

Entanglement boosts quantum turbo codes

Mark M. Wilde and Min-Hsiu Hsieh

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 practical “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. We give several examples of EAQ convolutional encoders that are both recursive and non-catastrophic and detail their relevant parameters. Finally, 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.

Index Terms—quantum communication, entanglement-assisted quantum turbo code, entanglement-assisted quantum error correction, recursive, non-catastrophic, entanglement-assisted quantum convolutional code

I. INTRODUCTION

Classical turbo codes represent one of the great successes of the modern coding era [1], [2], [3], [4]. 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], [4], [5].

The theory of quantum turbo codes is much younger than its classical counterpart [6], [7], and we still stand to learn more regarding these codes’ performance and structure. Poulin *et al.* set this theory on a firm foundation [7] in an attempt to construct explicit quantum codes that come close to achieving the quantum capacity of a quantum channel [8], [9], [10], [11]. The structure of a quantum serial turbo code is similar to its classical counterpart—one quantum convolutional encoder [12], [13] 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. One of the insights of Poulin *et al.* in Ref. [7] was to “quantize” the classical notion of a state diagram [14], [15]—this diagram helps in analyzing important properties of the constituent quantum convolutional encoders that directly affect the performance of the resulting quantum turbo code.

Despite Poulin *et al.*’s success in providing a solid theoretical construction, the engines of their quantum turbo codes had an unexpected breakdown.¹ 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], [4]. 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 [5], [16], [17]. 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. [7]). 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 [18]. 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 both the theory of quantum error correction [19], [20] and the theory of quantum channels [21], [22]. In entanglement-assisted quantum (EAQ) error correction, it is not necessary for a set of stabilizer operators to satisfy the stringent commutativity constraints that a standard quantum code should satisfy, allowing us to produce EAQ codes from arbitrary classical codes.² In quantum channel theory, the classical and quantum capacities of a quantum channel assisted by entanglement are the only known capacities for which we can claim a complete understanding in the general case—both are formulas involving an optimization of the quantum mutual information with respect to all pure, bipartite entangled inputs to *a single use* of the channel (formally analogous to

¹Please excuse the unavoidable pun!

²This holds for EAQ convolutional codes in addition to EAQ block codes [23], [24].

Mark M. Wilde is a postdoctoral fellow with the School of Computer Science, McGill University, Montreal, Quebec, Canada H3A 2A7. Min-Hsiu Hsieh was with the ERATO-SORST Quantum Computation and Information Project, Japan Science and Technology Agency 5-28-3, Hongo, Bunkyo-ku, Tokyo, Japan and is now a postdoctoral fellow with the Statistical Laboratory, University of Cambridge, Wilberforce Road, Cambridge CB3 0WB, UK. (E-mail: mark.wilde@mcgill.ca and minhsiuh@gmail.com)

Shannon’s formula for the classical capacity of a classical channel [25]). The simplification that entanglement offers to the theory of quantum information has led to the following musing of Hayden *et al.* [26]:

“To what extent does the addition of free entanglement make quantum information theory similar to classical information theory?”

In this paper, we show that entanglement can “boost the engines of quantum turbo codes.” Specifically, we find many examples of EAQ convolutional encoders that can simultaneously be recursive and non-catastrophic. A “quantized” version of the result in Ref. [5] then implies that a quantum serial turbo code employing such an encoder along with another non-catastrophic encoder has an unbounded minimum distance [17], and non-catastrophicity implies that it has good iterative decoding performance. This result for EAQ convolutional encoders holds partly because all four Pauli operators acting on half of a Bell state are distinguishable when performing a measurement on both qubits in the Bell state (much like the super-dense coding effect [27]). The ability of EAQ convolutional encoders to be simultaneously non-catastrophic and recursive is another way in which shared entanglement aids in a straightforward quantization of a classical result—this assumption thus simplifies and enhances the existing theory of quantum turbo coding.

Our simulation results indicate that particular constructions of entanglement-assisted 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.* [7], in the sense that 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, essentially because entanglement increases the ability of a code to correct errors [28]. 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. The unassisted quantum turbo codes have performance similar to those of Poulin *et al.* in Ref. [7]. 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. 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 [21], [29], 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, but one advantage of them is that other simulations indicate that they are more tolerant to noise on the ebits. The quantum turbo codes with outer encoder

entanglement assistance have performance not far beyond that of the unassisted turbo codes. 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.

We organize this paper as follows. The first section establishes notations and definitions for EAQ codes similar to those in Ref. [7], and it also shows a way in which an EAQ code with only ebits is remarkably similar to a classical code. Section III defines the state diagram of an EAQ convolutional encoder—it reveals if an encoder is non-catastrophic and recursive, and we review how to check for these properties. Section IV gives several examples of non-catastrophic, recursive EAQ convolutional encoders and details their distance spectra. We discuss the construction of an EAQ serial turbo code in Section V and give several combinations of serial concatenations that have good minimum-distance scaling. Section VI contains our simulation results with accompanying interpretations of them. In Section VII, we show that entanglement is in fact *the* resource that enables a convolutional encoder to be both recursive and non-catastrophic—a corollary of Theorem 1 in Ref. [7] states that other resources such as classical bits, gauge qubits, and ancilla qubits do not help. Section VIII then discusses encoders that act on information qubits, ancilla qubits, ebits, and classical bits, and it gives an example of an encoders that can be recursive and non-catastrophic. Section IX states some general observations regarding recursiveness and non-catastrophicity for different types of encoders. The conclusion summarizes our contribution and states many open questions.

II. EAQ CODES

We first review some important ideas from the theory of EAQ codes in order to prepare us for defining convolutional versions of them along with their corresponding state diagrams. The development is similar to that in Section III of Ref. [7].

The encoder V of an EAQ code produces an encoded state by acting on a set of k information qubits in a state $|\psi\rangle$, a ancilla qubits, and c ebits:

$$|\bar{\psi}\rangle^{AB} \equiv V^A(|\psi\rangle^A \otimes |0_a\rangle^A \otimes |\Phi_c^+\rangle^{AB}),$$

where

$$\begin{aligned} |0_a\rangle^A &\equiv |0\rangle^{\otimes a}, \\ |\Phi_c^+\rangle^{AB} &\equiv \left(|\Phi^+\rangle^{AB}\right)^{\otimes c}, \\ |\Phi^+\rangle^{AB} &\equiv \frac{1}{\sqrt{2}} \left(|00\rangle^{AB} + |11\rangle^{AB}\right), \\ n &= k + a + c, \end{aligned}$$

and the sender Alice possesses c halves of the entangled pairs while the receiver Bob possesses the other c halves (see Figure 1). In what follows, we abuse notation by having V refer to the “Clifford group” unitary operator that acts as above, but having it also refer to a binary matrix that acts on

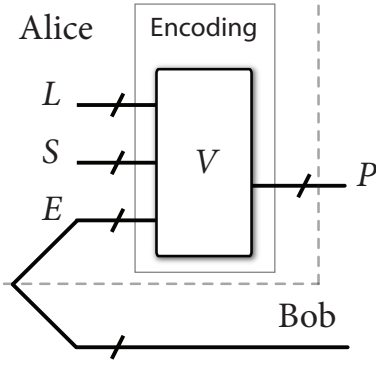


Fig. 1. The encoder of an EAQ code. Alice acts on her logical qubits L , local ancillas S , and her halves of the ebits E with an encoding unitary V . This encoding produces physical qubits P that she then inputs to a noisy quantum channel. The entanglement-assisted paradigm assumes that noise does not occur on Bob's half of the ebits, but we later study this setting in some simulations because it could occur in practice.

binary vectors—these binary vectors represent different Pauli operators that are part of the specification of an EAQ code (e.g., see Ref. [20]).³

Suppose now that Alice transmits her n qubits of the encoded state $|\bar{\psi}\rangle^{AB}$ over a noisy Pauli channel. Then the resulting state is $P^A |\bar{\psi}\rangle^{AB}$ where P^A is some n -fold tensor product of Pauli operators (in what follows, we simply say an “ n -qubit Pauli operator”). Suppose that Bob applies the inverse $(V^A)^\dagger$ of the encoding to the state $P^A |\bar{\psi}\rangle^{AB}$. The resulting state has the following form:

$$\begin{aligned} (V^A)^\dagger P^A |\bar{\psi}\rangle^{AB} &= (V^A)^\dagger P^A V^A (|\psi\rangle^A \otimes |0_a\rangle^A \otimes |\Phi_c^+\rangle^{AB}) \\ &= L^A |\psi\rangle^A \otimes S^A |0_a\rangle^A \otimes E^A |\Phi_c^+\rangle^{AB}, \end{aligned} \quad (1)$$

where L^A is some k -qubit Pauli operator, $S^A = S_1^A \otimes \dots \otimes S_a^A$ is an a -qubit Pauli operator, and $E^A = E_1^A \otimes \dots \otimes E_c^A$ is some c -qubit Pauli operator. Observe that

$$S^A |0_a\rangle^A = |s_1\rangle^A \otimes \dots \otimes |s_a\rangle^A,$$

where $s_i = 0$ if $S_i \in \{I, Z\}$ and $s_i = 1$ otherwise. The fact that s_i is invariant under the application of a Pauli Z operator implies that a quantum code can be degenerate (where two different errors mapping to the same syndrome have the same effect on the encoded state). Also, observe that

$$E^A |\Phi_c^+\rangle^{AB} = |\Phi(e_{1,x}, e_{1,z})\rangle^{AB} \otimes \dots \otimes |\Phi(e_{c,x}, e_{c,z})\rangle^{AB},$$

where $|\Phi(e_{i,x}, e_{i,z})\rangle^{AB}$ denotes the four distinguishable Bell states and

$$\begin{aligned} (e_{i,x}, e_{i,z}) &= (0, 0) \text{ if } E_i^A = I, \\ (e_{i,x}, e_{i,z}) &= (0, 1) \text{ if } E_i^A = Z, \\ (e_{i,x}, e_{i,z}) &= (1, 0) \text{ if } E_i^A = X, \\ (e_{i,x}, e_{i,z}) &= (1, 1) \text{ if } E_i^A = Y. \end{aligned}$$

³The representation of the encoder as a binary matrix leads to a loss of global phase information. Though, this global phase information is not important because measurement of the syndrome destroys it, and it is not necessary for faithful recovery of the encoded state.

Thus all four Pauli operators are distinguishable in this case by performing a Bell measurement (similar to the super-dense coding effect [27]). Ebits do not contribute to the degeneracy of a quantum code because different errors E^A lead to distinct measurement results.

Bob can perform Z basis measurements on the ancillas and Bell measurements on the ebits to determine the syndrome $r(P)$ of the Pauli error P :

$$r(P) \equiv (s_1, \dots, s_a, e_{1,x}, e_{1,z}, \dots, e_{c,x}, e_{c,z}).$$

Consider the following relation between the binary representations of P , V , L , S , and E in (1):

$$PV^{-1} = (L : S : E).$$

The syndrome $r(P)$ only partially determines S , but it fully determines E . Let us decompose the binary representation of S as $S = S^z + S^x$ and that of E as $E = E^z + E^x$. When Bob performs his measurements, he determines S^x , E^z , and E^x . That is, he determines the following relations between the components S_i^x of S^x and the components s_i of the syndrome $r(P)$:

$$S_i^x = X \text{ if } s_i = 1, \quad S_i^x = I \text{ otherwise.}$$

The syndrome also determines the i^{th} components E_i^x and E_i^z of E :

$$\begin{aligned} E_i^x &= X \text{ if } e_{i,x} = 1, & E_i^x &= I \text{ otherwise,} \\ E_i^z &= Z \text{ if } e_{i,z} = 1, & E_i^z &= I \text{ otherwise.} \end{aligned}$$

The phenomenon of degeneracy represents the most radical departure of quantum coding from classical coding [30], [31]. Consider two different physical errors P and P' that differ only by Z operators acting on the ancillas:

$$\begin{aligned} P &= (L : S^x + S^z : E^x + E^z)V \\ P' &= (L : S^x + S'^z : E^x + E^z)V \\ &= P + (I_k : S^z + S'^z : I_c)V, \end{aligned}$$

where I_k is a length $2k$ zero vector (the binary representation of a k -fold tensor product of identity operators). These different errors lead to the same error syndrome. In the classical world, this would present a problem for error correction. But this situation does not cause a problem in the quantum world for the errors P and P' —the logical error affecting the encoded quantum information is the same for both P and P' , and Bob can correct either of these errors simply by applying L^{-1} after decoding.

We now define several sets of operators that are important for determining the properties and performance of EAQ codes. The set $C(I)$ of harmless, undetected errors consists of all operators P that have a zero syndrome, yet have no effect on the encoded state:

$$C(I) \equiv \{P : P = (I_k : S^z : I_c)V, \quad S^z \in \{I, Z\}^a\}.$$

This set of operators is equivalent to the isotropic subgroup, in the language of Refs. [19], [20]. It is also analogous to the all-zero codeword of a classical code. The set $C(L)$ of harmful, undetected errors consists of all operators P that have a zero

syndrome, yet change the quantum information in the encoded state:

$$C(L) \equiv \{P : P = (L : S^z : I_c)V, \quad S^z \in \{I, Z\}^a\},$$

where $L \neq I_k$. This set of operators corresponds to a single logical transformation on the encoded state, depending on the choice of L , and it is analogous to a single codeword of a classical code. The set $C(L, S^x, E^x, E^z)$ corresponds to a particular logical transformation and syndrome, and is thus a logical coset:

$$C(L, S^x, E^x, E^z) \equiv \{P : P = (L : S^z + S^x : E^z + E^x)V, \quad S^z \in \{I, Z\}^a\}.$$

It is analogous to a single erred codeword of a classical code if S^x , E^x , or E^z is non-zero. The operator codewords of an EAQ code belong to the following set C :

$$C \equiv \bigcup_L C(L), \quad (2)$$

where L is an arbitrary k -qubit Pauli operator. The set C is equivalent to the full set of logical operators for the code, and it is analogous to the set of all codewords of a classical code. These definitions lead to the definition of the minimum distance of an EAQ code as the minimum weight of an operator P in $C - C(I)$:

$$d(C) \equiv \min \{w(P) : P \in C - C(I)\}.$$

This definition is similar to the definition of the distance of a classical code, but it incorporates the coset structure of a quantum code. Thus, we can determine the performance of the code in terms of distance by tracking its logical operators, and this intuition is important when we move on to EAQ convolutional codes. Also, the logical operators play an important role in decoding because a maximum likelihood decoding algorithm for a quantum code estimates the most likely logical error given the syndrome and a particular physical noise model.⁴

We end this section with a final remark concerning EAQ codes and the musing of Hayden *et al.* in Ref. [26]. Suppose that an EAQ code does not exploit any ancilla qubits and uses only ebits. Then the features of the code become remarkably similar to that of a classical code. Degeneracy, a uniquely quantum feature of a code, does not occur in this case because the syndrome completely determines the error, in analogy with error correction in the classical world. Also, the code loses its coset structure, so that $C(I)$ is equal to the identity operator, $C(L)$ is equivalent to just one logical operator, and the definition of the code's minimum distance is the same as the classical definition.

III. EAQ CONVOLUTIONAL CODES

An EAQ convolutional code is a particular type of EAQ code that has a convolutional structure. In past work on this topic [23], [24], [32], we adopted the ‘‘Grassl-Rötteler’’ approach to this theory [33], by beginning with a mathematical

description of the code and determining a Grassl-Rötteler pearl-necklace encoder that can encode it. Here, we adopt the approach of Poulin *et al.* [7] which in turn heavily borrows from ideas in classical convolutional coding [14]. We begin with a seed transformation (a ‘‘convolutional encoder’’ or a ‘‘quantum shift-register circuit’’) and determine its state diagram, which yields important properties of the encoder. We can always rearrange a Grassl-Rötteler pearl-necklace encoder as a convolutional encoder [34], [35], [36], but it is not clear that every convolutional encoder admits a form as a Grassl-Rötteler pearl necklace encoder. For this reason and others, we adopt the Poulin *et al.* approach in what follows.

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 physical or channel qubits,⁵ where $n = k + a + c$. The transformation that it induces on binary representations of Pauli operators acting on these registers is as follows:

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

where M' acts on the m output memory qubits, P acts on the n output physical qubits, M acts on the m input memory qubits, L acts on the k information qubits, S acts on the a ancilla qubits, and E acts on the c halves of ebits. 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 encoding circuit (recall that the goal of a decoding algorithm is to produce good estimates of logical errors). This representation is similar to the shift-register representation of classical convolutional codes, with the difference that the representation there corresponds to the actual flow of bit information through a convolutional circuit, while here it is merely a useful tool for analyzing the properties of the encoder.

The overall encoding operation for the code 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. [7] 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 [7]. 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 .

⁴The definitions for the maximum likelihood decoder of an EAQ code are nearly identical to those for stabilizer codes in Section IIIC of Ref. [7]. Thus, we do not give them here.

⁵Physical or channel qubits in the entanglement-assisted paradigm are the ones that Alice transmits over the channel.

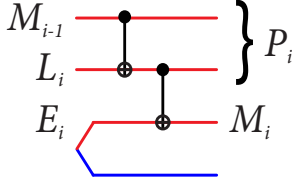


Fig. 2. (Color online) Seed transformation for an $n = 2$, $k = 1$, $c = 1$, $m = 1$ EAQ convolutional code.

A. 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 [14], [15]. 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. [7]. 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 $M \rightarrow M'$, 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

$$(M' : P) = (M : L : S^z : I_c)U. \quad (3)$$

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 2. It acts on one memory qubit, one information qubit, and one half of an ebit to produce two channel qubits and one memory qubit. Figure 3 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.

B. Non-catastrophicity

We now recall the definition of non-catastrophicity in Ref. [7], which is the formal quantization of the definition in Section IX of Ref. [14]. The definition from Ref. [7] 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. [7] to decode EAQ convolutional codes. A *path* through the state diagram is a sequence M_1, \dots, M_t of vertices such that $M_i \rightarrow M_{i+1}$ is an edge belonging to it. Each logical operator of C in (2) 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

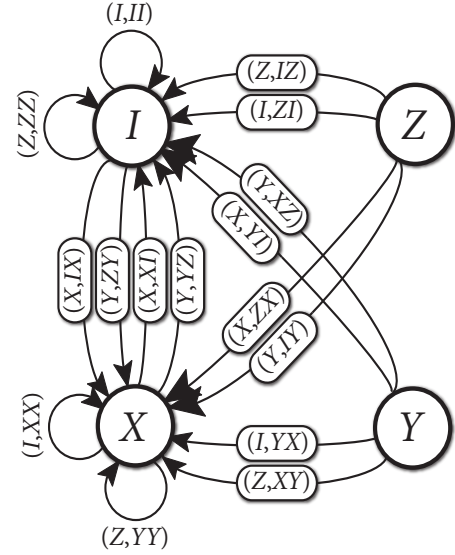


Fig. 3. The state diagram corresponding to the seed transformation in Figure 2. The state diagram allows us to check that the encoder is non-catastrophic and non-recursive.

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.

Why is this definition an appropriate definition of non-catastrophicity? We briefly review the argument in Ref. [7]. First, consider Figure 8 of Ref. [7]. There, the seed transformation is the same as that in our Figure 2, with the exception that the ebit is replaced by an ancilla qubit. Such a replacement leads to a doubling of the number of edges in the state diagram in our Figure 3 because the state diagram should include all of the transitions where a Z operator acts on the ancilla qubits (these all lead to other logical operators in their case). The new state diagram (see Figure 9 of Ref. [7]) includes a self-loop at memory state Z with zero physical weight and non-zero logical weight, and it is thus catastrophic according to the definition. The problem with such a loop is that it can “throw off” the iterative decoding algorithm. Consider again Figure 8 of Ref. [7]. If a Y error were to act on the second physical qubit in one frame of the code (while the identity acts on the rest), then “pushing” this error through the inverse of the encoder applies an X operator to the ancilla qubit and produces one syndrome bit for that frame of the code, but it propagates Z errors onto every logical qubit in the stream while applying Z errors to every memory qubit. All of these other errors go undetected by an iterative decoder because the error propagation does not trigger any additional syndrome bits besides the initial one that the Y error triggered.

Observe that the state diagram in Figure 3 for the EAQ convolutional encoder does not feature a zero physical-weight cycle with non-zero logical weight. Thus, the encoder is non-catastrophic, illustrating another departure from classical theory. *Non-catastrophicity in the quantum world is not only a property of the encoder, but it also depends on the resources*

available for encoding. If we analyze the above scenario that leads to catastrophic error propagation in the encoder of Figure 8 of Ref. [7], we see that it does not lead to such propagation for our setting in Figure 2. Indeed, suppose again that a Y error acts on the second physical qubit in a particular frame of the code (with the identity acting on all other qubits). Pushing this Y error through the inverse of the encoder leads to an X operator acting on the ebit and a Z operator acting on the memory. The X operator is detectable by a Bell measurement, and the Z operator acting on the memory propagates to a Z operator acting on an ebit in the next frame and then to all ebits and information qubits in successive frames. These Z operators acting on the ebits are all detectable by a Bell measurement (whereas they are not detectable when acting on an ancilla), so that the iterative decoding algorithm can still correct for errors in the propagation because all these errors trigger syndromes.

C. 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.⁶ 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 [16], [17] is essentially a direct translation of the classical proof [5]. 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 [7]. 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.⁷ One might think that quasi-recursive is a sufficient requirement for good performance, but our simulation results in Section VI 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 *admissible path* to be a path in which its first edge is not part of a zero physical-weight cycle [7]. Now, consider any vertex belonging to a zero-physical weight loop and any admissible 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 [7]. 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 2 is not recursive. The only vertex in the state diagram in Figure 3 belonging to a zero physical-weight cycle is the vertex labeled I . If the logical

⁶Recall that the inner encoder is the one closer to the channel, and the outer encoder is the one farther from the channel.

⁷This definition thus implies that a recursive encoder is infinite-depth (it transforms a finite-weight Pauli operator to an infinite-weight one) [33], [23], but the other implication does not necessarily have to hold.

input to the encoder is a Z operator followed by an infinite sequence of identity operators, the circuit outputs ZZ as the physical output, return to the memory state I , and then output 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 IV details many examples of EAQ convolutional encoders that are both recursive and non-catastrophic.

D. Distance Spectrum

We end this section by reviewing the performance measures from Ref. [7], which are also quantizations of the classical measures [14]. The *distance spectrum* $F(w)$ of an EAQ convolutional encoder is the number of admissible paths beginning and ending in memory states that are part of a zero physical-weight cycle, where the physical weight of each admissible path is w and the logical weight is greater than zero. This performance measure is most similar to the weight enumerator polynomial of a quantum block code [37], which helps give an upper bound on the error probability of a non-degenerate quantum code on a depolarizing channel under maximum likelihood decoding [38]. 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 next section details a simple method to compute the distance spectrum by using the state diagram and ideas rooted in Refs. [14], [39], [40], [41]. 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.

IV. EXAMPLE ENCODERS

Our first example of an EAQ convolutional encoder 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 first example in detail, verifying its non-catastrophicity and recursiveness, and we give a method to compute its distance spectrum. We then give tables that detail our other examples. We found all of these examples by picking encoders uniformly at random from the Clifford group, according to the algorithm in Section VI-A.2 of Ref. [42].

The seed transformation for our first example is as follows:

$$\begin{array}{cccc} Z & I & I & Z & I & X \\ I & Z & I & X & Z & Y \\ I & I & Z & X & Y & Z \\ X & I & I & X & X & X \\ I & X & I & Y & I & Y \\ I & I & X & Y & X & Y \end{array} \rightarrow \begin{array}{ccc} X & X & X \\ X & X & X \\ Y & I & Y \\ Y & X & Y \end{array}, \quad (4)$$

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. We can abbreviate the above encoding by taking the binary representation of each row at the output and encoding it as a decimal number. For example, the first row ZIX has the binary representation $\begin{bmatrix} 1 & 0 & 0 & | & 0 & 0 & 1 \end{bmatrix}$ which is the decimal number 33. Thus, we can specify this encoder as $\{33, 29, 30, 7, 45, 47\}$.⁸

The seed transformation in (4) leads to the state diagram of Figure 4, by exploiting (3). We can readily check that the encoder is non-catastrophic and recursive by inspecting Figure 4. 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 admissible 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. We can then check that inputting a Z logical operator followed by identities keeps us in the self-loop at the X memory state while still outputting non-zero physical weight operators, and inputting a Y logical operator followed by identities keeps us in the self-loop at the Z memory state. The encoder is thus recursive.

There is a straightforward way to compute the distance spectrum of the encoder. This technique borrows from similar ideas in the classical theory of convolutional coding [14], [39], [40], [41]. We would like to know the number of admissible paths with a particular weight beginning and ending in memory states that are part of a zero physical-weight cycle. Again, for our example, the identity memory state is the only memory state part of a zero physical-weight cycle. We create a *weight adjacency matrix* whose entries correspond to edges in the state diagram. This matrix has x^w in entry (i, j) if there is a physical-weight- w edge from vertex i to vertex j (with the exception of the self-loop at the identity memory state). The weight adjacency matrix A for our example is

$$A \equiv \begin{bmatrix} 0 & x^2 & x & x \\ x^2 & x^2 & x^2 & x^2 \\ x^2 & x & x & x^2 \\ x^2 & x & x^2 & x \end{bmatrix},$$

where the ordering of vertices is $I, X, Y,$ and Z . Note that we place a zero in the $(1, 1)$ entry because we do not want to overcount the number of admissible paths starting and ending in memory states that are part of a zero physical-weight cycle. If we would like the number of admissible paths up to an arbitrary weight that start and end in the identity memory state, then we compute the $(1, 1)$ entry of the following matrix:

$$(I - A)^{-1} = I + A + A^2 + A^3 + \dots$$

The coefficient of x^w in the polynomial entry $B(1, 1)$ is the number of admissible paths with weight w starting and ending

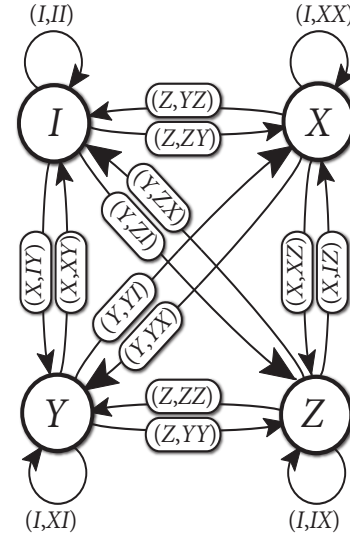


Fig. 4. The state diagram corresponding to the seed transformation in (4), acting on one memory qubit, one information qubit, one ebit, and producing two physical qubits. The above state diagram allows us to check that the encoder is both recursive and non-catastrophic.

in the identity memory state. We can approximate the distance spectrum, e.g., by computing the matrix B where

$$B = \sum_{i=1}^{10} A^i.$$

Computing the above matrix can be computationally expensive, but we can dramatically reduce the number of computations by truncating the polynomial entries of A above degree ten before performing each multiplication. For our example, the first ten entries of the distance spectrum polynomial are

$$2x^3 + 5x^4 + 6x^5 + 23x^6 + 54x^7 + 122x^8 + 298x^9 + 737x^{10}.$$

These coefficients appear in the second column of Table II as the first ten values of the distance spectrum for this first example encoder. Note that there are faster ways of computing the distance spectrum for classical convolutional codes [43], and it remains open to determine how to exploit these techniques for quantum convolutional encoders.

Table I lists the specifications of many other examples of EAQ encoders that are both recursive and non-catastrophic—a computer program helped check that these properties hold for each of the examples [44]. Included in the list of example encoders are some which act on ancilla qubits in addition to ebits. These examples demonstrate that we do not necessarily require the auxiliary resource of an EAQ convolutional encoder to be ebits alone in order for the encoder to possess both properties. Table II gives the distance spectrum for each of these encoders.

V. EAQ TURBO CODES

We comment briefly on the construction and minimum distance of a quantum serial turbo code that employs our example encoders as a constituent encoder (the next section details our

⁸Note that this convention is different from that of Poulin *et al.* in Ref. [7].

Encoder	M	L	A	E	Seed Transformation	Free Dist.
1	1	1	0	1	{33, 29, 30, 7, 45, 47}	3
2	3	2	0	1	{2188, 246, 115, 2053, 1847, 833, 1658, 2571, 1566, 2783, 2990, 3229}	4
3	3	3	0	1	{12515, 8790, 10280, 11314, 6500, 14691, 1430, 7105, 8817, 1420, 10014, 7061, 10739, 8972}	4
4	3	4	0	1	{23233, 28350, 13963, 43904, 58908, 19553, 6318, 63573, 12838, 7558, 22611, 27045, 48320, 9596, 48500, 54018}	3
5	2	1	1	1	{159, 1006, 727, 641, 925, 522, 726, 314, 793, 648, 119, 210}	4
6	2	1	1	2	{1116, 1363, 1495, 1326, 241, 2411, 2268, 1480, 2032, 1589, 810, 3351}	5
7	2	2	1	1	{141, 509, 3495, 2470, 2702, 3576, 1522, 905, 2622, 1598, 642, 773}	3
8	2	6	0	1	{113633, 199924, 181760, 243189, 25748, 110950, 158559, 282, 205474, 193680, 199692, 252779, 245067, 64266, 147306, 152171, 230343, 75396}	2
9	2	8	0	1	{2432999, 1503627, 1816960, 1050871, 1297694, 3894582, 410463, 2344289, 1908709, 3176421, 3668357, 1860207, 1511167, 3829280, 3008050, 2896381, 999389, 374648, 4000734, 885953, 2452389, 3608225}	2
10	2	9	0	1	{4943947, 12156608, 10237254, 2501342, 2665695, 7306816, 8727132, 80870, 13726997, 16078090, 11897398, 9857749, 16524053, 972786, 5098459, 8962232, 10325041, 12705543, 8324846, 13241728, 11521711, 7907747, 16588769, 5842661}	N/A

TABLE I

SPECIFICATION OF OUR EXAMPLE EAQ CONVOLUTIONAL ENCODERS THAT ARE RECURSIVE AND NON-CATASTROPHIC. THE FIRST COLUMN INDEXES THE DIFFERENT ENCODERS, AND ALL OF THE OTHER COLUMNS CORRESPOND TO A PARTICULAR ENCODER. COLUMN “M” GIVES THE NUMBER OF MEMORY QUBITS, COLUMN “L” GIVES THE NUMBER OF INFORMATION QUBITS, COLUMN “A” GIVES THE NUMBER OF ANCILLA QUBITS, AND COLUMN “E” GIVES THE NUMBER OF EBITS. THE COLUMN LABELED “SEED TRANSFORMATION” SPECIFIES THE SEED TRANSFORMATION FOR EACH ENCODER, USING A DECIMAL REPRESENTATION. THE CONVENTION FOR QUBIT ORDERING IS THAT AN ENCODER ACTS ON MEMORY QUBITS, INFORMATION QUBITS, ANCILLA QUBITS, AND EBITS TO PRODUCE OUTPUT MEMORY QUBITS AND PHYSICAL OR CHANNEL QUBITS. THE CONVENTION FOR THE BIT REPRESENTATION OF A TENSOR PRODUCT OF PAULI OPERATORS IS $ZXYZ$ MAPS TO $[1011|0110]$, AND THE DECIMAL REPRESENTATION OF THIS BIT VECTOR IS 182 (SEE THE DISCUSSION AROUND (4) IN THE TEXT). THE LAST COLUMN GIVES THE FREE DISTANCE OF THE ENCODER.

w	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	2	0	0	3	0	0	3
4	5	1	8	32	3	0	22
5	6	6	69	292	3	1	73
6	23	49	463	2,622	23	1	286
7	54	218	3,478	24,848	41	1	1,309
8	122	1,077	25,057	227,262	127	3	5,696
9	298	5,477	181,959	$2.1 \cdot 10^6$	325	11	23,975
10	737	27,428	1,326,070	$1.9 \cdot 10^7$	1,061	17	102,132

TABLE II

THE DISTANCE SPECTRUM FOR THE FIRST SEVEN OF OUR EXAMPLE EAQ CONVOLUTIONAL ENCODERS. THE FIRST COLUMN ON THE LEFT GIVES THE FIRST 11 VALUES OF THE WEIGHT w , AND THE OTHER COLUMNS GIVE THE FIRST 11 VALUES OF THE DISTANCE SPECTRUM $F(w)$ OF THE FIRST SEVEN OF OUR EAQ CONVOLUTIONAL ENCODERS FROM TABLE I.

simulation results with different encoders). The construction of an EAQ serial turbo code is the same as that in Ref. [7] (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 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.

Perhaps the best combination for an EAQ serial turbo code is to choose the inner quantum convolutional encoder to be a recursive, non-catastrophic EAQ convolutional encoder and the outer quantum convolutional encoder to be a non-recursive, non-catastrophic standard quantum convolutional encoder. This combination reduces entanglement consumption, ensures good iterative decoding performance, and ensures that the minimum distance of the quantum serial turbo code grows as $N^{(d^* - 2)/d^*}$ where N is the length of the code and d^* is the free distance of the outer quantum convolutional encoder. The proof of this last statement [17], [16] is essentially identical to the classical proof [5]. Section VI-A shows that this combination also performs well in practice if noise occurs on the ebits. Additionally, choosing the outer quantum convolutional encoder to encode a highly degenerate code may increase the number of errors that the quantum turbo code can correct, in a vein similar to the results in Ref. [31] (though we have not yet fully investigated this possibility).

We can construct EAQ serial turbo codes, by serially concatenating some of our example “WH encoders” in Table I with the “PTO encoders” in Table 1 of Ref. [7] (ordered from left to right). Table III details these different combinations, giving their rates and average minimum distance scaling.

The columns of Table III give the outer encoder, the inner encoder, the quantum communication rate, the entanglement consumption rate, and the average minimum distance growth of a particular EAQ turbo code. The first four combinations all have a good average minimum distance scaling, but the catalytic rate⁹ for each of them is zero. The last six combinations both have a good average minimum distance scaling and a positive catalytic rate.

⁹The catalytic rate is the difference between the quantum communication rate and the entanglement consumption rate [20].

Outer	Inner	Q	E	Min. Dist.
PTO1	WH3	1/4	1/4	$N^{2/3}$
PTO2	WH3	1/4	1/4	$N^{5/7}$
PTO3	WH2	1/3	1/3	$N^{3/4}$
PTO3	WH7	1/4	1/4	$N^{3/4}$
PTO3	WH4	2/5	1/5	$N^{3/4}$
PTO2	WH8	2/7	1/7	$N^{5/7}$
PTO3	WH8	3/7	1/7	$N^{3/4}$
PTO3	WH9	4/9	1/9	$N^{3/4}$
PTO2	WH10	3/10	1/10	$N^{5/7}$
WH11	WH3	1/2	1/4	$N^{1/3}$

TABLE III

VARIOUS COMBINATIONS OF ENCODERS FOR QUANTUM TURBO CODES AND THEIR MINIMUM DISTANCE SCALING.

VI. SIMULATION RESULTS

We performed several simulations of EAQ turbo codes and detail the results in this section. This section begins with a description of the parameters of the constituent quantum convolutional encoders. We then describe how the simulation was run, and we finally discuss and interpret the simulation results.

We would like to compare our results with those of Poulin *et al.* [7]—our original intent was to exploit their encoders, but the lack of a clear exposition of their decimal representation convention has excluded us from doing so. So we instead randomly generated and filtered encoders that have comparable attributes to their encoders. The first encoder, dubbed “PTO1R,” acts on three input memory qubits, one information qubit, and two ancillas to produce three output memory qubits and three physical qubits. Its decimal representation is

$$\{1355, 2847, 558, 2107, 3330, 739, 2009, 286, 473, 1669, 1979, 189\},$$

and its distance spectrum polynomial is

$$11x^5 + 47x^6 + 253x^7 + 1187x^8 + 6024x^9 + 30529x^{10} + 153051x^{11} + 771650x^{12}.$$

This encoder is non-catastrophic and quasi-recursive, and its parameters and distance spectrum are comparable to those of Poulin *et al.*’s first encoder (though they did not comment there whether theirs is quasi-recursive) [7]. Replacing the two ancilla qubits in the encoder with two ebits gives a dramatic improvement in the distance spectrum polynomial:

$$2x^9 + x^{10} + 5x^{11} + 8x^{12} + 11x^{13} + 25x^{14} + 56x^{15} + 102x^{16} + 217x^{17} + 387x^{18} + 787x^{19}.$$

The encoder also becomes recursive after this replacement. Let “PTO1REA” denote the EA version of this encoder.

Our second encoder, dubbed “PTO3R,” acts on four input memory qubits, one information qubit, and one ancilla qubit to produce four output memory qubits and two physical qubits. Its decimal representation is

$$\{3683, 3556, 2872, 2211, 3561, 3534, 729, 3136, 743, 2643, 1330, 1656\},$$

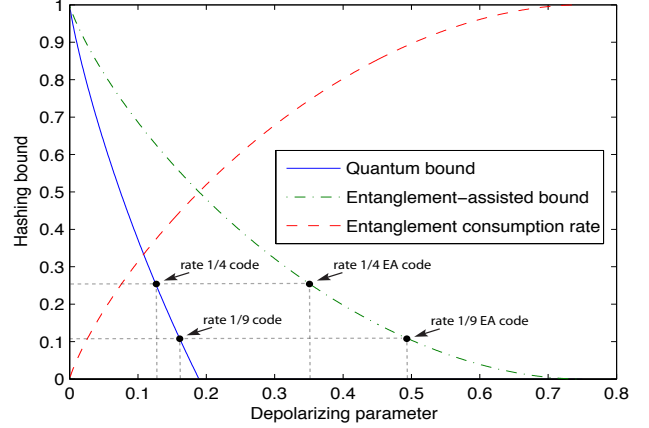


Fig. 5. The figure plots the hashing bound for quantum codes (solid blue curve), the entanglement-assisted hashing bound for EAQ codes (the dash-dotted green curve), and the entanglement consumption rate of the father protocol that meets the entanglement-assisted hashing bound (dashed red curve). The figure plots these different bounds as a function of the depolarizing parameter p . Observe that the noise limit for a rate 1/4 quantum code is ≈ 0.12689 , the noise limit for a rate 1/9 quantum code is ≈ 0.16028 , the noise limit for a rate 1/4 EAQ code is ≈ 0.35454 , and the noise limit for a rate 1/9 EAQ code is ≈ 0.49088 . We should compare our simulation results with these noise limits to observe how close our code constructions come to achieving capacity.

and its distance spectrum polynomial is

$$12x^5 + 93x^6 + 600x^7 + 4320x^8 + 31098x^9 + 224014x^{10} + 1604435x^{11} + 11469935x^{12}.$$

The encoder is non-catastrophic and quasi-recursive with its parameters and distance spectrum comparable to those of Poulin *et al.*’s third encoder. Replacing the ancilla with an ebit gives an improvement to the distance spectrum polynomial:

$$x^6 + 3x^7 + 7x^8 + 29x^9 + 88x^{10} + 237x^{11} + 716x^{12} + 2166x^{13} + 6245x^{14} + 18696x^{15} + 55889x^{16} + 165971x^{17} + 492805x^{18} + 1465529x^{19},$$

and the encoder becomes recursive after this replacement. Let “PTO3REA” denote the EA version of the “PTO3” encoder.

Our turbo codes consist of interleaved serial concatenation of the above encoders with themselves, and we varied the auxiliary resources of the encoders to be ebits, ancillas, or both. Concatenating PTO1R with itself leads to a rate 1/9 quantum turbo code, and concatenating PTO3R with itself leads to a rate 1/4 turbo code.

We simulated the performance of these EAQ turbo codes on a memoryless depolarizing channel with parameter p . The action of the channel on a single qubit density operator ρ is as follows:

$$\rho \rightarrow (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z).$$

The benchmarks for the performance of any standard or entanglement-assisted quantum code on a depolarizing channel are the hashing bounds [45], [21]. The quantum hashing bound determines the rate at which a random quantum code can

operate reliably for a particular depolarizing parameter p , but note that it does not give the ultimate capacity limit because degeneracy can improve performance [31], [46], [47], [48]. On the other hand, the entanglement-assisted hashing bound does give the ultimate capacity at which an EAQ code can operate reliably for a particular depolarizing parameter p , whenever an unbounded amount of entanglement is available [21], [29]. The hashing bound for quantum communication is

$$1 - [H_2(p) + p \log_2(3)],$$

and the hashing bound for an entanglement-assisted quantum code is

$$1 - \frac{1}{2} [H_2(p) + p \log_2(3)].$$

The father protocol is a quantum communication protocol that achieves the entanglement-assisted quantum capacity [49], [50], [51], while attempting to minimize its entanglement consumption rate. Its entanglement consumption rate is provably optimal for certain channels such as the dephasing channel [52], [53], [54], but it is not necessarily optimal for the depolarizing channel. The entanglement consumption rate of the father protocol on a depolarizing channel is

$$\frac{1}{2} [H_2(p) + p \log_2(3)].$$

This entanglement consumption rate implies that the only resources involved in an encoded transmission of the father protocol are information qubits and ebits because the sum of its quantum communication rate and its entanglement consumption rate is equal to one. Figure 5 plots these different hashing bounds and depicts the location of these bounds for our different quantum turbo codes. We performed Monte Carlo simulations to determine the performance of our example EAQ turbo codes when decoded with an iterative decoding algorithm (the iterative decoding algorithm is similar to that from Ref. [7], with the exception that it decodes EAQ turbo codes). We developed a Matlab computer program [44], and we conducted these simulations for about one month on approximately 70 Ubuntu Linux servers in the School of Computer Science at McGill University.

A single run of a simulation selects a quantum turbo code with a particular number of logical qubits and a random choice of interleaver, and it then generates a Pauli error randomly according to a depolarizing channel with parameter p . This Pauli error leads to an error syndrome, and the syndrome and channel model act as inputs to the iterative decoding algorithm. The iterative decoding algorithm terminates if the hard decision on a recovery operation is the same decision from the previous iteration, or it terminates after a maximum number of iterations (though we never observed the number of iterations until convergence exceeding six). One run of the simulation declares a failure if the estimated recovery operation is different from the correct recovery operation. The ratio of simulation failures to the total number of simulation runs is the *word error rate* (WER). We ran every configuration (choice of code, depolarizing parameter, and number of logical qubits) until we observed at least 100 failures—this number guarantees a reasonable statistical confidence in the results of the simulations.

Our first simulation involved the serial concatenation of the unassisted PTO1R encoder with itself, and Figure 6(a) displays the results. The performance is similar to that of the first encoder of Poulin *et al.* (see Figure 12 of Ref. [7]). A noticeable feature of Figure 6(a) is the existence of a pseudothreshold, such that increasing the number of encoded qubits of the turbo code decreases the WER for all depolarizing noise rates below the pseudothreshold. The pseudothreshold is not a true threshold because this particular turbo code has a bounded minimal distance, and at some point, the WER should begin increasing if we continue to increase the number of encoded qubits [7]. The pseudothreshold 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.

Our second simulation tested the serial concatenation of the PTO1REA encoder with itself, and Figure 6(b) displays the results. This turbo code uses the maximal amount of entanglement at a rate of 8/9 and thus is an instance of the father protocol. Entanglement assistance gives the turbo code a dramatic boost in performance, in the sense that it can withstand far higher depolarizing noise rates than the unassisted turbo code. The true threshold occurs at ≈ 0.345 —it is a true threshold because the code has a provably unbounded minimal distance [17], 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. Thus, this code construction is operating in a noise regime in which standard quantum codes are simply not able to operate (compare with the results in Refs. [55], [56], [57], [7], [58], [59], [60], [61]).

Our third simulation tested the serial concatenation of the PTO1REA inner encoder with the PTO1R outer encoder, and this EAQ turbo code has an entanglement consumption rate of 6/9. The inner encoder is recursive, but the outer encoder's free distance is not as high as that in the previous simulation. Thus, we should expect performance not to be as high as in the previous simulation. Figure 6(c) displays the results. Since the inner encoder is recursive, the EAQ turbo code has an unbounded minimum distance, and the threshold in Figure 6(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.

Our final simulation tested the serial concatenation of the PTO1R inner encoder with the PTO1REA outer encoder, and this EAQ turbo code has an entanglement consumption rate of 2/9. The inner encoder is quasi-recursive, and the outer encoder has a significantly higher free distance than in the previous simulation because it has entanglement assistance. This simulation provides a good test to determine the effectiveness of an inner encoder that is quasi-recursive. That is, one might think that quasi-recursiveness of the inner encoder combined with an outer encoder with high free distance would be sufficient to produce a turbo code with good performance (the thought is that this would explain the good performance in the first simulation), but Figure 6(d) demonstrates that this intuition does not hold. The pseudothreshold occurs at

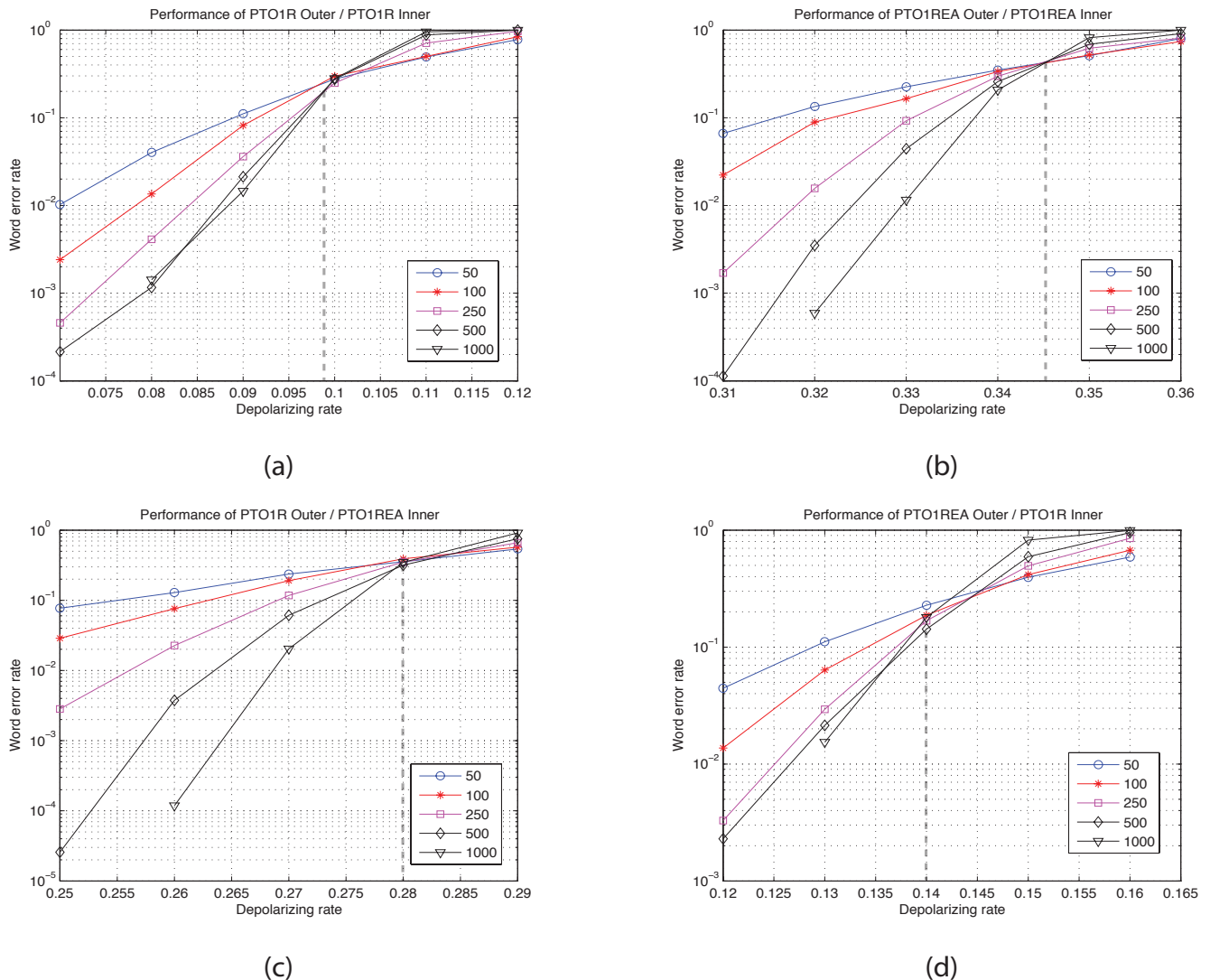


Fig. 6. The figure plots the results of four different simulations that exploit the PTO1R and PTO1REA encoders. The resulting EAQ turbo codes have rate $1/9$ and varying entanglement consumption rates. Each plot demonstrates the existence of a threshold, where the code performance increases whenever the channel noise rate is below the threshold. The vertical dotted line in each plot indicates the approximate location of the threshold.

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.

We conducted similar simulations with the PTO3R and PTO3REA encoders, and Figures 7(a-d) display the results. The entanglement consumption rates in Figures 7(a-d) are 0, $3/4$, $2/4$, and $1/4$, respectively. The results are similar to the previous simulations with the difference that the noise limits and thresholds are lower because these codes have higher quantum transmission rates. The thresholds (pseudo and true) occur at approximately 0.067, 0.216, 0.17, and 0.09 in Figures 7(a-d), respectively. There is one feature of the result in Figure 7(c) that is worth discussing. Consider that the midpoint of the highest threshold 0.216 and the threshold

0.09 is 0.153. One might expect then that a turbo code with entanglement consumption rate halfway between $1/4$ and $3/4$ should have a threshold occurring at the halfway point 0.153. But this is not the case for the code in Figure 7(c) with entanglement consumption rate $2/4$. Its threshold occurs at 0.17, which is slightly higher than 0.153. Thus, this EAQ turbo code is making judicious use of the available entanglement by placing the two ebits in the inner encoder. We would have to conduct further simulations to determine if placing one ebit in the outer encoder and one in the inner encoder would do better, but our suspicion is that the aforementioned use of entanglement is better because the inner encoder is recursive under this choice.

A. Noise on Ebits

We conducted another set of simulations to determine how noise on Bob's half of the ebits affects the performance of a

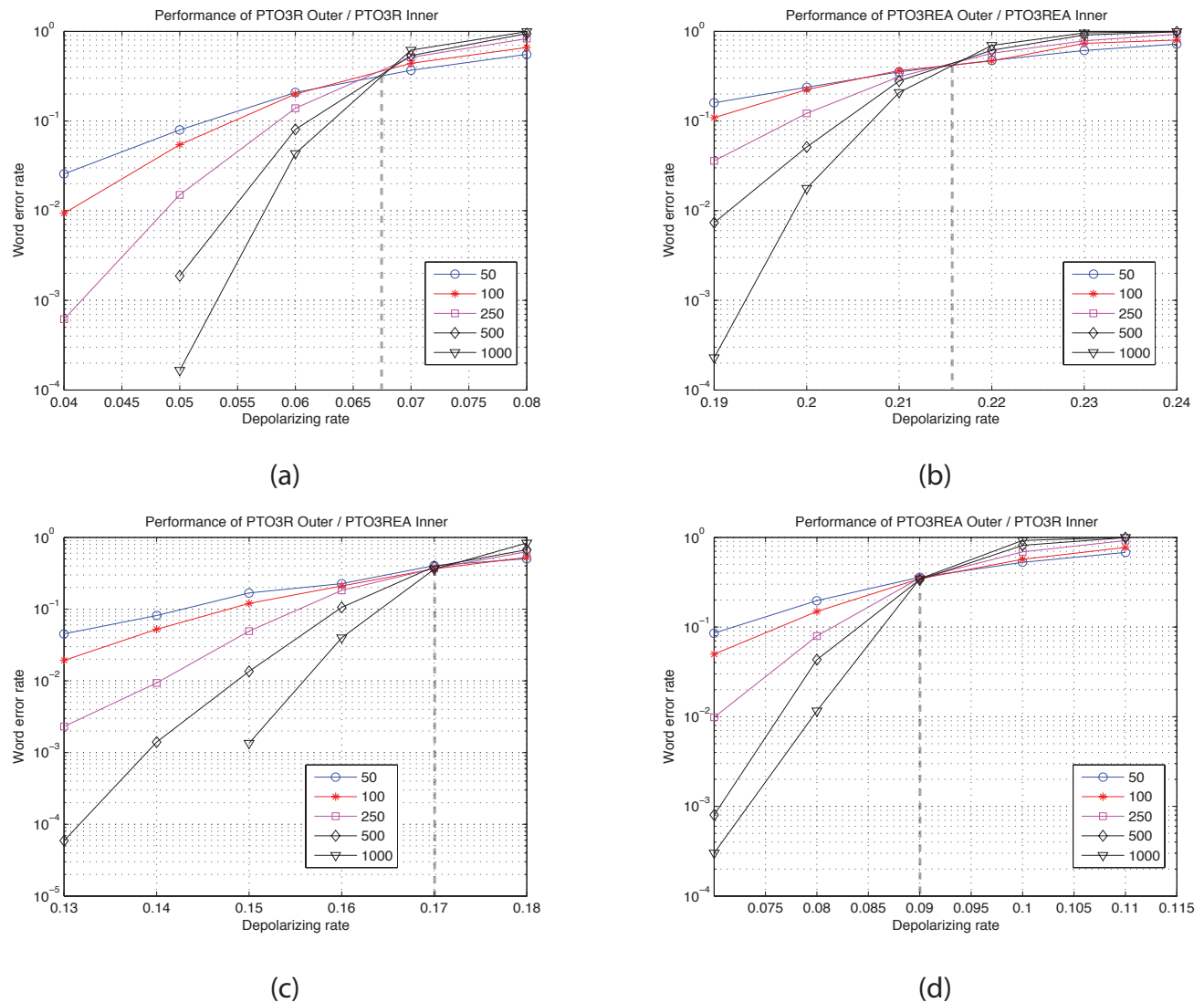


Fig. 7. The figure plots the results of four different simulations that exploit the PTO3R and PTO3REA encoders. The resulting EAQ turbo codes have rate $1/4$ and varying entanglement consumption rates. Each plot demonstrates the existence of a threshold, where the code performance increases whenever the channel noise rate is below the threshold. The vertical dotted line in each plot indicates the approximate location of the threshold.

code. This possibility has long been one of the important practical questions concerning the entanglement-assisted paradigm, and some researchers have provided partial answers [62], [63], [64], [65]. We briefly review some of these contributions. Shaw *et al.* first observed that the $[[7, 1, 3]]$ Steane code is equivalent to a $[[6, 1, 3; 1]]$ entanglement-assisted code that can also correct a single error on Bob's half of the ebit. This observation goes further: any standard, non-degenerate $[[n, k, d]]$ quantum code is equivalent to an $[[n - d + 1, k, d; d - 1]]$ entanglement-assisted code that can correct any $\lfloor (d - 1) / 2 \rfloor$ errors on Alice and Bob's qubits. This result holds because tracing over any $n - d + 1$ qubits in the original standard code gives a maximally mixed state on $d - 1$ qubits, and the purification of these qubits are $n - d + 1$ encoded halves of ebits that Alice possesses [66]. Wilde and Fattal observed that entanglement-assisted codes correcting for errors on Bob's

side slightly improve the threshold for quantum computation if ebit errors occur less frequently than gate errors [63]. Hsieh and Wilde studied this question in the Shannon-theoretic context and determined an expression for capacity when channel errors and entanglement errors occur [64]. As a side note, Lai and Brun recently looked for codes attempting to achieve the opposite goal [28]—their codes try to maximize the number of channel errors that can be corrected while minimizing the correction on Bob's half of the ebits.

Figure 8 plots the results of our simulations that allow for noise on Bob's half of the ebits. We performed three different types of simulations: the first was with the PTO3REA inner / PTO3R outer combination, the second with the PTO3R inner / PTO3REA outer combination, and the third with the PTO3REA inner / PTO3REA outer combination. For each simulation, we kept the channel noise rates fixed at 0.14, 0.07,

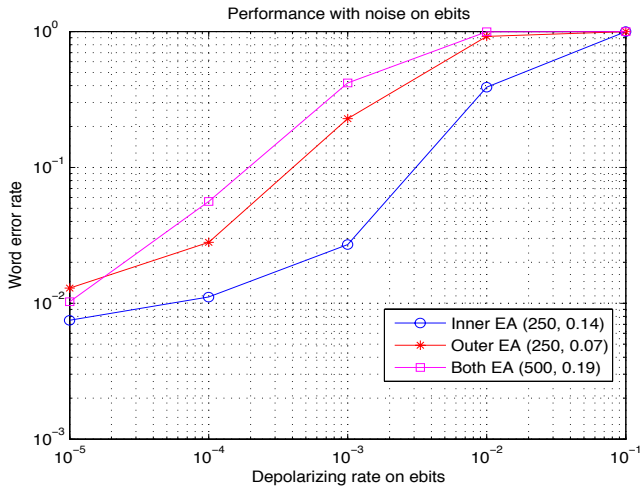


Fig. 8. The figure plots the performance of different inner and outer encoder combinations as a function of noise rate on Bob’s half of the ebits. It is surprising that the combination PTO3REA inner / PTO3R outer can withstand more ebit noise than the combination PTO3R inner / PTO3REA outer even though it uses more ebits than this latter combination.

and 0.19, respectively, because the codes already performed reasonably well at these noise rates, and our goal was to understand the effect of ebit noise on code performance. The codes all performed about the same as they did without ebit noise if we set the ebit noise rate at 10^{-5} . Increasing the ebit noise rate an order of magnitude to 10^{-4} has the least effect on the PTO3REA inner / PTO3R outer combination. Increasing it further to 10^{-3} deteriorates the performance of the other combinations while still having the least effect on the PTO3REA inner / PTO3R outer combination. This result is surprising, considering that this combination has an entanglement consumption rate of $2/4$ while the entanglement consumption rate of the PTO3R inner / PTO3REA outer combination is smaller at $1/4$. The result suggests that it would be wiser to place ebits in the inner encoder rather than in the outer encoder when these codes operate in practice.

VII. RECURSIVE, CLASSICALLY-ENHANCED SUBSYSTEM ENCODERS ARE CATASTROPHIC

We can construct other variations of quantum convolutional encoders and study their state diagrams to determine their properties. One example of a variation mentioned at the end of Ref. [7] is a subsystem convolutional code (based on the idea of a subsystem quantum code [67], [68], [69] that is useful in fault-tolerant quantum computation [70]). 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. 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 (such codes are known as “classically-enhanced” codes [71] and are based on trade-off coding ideas

from quantum Shannon theory [72]).

Unfortunately, encoders that act on logical qubits, classical bits, ancilla qubits, and gauge qubits cannot possess both properties simultaneously, and we state this result below as a corollary of Theorem 1 in Ref. [7]. 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).

Corollary 1: Suppose that a classically-enhanced subsystem convolutional encoder is recursive. Then it is catastrophic.

Proof: First, consider that the state diagram for a classically-enhanced subsystem quantum convolutional encoder includes an edge from M to M' if there exists a k_q -qubit Pauli operator $L_q \in \{I, X, Y, Z\}^{k_q}$, an a -qubit Pauli operator $S^z \in \{I, Z\}^a$, a k_c -qubit Pauli operator $L_c^x + C^z \in \{I, X, Y, Z\}^{k_c}$, and a g -qubit Pauli operator $G^x + G^z \in \{I, X, Y, Z\}^g$ such that

$$(M' : P) = (M : L_q : S^z : L_c^x + C^z : G^x + G^z)U, \quad (5)$$

where the binary representations of Pauli operators are the same as in (3). We break the operator acting on the k_c classical bits into two parts because L_c^x represents the X component of the operator that can flip a classical bit from $|0\rangle$ to $|1\rangle$ and back, while C^z represents the Z component of the operator that has no effect on a classical bit in state $|0\rangle$ or $|1\rangle$ (it merely adds an irrelevant global phase in the case that the bit is equal to $|1\rangle$). The entries G^x and G^z are for the “gauge qubits” in a subsystem code [69] (qubits in a maximally mixed state that are invariant under the random application of an arbitrary Pauli operator). We include these transitions in the state diagram because a particular logical operator $L \equiv (L_q : L_c^x)$ in a classically-enhanced subsystem code is equivalent up to Z operators acting on the ancilla qubits, Z operators acting on the classical bits, and X and Z operators acting on gauge qubits. The set $C(L)$ corresponding to a particular logical input $L \equiv (L_q : L_c^x)$ consists of all operators P of the following form:

$$C(L) \equiv \left\{ \begin{array}{l} P : P = (L_q : S^z : L_c^x + C^z : G^x + G^z)V, \\ S^z \in \{I, Z\}^a, \quad C^z \in \{I, Z\}^{k_c}, \\ G^x + G^z \in \{I, X, Y, Z\}^g \end{array} \right\},$$

where V in this case consists of the infinite, repeated, overlapping application of the convolutional encoder U .

Suppose that the encoder is recursive. By definition, it follows that every weight-one logical input L and its coset $C(L)$ has an infinite response. Suppose now that we change the resources in the encoder so that all of the classical bits and gauge qubits become ancilla qubits. The resulting code is now a standard stabilizer code. Additionally, we can remove the X operators L_c^x from the definition of $C(L)$ because they no longer play a role as a logical operator, and we can remove the X operators G^x from the definition of $C(L)$ because they are acting on ancilla qubits. Let $C'(L')$ denote the new set corresponding to a particular logical operator $L' \equiv (L_q : I_{k_c})$:

$$C'(L') \equiv \left\{ \begin{array}{l} P : P = (L_q : S^z : C^z : G^z)V, \\ S^z \in \{I, Z\}^a, \quad C^z \in \{I, Z\}^{k_c}, \\ G^z \in \{I, Z\}^g \end{array} \right\}.$$

The encoder is still recursive because $C'(L') \subset C(L')$ and because the original encoder is recursive (recursiveness is a property invariant under the replacement of cbits and gauge qubits with ancilla qubits). Then Theorem 1 of Ref. [7] implies that the encoder for the stabilizer code is catastrophic, i.e., it features a zero physical-weight cycle with non-zero logical weight. It immediately follows that the original encoder for the classically-enhanced subsystem code is catastrophic because its state diagram contains all of the edges of the stabilizer encoder, plus additional edges that correspond to the logical transitions for the classical bits and the X operators acting on the gauge qubits. ■

We should note that the above argument only holds if the original classically-enhanced subsystem convolutional encoder acts on a non-zero number of logical qubits (this of course is the case in which we are really interested in order to have a non-zero quantum communication rate). For example, the encoder in Figure 2 becomes recursive and non-catastrophic when replacing the logical qubit with a classical bit and the ebit with an ancilla. One can construct the state diagram from the specification in (5) and discover that these two properties hold for the encoder acting on the cbit and ancilla.

The above argument also does not apply if an ebit is available as an auxiliary resource for an encoder. We have found an example of a non-catastrophic, recursive encoder that acts on six memory qubits, one logical qubit, one ancilla qubit, one ebit, one cbit, and one gauge qubit. The seed transformation for this example is as follows:

$$\{2934387, 3034525, 2323986, 3804870, 964819, 2111270, 3722470, 1017852, 2678995, 912985, 1575948, 3138834, 142503, 317898, 3473283, 1492935, 2701400, 2492844, 2078030, 1894781, 915544, 75029\}.$$

A non-catastrophic, non-recursive subsystem convolutional encoder with a high free distance could potentially serve well as an outer encoder of a quantum turbo code, but this might not necessarily be beneficial if our aim is to achieve the capacity of a quantum channel. The encoder for a subsystem code is effectively a noisy encoding map because it is a unitary acting on information qubits in a pure state, ancilla qubits in a pure state, and gauge qubits in the maximally mixed state. Ref. [52] proves that an isometric encoder is sufficient to attain capacity, and we can thus restrict our attention to subspace codes rather than subsystem codes. Though, this line of reasoning does not rule out the possibility that iterative decoding could somehow benefit from the extra degeneracy available in a subsystem code, but this extra degeneracy would increase the decoding time.

VIII. CLASSICALLY-ENHANCED EAQ ENCODERS

We might also wish to construct classically-enhanced EAQ turbo codes that transmit classical information in addition to quantum information, in an effort to reach the optimal trade-off rates from quantum Shannon theory [52], [53]. These codes are then based on the structure of the codes in Refs. [71], [73]. The state diagram for the encoder includes an edge from M to M' if there exists a k_q -qubit Pauli operator $L_q \in \{I, X, Y, Z\}^{k_q}$, a k_c -qubit Pauli operator $L_c^x \in \{I, X\}^{k_c}$, a k_c -qubit Pauli

operator $L_c^z \in \{I, Z\}^{k_c}$, and an a -qubit Pauli operator $S^z \in \{I, Z\}^a$ such that

$$(M' : P) = (M : L_q : S^z : L_c^x + L_c^z : I_c)U.$$

The logical operator L_q acts on k_q qubits while the operator $L_c^x + L_c^z$ acts on k_c classical bits. We break this latter operator into two parts for the same reason discussed in the previous section. The state diagram for an encoder of this form is similar to that for an EAQ convolutional encoder because it includes all transitions for the classical bits. The difference is in the interpretation of the logical weight of edge transitions and in the logical label of an edge. If an edge features a Z operator acting on a classical bit, then this operator does not contribute to the logical weight of the transition and does not appear on the logical labels—an I appears on the logical label if I or Z acts on the classical bit and an X appears on the logical label if an X or Y acts on it.

We have found several examples of recursive, non-catastrophic encoders acting on these resources. One of our examples acts on five memory qubits, one logical qubit, one ancilla qubit, one ebit, and one classical bit. Its seed transformation is as follows:

$$\{162568, 174333, 260907, 261622, 168521, 3644, 101236, 204504, 227699, 260074, 138781, 9252, 257257, 179548, 78687, 6352, 230925, 180362\}.$$

IX. THE PRESERVATION OF RECURSIVENESS AND NON-CATASTROPHICITY UNDER RESOURCE SUBSTITUTION

The technique used to prove Corollary 1 motivates us to consider which resource substitutions preserve the properties of recursiveness and non-catastrophicity. We have two different cases:

- 1) A resource substitution that removes edges from the state diagram preserves non-catastrophicity and recursiveness.
- 2) A resource substitution that adds edges to the state diagram preserves catastrophicity and non-recursiveness.

To see the first case for recursiveness preservation, consider a general encoder acting on logical qubits, ancilla qubits, ebits, cbits, and gauge qubits. Each logical input $L \equiv (L_q : L_c^x)$ to the encoder has the following form:

$$C(L) \equiv \left\{ \begin{array}{l} P : \\ P = (L_q : S^z : I_c : L_c^x + C^z : G^x + G^z)V, \\ S^z \in \{I, Z\}^a, \quad C^z \in \{I, Z\}^{k_c}, \\ G^x + G^z \in \{I, X, Y, Z\}^g \end{array} \right\},$$

where the conventions are similar to what we had before. Suppose the encoder is recursive so that $C(X_i : I)$, $C(Y_i : I)$, $C(Z_i : I)$, and $C(I : X_j)$ all have an infinite response. Then the encoder is still recursive if we replace an ancilla with an ebit because the original encoder is recursive and we no longer have to consider the Z operator acting on the replaced ancilla. The encoder is still recursive if we replace a cbit with an ancilla qubit because we no longer have to consider the coset $C(I : X_j)$. Finally, it is still recursive if we replace a gauge qubit with an ancilla qubit because we no longer have to consider the X operator acting on the replaced gauge qubit.

To see the first case for non-catastrophicity preservation, suppose that an encoder is already non-catastrophic. Then a resource substitution that removes edges from the state diagram preserves non-catastrophicity because this removal cannot create a zero physical-weight cycle with non-zero logical weight.

To see the second case for non-recursiveness preservation, suppose that an encoder acting on logical qubits and ebits is non-recursive, meaning that at least one of the weight-one logical inputs X_i , Y_i , or Z_i has a finite response. Then replacing an ebit with an ancilla certainly cannot make the resulting encoder recursive because we have to consider the response to the operators X_i , Y_i , or Z_i and one of these is already finite from the assumption of non-recursiveness of the original encoder. Furthermore, consider a non-recursive encoder acting on logical qubits, ebits, and ancilla qubits. Replacing some of the ancilla qubits with cbits or gauge qubits cannot make the encoder become recursive for the same reasons.

To see the second for catastrophicity preservation, suppose that an encoder is catastrophic. Then a resource substitution that adds edges to the state diagram preserves catastrophicity because any zero physical-weight cycles with non-zero logical weight are still part of the state diagram for the new encoder.

The following diagram summarizes all of the above observations. The resources are L for logical qubits, S for ancilla qubits, E for ebits, C for cbits, and G for gauge qubits. Recursiveness and non-catastrophicity preservation flow downwards under the displayed resource substitutions, while non-recursiveness and catastrophicity preservation flow upwards (substitutions at the same level can go in any order).

$$\begin{array}{cccccc}
 (& L & : & S & : & E & : & C & : & G &) \\
 & & & \downarrow\uparrow & & & & \downarrow\uparrow & & \downarrow\uparrow & \\
 (& L & : & E & : & E & : & S & : & S &) \\
 & & & & & & & \downarrow\uparrow & & \downarrow\uparrow & \\
 (& L & : & E & : & E & : & E & : & E &)
 \end{array}$$

We can then understand the proof of Corollary 1 in the context of the above diagram. The original encoder acts on $(L : S : C : G)$ and is assumed to be recursive. Resource substitution of C and G preserves recursiveness, while making the encoder act on only ancilla qubits (the auxiliary resource for a standard quantum code). Using the fact that standard recursive quantum encoders are catastrophic [7], we then back substitute the resources, which is a catastrophicity preserving substitution.

X. CONCLUSION AND CURRENT WORK

We have constructed a theory of EAQ serial turbo coding as an extension of Poulin *et al.*'s theory in Ref. [7]. The introduction of shared entanglement simplifies the theory because an EAQ convolutional encoder can be both recursive and non-catastrophic. These two properties are essential for a quantum serial turbo code to have a minimum distance that grows near-linearly with the length of the code, while still performing well under iterative decoding. We provided many examples of EAQ convolutional encoders that satisfy both properties, and we detailed their parameters. We then showed

how the concatenation of these encoders with some of Poulin *et al.*'s and some of our own lead to EAQ serial turbo codes with near-linear minimum distance scaling that outperforms the scaling of the codes in Ref. [74]. We conducted several simulations of EAQ turbo codes—two notable surprises were that placing ebits in the inner encoder can achieve a better performance than expected in both scenarios with and without ebit noise. Our simulations are generally consistent with the findings in Ref. [32], [28] and other results from quantum Shannon theory [21], [50], namely, that entanglement assistance can significantly enhance error correction ability. Finally, we considered how to construct the state diagram for encoders that derive from other existing extensions to the theory of quantum error correction, and we showed that classically-enhanced subsystem convolutional encoders cannot simultaneously be recursive and non-catastrophic.

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 Section VIII to determine if they could come close to achieving the optimal rates from quantum Shannon theory [52], [53]. For example, what is the best arrangement for a classically-enhanced EAQ code? Should we place the classical bits in the inner or outer encoder? Are there more clever ways to use entanglement so that we increase error-correcting ability while reducing entanglement consumption? Consider that Hsieh *et al.* recently constructed a class of entanglement-assisted codes that exploit one ebit and still have good performance [75].

We should stress that the behavior of the entanglement-assisted codes using maximal entanglement is exactly like that of a classical turbo code. There is no degeneracy, and the iterative decoding algorithm is exactly the same as the classical one. Furthermore, analyses of classical turbo codes should apply directly in these cases [4], [76], and it would be good to determine the exact correspondence. These analyses studied the bit error rate rather than the word error rate, so any study of EAQ turbo codes would have to factor into account this difference.

Much of the classical literature has focused on the choice of a practical interleaver rather than a random one [77], [78], [79], [80], and it might be interesting to import the knowledge discovered here to the quantum case.

Finally, it would be great to find examples of EAQ turbo codes with a positive catalytic rate that outperform the turbo codes in Ref. [7], in the sense that they either have a higher catalytic rate while tolerating the same noise levels or they have the same catalytic rate while tolerating higher noise levels. We tried about five different combinations with no success for these examples.

We acknowledge David Poulin for providing us with a copy of Ref. [17] and for many useful discussions, e-mail interactions, and feedback on the manuscript. We acknowledge Jean-Pierre Tillich for originally suggesting that shared entanglement might help in quantum serial turbo codes. We acknowledge Todd Brun, Hilary Carteret, and Jan Florjanczyk for useful discussions, and Patrick Hayden for the observation that non-degenerate quantum codes lead to entanglement-assisted codes with particular error correction power on Bob's

half of the ebits. We acknowledge the computer administrators in the McGill School of Computer Science for making their computational resources available for this scientific research. MMW acknowledges the warm hospitality of the ERATO-SORST project and the support of the MDEIE (Québec) PSR-SIIRI international collaboration grant.

REFERENCES

- [1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," in *Technical Program of the IEEE International Conference on Communications*, 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] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: Turbo-codes," *IEEE Transactions on Communications*, vol. 44, no. 10, pp. 1261–1271, October 1996.
- [4] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara, "Serial concatenation of interleaved codes: performance analysis, design, and iterative decoding," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 909–926, May 1998.
- [5] N. Kahale and R. Urbanke, "On the minimum distance of parallel and serially concatenated codes," in *Proceedings of the International Symposium on Information Theory*, Cambridge, Massachusetts, USA, August 1998, p. 31. [Online]. Available: <http://lthcwww.epfl.ch/~ruediger/papers/weight.ps>
- [6] H. Ollivier and J.-P. Tillich, "Trellises for stabilizer codes: Definition and uses," *Physical Review A*, vol. 74, no. 3, p. 032304, September 2006.
- [7] D. Poulin, J.-P. Tillich, and H. Ollivier, "Quantum serial turbo-codes," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2776–2798, June 2009.
- [8] S. Lloyd, "Capacity of the noisy quantum channel," *Physical Review A*, vol. 55, no. 3, pp. 1613–1622, March 1997.
- [9] P. W. Shor, "The quantum channel capacity and coherent information," in *Lecture Notes, MSRI Workshop on Quantum Computation*, 2002.
- [10] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Transactions on Information Theory*, vol. 51, pp. 44–55, January 2005.
- [11] P. Hayden, M. Horodecki, A. Winter, and J. Yard, "A decoupling approach to the quantum capacity," *Open Systems & Information Dynamics*, vol. 15, pp. 7–19, March 2008.
- [12] H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Physical Review Letters*, vol. 91, no. 17, p. 177902, October 2003.
- [13] G. D. Forney, M. Grassl, and S. Guha, "Convolutional and tail-biting quantum error-correcting codes," *IEEE Transactions on Information Theory*, vol. 53, pp. 865–880, 2007.
- [14] 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.
- [15] A. J. Viterbi, A. M. Viterbi, and N. T. Sindhusayana, "Interleaved concatenated codes: New perspectives on approaching the Shannon limit," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 94, pp. 9525–9531, September 1997.
- [16] 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
- [17] H. Ollivier, D. Poulin, and J.-P. Tillich, "Quantum turbo codes," October 2008, unpublished manuscript.
- [18] J.-P. Tillich, "Quantum codes suitable for iterative decoding," Online presentation, May 2009. [Online]. Available: <http://www.infres.enst.fr/~markham/QuPa/28May/exposeJPTillich.pdf>
- [19] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, October 2006.
- [20] I. Devetak, T. A. Brun, and M.-H. Hsieh, *New Trends in Mathematical Physics*. Springer Netherlands, 2009, ch. Entanglement-Assisted Quantum Error-Correcting Codes, pp. 161–172.
- [21] 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.
- [22] —, "Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem," *IEEE Transactions on Information Theory*, vol. 48, pp. 2637–2655, 2002.
- [23] M. M. Wilde and T. A. Brun, "Entanglement-assisted quantum convolutional coding," *Physical Review A*, vol. 81, no. 4, p. 042333, April 2010.
- [24] —, "Quantum convolutional coding with shared entanglement: General structure," *Quantum Information Processing*, vol. 9, no. 5, pp. 509–540, October 2010, arXiv:0807.3803.
- [25] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 1948.
- [26] F. Dupuis, P. Hayden, and K. Li, "A father protocol for quantum broadcast channels," *IEEE Transactions on Information Theory*, vol. 56, no. 6, pp. 2946–2956, June 2010.
- [27] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Physical Review Letters*, vol. 69, no. 20, pp. 2881–2884, November 1992.
- [28] C.-Y. Lai and T. Brun, "Entanglement increases the error-correcting ability of quantum error-correcting codes," August 2010, arXiv:1008.2598.
- [29] G. Bowen, "Entanglement required in achieving entanglement-assisted channel capacities," *Physical Review A*, vol. 66, no. 5, p. 052313, November 2002.
- [30] P. W. Shor and J. Smolin, "Quantum error-correcting codes need not completely reveal the error syndrome," April 1996, arXiv:quant-ph/9604006.
- [31] D. P. DiVincenzo, P. W. Shor, and J. A. Smolin, "Quantum-channel capacity of very noisy channels," *Physical Review A*, vol. 57, no. 2, pp. 830–839, February 1998.
- [32] M. M. Wilde and T. A. Brun, "Extra shared entanglement reduces memory demand in quantum convolutional coding," *Physical Review A*, vol. 79, no. 3, p. 032313, March 2009.
- [33] M. Grassl and M. Rötteler, "Noncatastrophic encoders and decoder inverses for quantum convolutional codes," in *Proceedings of the IEEE International Symposium on Information Theory*, Seattle, Washington, USA, July 2006, pp. 1109–1113, arXiv:quant-ph/0602129.
- [34] M. M. Wilde, "Quantum-shift-register circuits," *Physical Review A*, vol. 79, no. 6, p. 062325, June 2009.
- [35] M. Houshmand, S. Hosseini-Khayat, and M. M. Wilde, "Minimal memory requirements for pearl necklace encoders of quantum convolutional codes," April 2010, arXiv:1004.5179.
- [36] M. Houshmand and S. Hosseini-Khayat, "Minimal-memory realization of pearl-necklace encoders of general quantum convolutional codes," September 2010, arXiv:1009.2242.
- [37] P. Shor and R. Laflamme, "Quantum analog of the MacWilliams identities for classical coding theory," *Physical Review Letters*, vol. 78, no. 8, pp. 1600–1602, February 1997.
- [38] D. Poulin, "Optimal and efficient decoding of concatenated quantum block codes," *Physical Review A*, vol. 74, no. 5, p. 052333, November 2006.
- [39] R. J. McEliece, *Communications and Coding (P. G. Farrell 60th birthday celebration)*. New York: John Wiley & Sons, 1998, ch. How to Compute Weight Enumerators for Convolutional Codes, pp. 121–141.
- [40] R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding*. Wiley-IEEE Press, 1999.
- [41] R. J. McEliece, *The Theory of Information and Coding*. Cambridge University Press, 2002.
- [42] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, "Quantum data hiding," *IEEE Transactions on Information Theory*, vol. 48, no. 3, pp. 580–598, March 2002.
- [43] M. L. Cedervall and R. Johannesson, "A fast algorithm for computing distance spectrum of convolutional codes," *IEEE Transactions on Information Theory*, vol. 35, no. 6, pp. 1146–1159, November 1989.
- [44] M. M. Wilde, "EA-Turbo," <http://code.google.com/p/ea-turbo/>, September 2010, Matlab and MEX software for characterizing and simulating entanglement-assisted quantum turbo codes (source code available under a GPL license).
- [45] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Physical Review A*, vol. 54, no. 5, pp. 3824–3851, November 1996.
- [46] G. Smith and J. A. Smolin, "Degenerate quantum codes for Pauli channels," *Physical Review Letters*, vol. 98, no. 3, p. 030501, January 2007.
- [47] J. Fern and K. B. Whaley, "Lower bounds on the nonzero capacity of Pauli channels," *Physical Review A*, vol. 78, no. 6, p. 062335, December 2008.

- [48] J. Fern, "Correctable noise of quantum-error-correcting codes under adaptive concatenation," *Physical Review A*, vol. 77, no. 1, p. 010301, January 2008.
- [49] I. Devetak, A. W. Harrow, and A. Winter, "A family of quantum protocols," *Physical Review Letters*, vol. 93, no. 23, p. 230504, December 2004.
- [50] —, "A resource framework for quantum Shannon theory," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4587–4618, October 2008.
- [51] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, "The mother of all protocols: restructuring quantum information's family tree," *Proceedings of the Royal Society A*, vol. 465, no. 2108, pp. 2537–2563, 2009.
- [52] M.-H. Hsieh and M. M. Wilde, "Entanglement-assisted communication of classical and quantum information," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4682–4704, September 2010, arXiv:0811.4227.
- [53] —, "Trading classical communication, quantum communication, and entanglement in quantum Shannon theory," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4705–4730, September 2010, arXiv:0901.3038.
- [54] M. M. Wilde and M.-H. Hsieh, "The quantum dynamic capacity formula of a quantum channel," April 2010, arXiv:1004.0458.
- [55] D. J. MacKay, G. Mitchison, and P. L. McFadden, "Sparse graph codes for quantum error-correction," *IEEE Transactions on Information Theory*, vol. 50, no. 10, p. 2315, October 2004.
- [56] M. Hagiwara and H. Imai, "Quantum quasi-cyclic LDPC codes," in *Proceedings of the 2007 IEEE International Symposium on Information Theory*, Nice, France, June 2007, pp. 806–810, arXiv:quant-ph/0701020.
- [57] T. Camara, H. Ollivier, and J.-P. Tillich, "A class of quantum LDPC codes: construction and performances under iterative decoding," in *Proceedings of the 2007 International Symposium on Information Theory*, Nice, France, June 2007, pp. 811–815.
- [58] M.-H. Hsieh, T. A. Brun, and I. Devetak, "Entanglement-assisted quantum quasicyclic low-density parity-check codes," *Physical Review A*, vol. 79, no. 3, p. 032340, March 2009.
- [59] P. Tan and J. Li, "Efficient quantum stabilizer codes: LDPC and LDPC-convolutional constructions," *IEEE Transactions on Information Theory*, vol. 56, no. 1, pp. 476–491, January 2010.
- [60] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, "Quantum error correction beyond the bounded distance decoding limit," July 2010, arXiv:1007.1778.
- [61] Y. Fujiwara, D. Clark, P. Vandendriessche, M. D. Boeck, and V. D. Tonchev, "Entanglement-assisted quantum low-density parity-check codes," 2010, arXiv:1008.4747.
- [62] B. Shaw, M. M. Wilde, O. Oreshkov, I. Kremsky, and D. Lidar, "Encoding one logical qubit into six physical qubits," *Physical Review A*, vol. 78, p. 012337, 2008.
- [63] M. M. Wilde and D. Fattal, "Nonlocal quantum information in bipartite quantum error correction," *Quantum Information Processing*, vol. 9, no. 5, pp. 591–610, September 2009.
- [64] M. M. Wilde and M.-H. Hsieh, "Entanglement generation with a quantum channel and a shared state," in *Proceedings of the 2010 IEEE International Symposium on Information Theory*, Austin, Texas, USA, June 2010, pp. 2713–2717.
- [65] Y. Dong, X. Deng, M. Jiang, Q. Chen, and S. Yu, "Entanglement-enhanced quantum error-correcting codes," *Physical Review A*, vol. 79, no. 4, p. 042342, April 2009.
- [66] J. Preskill, *Lecture Notes on Quantum Computation*, 1999, ch. Quantum Error Correction (Chapter 7), pp. 15–16. [Online]. Available: <http://www.theory.caltech.edu/people/preskill/ph229/notes/chap7.pdf>
- [67] D. Kribs, R. Laflamme, and D. Poulin, "Unified and generalized approach to quantum error correction," *Physical Review Letters*, vol. 94, no. 18, p. 180501, 2005.
- [68] D. W. Kribs, R. Laflamme, D. Poulin, and M. Lesosky, "Operator quantum error correction," *Quantum Information & Computation*, vol. 6, pp. 383–399, 2006.
- [69] D. Poulin, "Stabilizer formalism for operator quantum error correction," *Physical Review Letters*, vol. 95, no. 23, p. 230504, 2005.
- [70] P. Aliferis and A. W. Cross, "Subsystem fault tolerance with the Bacon-Shor code," *Physical Review Letters*, vol. 98, no. 22, p. 220502, 2007.
- [71] I. Kremsky, M.-H. Hsieh, and T. A. Brun, "Classical enhancement of quantum-error-correcting codes," *Physical Review A*, vol. 78, no. 1, p. 012341, 2008.
- [72] I. Devetak and P. W. Shor, "The capacity of a quantum channel for simultaneous transmission of classical and quantum information," *Communications in Mathematical Physics*, vol. 256, pp. 287–303, 2005.
- [73] M. M. Wilde and T. A. Brun, "Unified quantum convolutional coding," in *Proceedings of the IEEE International Symposium on Information Theory*, Toronto, Ontario, Canada, July 2008, pp. 359–363, arXiv:0801.0821.
- [74] J.-P. Tillich and G. Zémor, "Quantum LDPC codes with positive rate and minimum distance proportional to $n^{1/2}$," in *Proceedings of the 2009 IEEE International Symposium on Information Theory*, Seoul, Korea, June 2009, pp. 799–803.
- [75] M.-H. Hsieh, W.-T. Yen, and L.-Y. Hsu, "Performance of entanglement-assisted quantum LDPC codes constructed from finite geometries," June 2009, arXiv:0906.5532.
- [76] H. Jin and R. J. McEliece, "Coding theorems for turbo code ensembles," *IEEE Transactions on Information Theory*, vol. 48, no. 6, pp. 1451–1461, June 2002.
- [77] A. S. Barbulescu and S. S. Pietrobon, "Interleaver design for turbo codes," *Electronics Letters*, vol. 30, no. 25, pp. 2107–2108, December 1994.
- [78] S. Dolinar and D. Divsalar, "Weight distribution for turbo codes using random and nonrandom permutations," *JPL Progress report*, vol. 42, no. 122, pp. 56–65, August 1995.
- [79] J. Yuan, B. Vucetic, and W. Feng, "Combined turbo codes and interleaver design," *IEEE Transactions on Communications*, vol. 47, no. 4, pp. 484–487, April 1999.
- [80] H. R. Sadjadjpour, N. J. A. Sloane, M. Salehi, and G. Nebe, "Interleaver design for turbo codes," *IEEE Journal on Selected Areas in Communications*, vol. 19, no. 5, pp. 831–837, May 2001.