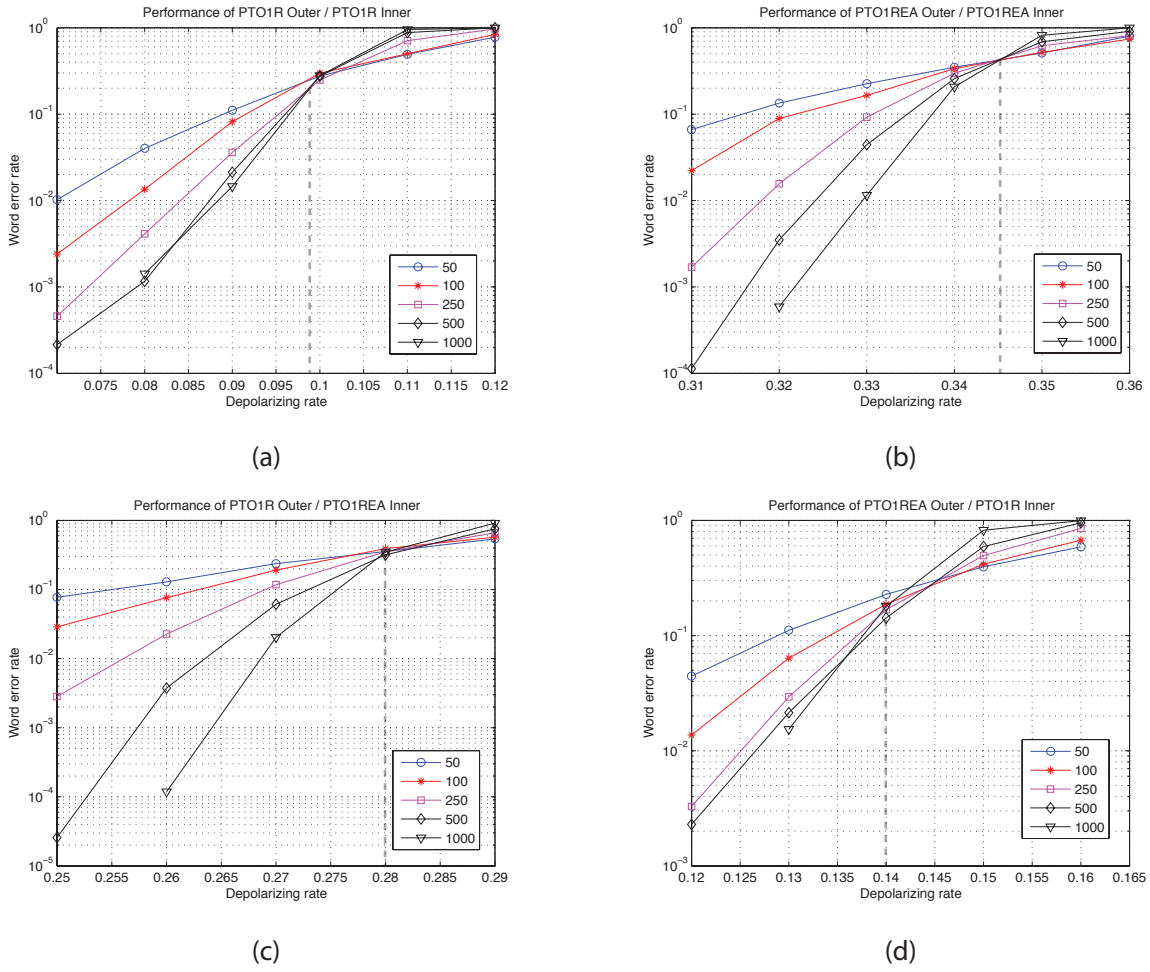

Fig. 4. The figure plots the results of four different simulations that exploit an encoder acting on three memory qubits, one information qubit, and two ancillas or two ebits. Let PTO1R denote the encoder acting on the three memory qubits, the information qubit, and the two ancillas, and let PTO1REA denote the same encoder with the two ancillas replaced by two ebits. Serially concatenated EAQ turbo codes resulting from combinations of PTO1R and PTO1REA have rate 1/9 and varying entanglement consumption rates. Each plot demonstrates the existence of a threshold, where the code performance increases whenever the channel noise rate is below the threshold. The vertical dotted line in each plot indicates the approximate location of the threshold. (a) The pseudothreshold for this simulation occurs at a depolarizing noise rate ≈ 0.098, and this pseudothreshold is within 2.14 dB of the 0.16028 noise limit for a rate $1/9$ code (noise limits come from the hashing bound). (b) The true threshold occurs at ≈ 0.345—it is a true threshold because the code has a provably unbounded minimal distance [8], and the WER should continue to decrease as we increase the number of encoded qubits. This threshold is 5.47 dB beyond the pseudothreshold of the unassisted turbo code, and it is within 1.53 dB of the 0.49088 noise limit from the EA hashing bound. (c) Since the inner encoder is recursive, the EAQ turbo code has an unbounded minimum distance, and the threshold in Figure 4(c) is a true threshold. It occurs approximately at a depolarizing noise rate of 0.28, which is within 0.91 dB of the previous threshold and within 2.44 dB of the 0.49088 noise limit from the EA hashing bound. (d) The pseudothreshold occurs at approximately 0.14, but this value is only a rough estimate because it is not as clearly defined. This pseudothreshold is only 1.55 dB higher than the threshold for the unassisted code, and it is 5.45 dB away from noise limit from the EA hashing bound.

[4] D. Poulin, J.-P. Tillich, and H. Ollivier, "Quantum serial turbo-codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2776–2798, June 2009.

[5] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Theory*, vol. 51, pp. 44–55, Jan. 2005.

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

[7] N. Kahale and R. Urbanke, "On the minimum distance of parallel and serially concatenated codes," in *Proc. Int. Symp. Inf. Theory*, Cambridge, Massachussetts, USA, August 1998, p. 31.

[8] H. Ollivier, D. Poulin, and J.-P. Tillich, "Quantum turbo codes," October 2008, unpublished manuscript.

[9] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, Oct. 2006.

[10] M. M. Wilde and M.-H. Hsieh, "Entanglement boosts quantum turbo codes," October 2010, arXiv:1010.1256.

[11] A. J. Viterbi, "Convolutional codes and their performance in communication systems," *IEEE Transactions on Communication Technology*, vol. 19, no. 5, pp. 751–772, October 1971.

[12] D. Poulin, "Iterative quantum coding schemes: LDPC and turbo codes," Online Presentation, April 2009, slide 92. [Online]. Available: http://www.physique.usherbrooke.ca/~dpoulin/Documents/IDQC09_McGill.pdf

[13] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted classical capacity of noisy quantum channels," *Physical Review Letters*, vol. 83, no. 15, pp. 3081–3084, October 1999.

[14] M.-H. Hsieh and M. M. Wilde, "Entanglement-assisted communication of classical and quantum information," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4682–4704, September 2010, arXiv:0811.4227.