Belief Propagation with Quantum Messages for Symmetric Classical-Quantum Channels

S. Brandsen, Avijit Mandal, and Henry D. Pfister

***Abstract*—Belief propagation (BP) is a classical algorithm that approximates the marginal distribution associated with a factor graph by passing messages between adjacent nodes in the graph. It gained popularity in the 1990's as a powerful decoding algorithm for LDPC codes. In 2016, Renes introduced a belief propagation with quantum messages (BPQM) and described how it could be used to decode classical codes defined by tree factor graphs that are sent over the classical-quantum pure-state channel. In this work, we propose an extension of BPQM to general binary-input symmetric classical-quantum (BSCQ) channels based on the implementation of a symmetric "paired measurement". While this new paired-measurement BPQM (PMBPQM) approach is suboptimal in general, it provides a concrete BPQM decoder can be implemented with local operations. Finally, we demonstrate that density evolution can be used to analyze the performance of PMBPQM on tree factor graphs. As an application, we compute noise thresholds of some LDPC codes with BPQM decoding for a class of BSCQ channels.**

I. Introduction

Low-density parity-check (LDPC) codes and iterative decoding were introduced by Gallager in 1960 [1] but they did not attract widespread interest until the introduction of Turbo codes [2] and the rediscovery of LDPC codes [3] four decades later. Belief propagation (BP), in its general form, was introduced by Pearl in 1982 [4] as an efficient algorithm to exactly compute marginals for tree-structured probability models. BP works by passing messages between neighboring nodes and it was subsequently shown that BP includes both Gallager's iterative decoding and turbo decoding as special cases [5], [6].

Starting in the 1990s, there has been a growing interest in generalizing concepts from classical coding to the case of classical quantum (CQ) channels. Holevo, Schumaker, and Westmoreland identified the maximum rate of classical information transfer over a CQ channel [7]. Subsequent works described code constructions and decoding strategies that achieve this optimal rate [8], [9]. At the same time, advances in photonic communication underscored the need for developing low-complexity decoding protocols [10], [11], [12], [13]. In particular, there is a significant gap between the information rate achievable by a receiver with individual pulse-by-pulse detection and the rate possible with optimal joint quantum receiver (i.e., measurement of the full output system) if the mean number of photons per received optical pulse is smaller than one.

A key question is whether generalizations of BP can also be used to efficiently decode codes transmitted over CQ channels. Just as direct computation of the marginal probability distribution is computationally infeasible for large factor graphs in the classical case, it is experimentally infeasible to naively implement the optimal (Helstrom) measurement for decoding a code defined by a large factor graph. This is because it would require many quantum operations involving all the qubits. The idea of generalizing BP to decode a classical binary code transmitted over a CQ channel was introduced by Renes [14] and it offers an alternative to experimentally infeasible collective measurements. The described approach is restricted to the pure-state channel (PSC) and codes whose Tanner graphs are trees. It is described based on a channel-combining perspective that also adopted in this work. Following [15], we will refer to this general decoding method as belief-propagation with quantum messages (BPQM). In [15], simulation results are presented for a simple 5-bit code (whose Tanner graph is a tree) and compared to a classical decoding approach. For the 5-bit code, it is observed in [15] (and proved in [16]) that bit-optimal decoding is actually block optimal in this context. However, this version of BPQM had exponential complexity due to the need for controlled unitary operations which grow with the size of the tree.

Piveteau and Renes significantly advanced the understanding of BPQM in [17], where they prove that BPQM is simultaneously optimal both for bit-error probability and block-error probability for binary linear codes with tree factor graphs on the PSC. They additionally reduce the overall decoding complexity from exponential to quadratic by introducing the idea of using a quantum reliability register for each qubit message.

In this work, we introduce a paired-measurement BPQM (PMBPQM) protocol which is the first extension of BPQM to more general symmetric binary-input CQ (BSCQ) channels. This extension is based on a lemma that shows any BSCQ channel can be approximated by an orthogonal mixture of BSCQ channels that output a single qubit. In some ways, this is similar to the fact that any symmetric binary-input classical channel can be represented as a stochastic mixture of binary symmetric channels (BSCs). For classical bit-flip channels, it is easy to verify that PMBPQM is optimal and we also demonstrate that it is optimal for the pure-state channel.

For more general BSCQ channels, we also have an example (see [18]) that shows *any* approach involving binary-outcome measurements will be suboptimal relative to the collective Helstrom success probability. However, by comparing the performance of PMBPQM to the Helstrom measurement for a variety of factor graphs with up to 13 qubits, we observe that PMBPQM is near optimal for the chosen instances. One interesting open question is "What is the worst-case gap between

PMBPQM and the collective Helstrom measurement?".

We also analyze the performance of PMBPQM for large factor graphs by deriving its density evolution equations. Density evolution, which was formalized in [19], is an asymptotic analysis method that can be used to find noise thresholds for BP decoding of long LDPC codes sent through symmetric channels. For LDPC codes on CQ channels with optimal Helstrom decoding, there are no currently known methods for computing channel noise thresholds. We demonstrate that PMBPQM lends itself to asymptotic analysis and characterize the region of channel parameters for a qubit BSCQ channel such that asymptotically reliable decoding is achievable via PMBPQM.

II. Notation

We define the set of natural numbers by $\mathbb{N} = \{1, 2, \ldots\}$ and use the shorthand $[m] \coloneqq \{1, \ldots, m\}$ for $m \in \mathbb{N}$. We denote the n-dimensional complex Hilbert space by $\mathcal{H}_n$ and write the i-th element of the standard basis of $\mathcal{H}_n$ as $|i\rangle$ for $i \in \{0, 1, \ldots, n-1\}$. A pure quantum state, $|\psi\rangle \in \mathcal{H}_n$, is an n-dimensional complex vector. The Hermitian transpose of $|\phi\rangle \in \mathcal{H}_n$ is denoted either by $|\phi\rangle^\dagger$ or $\langle\phi|$. The inner product between $|\psi\rangle$ and $|\phi\rangle$ is denoted by $\langle\phi|\psi\rangle \coloneqq |\phi\rangle^* |\psi\rangle$ and all pure states are normalized such that $|\langle\psi|\psi\rangle| = 1$.

A stochastic mixture of pure states is called a mixed state. Consider a random pure state defined by $\{p_i, |\psi_i\rangle\}_{i\in[m]}$ which takes value $|\psi_i\rangle$ with probability p_i. The associated mixed state is represented by the density matrix $\rho = \sum_{i=0}^{m-1} p_i |\psi_i\rangle\langle\psi_i|$, which is a positive semidefinite matrix with unit trace. Let $\mathcal{D}(\mathcal{H}_n)$ denote the set of density matrices (i.e., positive semidefinite $n \times n$ complex matrices with unit trace). When the value of n is not important, we will use $\mathcal{H}$ to denote the Hilbert space and $\mathcal{D}(\mathcal{H})$ to represent the set of density matrices.

Finally, we denote with $\mathcal{B}(\mathcal{H}_n)$ the set of positive semidefinite $n \times n$ complex matrices with bounded (not necessarily unit) trace. A quantum measurement on an n-dimensional quantum system is then represented by $\hat{\Pi} = \{\Pi_j\}|_{j=1}^m$ where each element $\Pi_j \in \mathcal{B}(\mathcal{H}_n)$ and $\sum_{j=1}^m \Pi_j = \mathbb{I}_n$.

A. Classical Quantum Channels

Definition 1. A BSCQ channel, $W\colon \{0,1\} \to \mathcal{D}(\mathcal{H}_n)$, maps classical input $z \in \{0,1\}$ to the density matrix output $W(z) \in \mathcal{D}(\mathcal{H}_n)$ such that the symmetry constraint $W(1) = UW(0)U$ for $U^2 = \mathbb{I}$ is satisfied. If $n = 2$, then the output lives in a 2-dimensional Hilbert space and we call this a *qubit channel*.

Definition 2. A minimum-error measurement $\hat{\Pi} = \{\Pi_j\}|_{j=1}^m$ for a given set of candidate states $\{\rho_j\}|_{j=1}^m$ with corresponding probabilities $p_j = \Pr(\rho = \rho_j)$ is a measurement that maximizes the probability of correct detection,

$$\sum_{j=1}^{m} p_j \mathrm{Tr}[\Pi_j \rho_j].$$

Definition 3. The Helstrom measurement is a minimum-error measurement for a given binary state set $\{\rho_+, \rho_-\}$ with corresponding probabilities $\{p, 1-p\}$. It is defined by projectors onto the positive and negative eigenspaces of the matrix $p\rho_+ - (1-p)\rho_-$ [20]. We denote the corresponding success probability as $P_{\mathrm{H}}(\rho_+, \rho_-, p)$.

III. Paired-Measurement BPQM

A. Representation of Symmetric CQ Channels

Lemma 4. *Any qubit BSCQ channel is unitarily equivalent to* $W\colon \{0,1\} \to \mathcal{D}(\mathcal{H}_2)$ *satisfying* $W(z) = \sigma_{\mathrm{x}}^z \rho(\theta, p) \sigma_{\mathrm{x}}^z$ *with*

$$\rho(\theta, p) \coloneqq \sigma_{\mathrm{x}}^z \Big((1-p) H |\theta\rangle\langle\theta| H^\dagger + \frac{p}{2}\mathbb{I} \Big) \sigma_{\mathrm{x}}^z,$$

where H *is the Hadamard operator and* $|\theta\rangle \coloneqq \cos(\frac{\theta}{2})|0\rangle + \sin(\frac{\theta}{2})|1\rangle$.

Proof: See [18]. ∎

We now introduce a "paired measurement" that processes the outputs of an arbitrary BSCQ channel into an orthogonal combination of qubit BSCQ channels. This illustrates the symmetry of collective Helstrom measurement. It is also one part of PMBPQM, which uses bit-node and check-node combining in concert with sequential applications of paired measurement.

Definition 5. For a BSCQ channel $W(z) = U^z \rho U^z$ with $\rho \in \mathcal{D}(\mathcal{H}_{2n})$, let $\{|v_j\rangle\}|_{j=1}^n$ be n orthogonal eigenvectors of $W(0) - W(1)$ with non-negative eigenvalues $\{\lambda_j\}|_{j=1}^n$ satisfying $(W(0) - W(1))U|v_j\rangle = -\lambda_j U|v_j\rangle$ and $U|v_j\rangle \perp |v_j\rangle$. The existence of such a set is established in Lemma 6 and the *paired measurement* for W is defined to be

$$\hat{\Pi}_W \coloneqq \Big\{ |v_j\rangle\langle v_j| + U|v_j\rangle\langle v_j|U \Big\}\Big|_{j=1}^n.$$

Lemma 6. *Consider the task of distinguishing between equiprobable outputs of a BSCQ channel* $\{W(0), W(1)\}$. *Then, the optimal Helstrom measurement* $\hat{\Pi}_H$ *for this channel is equivalent to first implementing the paired measurement for* W *and then using its outcome,* j, *to select the second measurement,* $\hat{\Pi}_W(j) = \{ |v_j\rangle\langle v_j|, U|v_j\rangle\langle v_j|U \}$.

Proof: Define $M \coloneqq \rho - U\rho U$ and let $|v_j\rangle$ be an eigenvector of M with eigenvalue λ_j. Then, $U|v_j\rangle$ is an eigenvector with eigenvalue $-\lambda_j$ because

$$\begin{aligned} M(U|v_j\rangle) &= (\rho U - U\rho)|v_j\rangle = U(U\rho U - \rho)|v_j\rangle \\ &= -UM|v_j\rangle = -\lambda_j U|v_j\rangle. \end{aligned}$$

The Helstrom measurement is determined by the positive and negative eigenspaces of M. Thus, one can choose an orthonormal basis $\{|v_j\rangle\}|_{j=1}^n$ for the n largest eigenvalues $\{\lambda_j\}|_{j=1}^n$ such that $\langle v_j|U|v_j\rangle = 0$ and the Helstrom measurement is given by

$$\hat{\Pi}_H = \left\{ \sum_{j=1}^{n} |v_j\rangle\langle v_j|, \sum_{j=1}^{n} U|v_j\rangle\langle v_j|U \right\}.$$

For the case where 0 is an eigenvalue of M, the corresponding eigenvectors can be grouped arbitrarily into these two projectors without affecting the error probability. However, the existence of the paired measurement decomposition requires a longer argument and this is given in [18]. ∎

Lemma 7. *For a BSCQ channel $W\colon \{0,1\} \to \mathcal{D}(\mathcal{H}_{2n})$ with equiprobable inputs, the channel W followed by paired measurement $\hat{\Pi}_W$ is equivalent to a BSCQ which defines the classical mixture of symmetric qubit channels given by*

$$\tilde{W}(z) = \sum_{i=0}^{n} p_i \Big(\sigma_{\mathrm{x}}^z \rho_i \sigma_{\mathrm{x}}^z \otimes |i\rangle\langle i| \Big).$$

From this, we see that the j-th paired outcome has probability $p_j = \mathrm{Tr}\big[\big(|v_j\rangle\langle v_j| + U |v_j\rangle\langle v_j| U\big)\rho\big]$ and results in a post-measurement density matrix equivalent to

$$\rho_j = \frac{1}{p_j} \begin{pmatrix} \langle v_j| \rho |v_j\rangle & \langle v_j| U\rho |v_j\rangle \\ \langle v_j| \rho U |v_j\rangle & \langle v_j| U\rho U |v_j\rangle \end{pmatrix}.$$

Proof: See [18]. ∎

B. Channel Combining for Bit and Check Nodes

The following definitions of bit-node and check-node combining can be found in [21] and are straightforward generalizations of classical definitions for LDPC codes. Since these operations preserve channel symmetry, the paired-measurement can also be applied to the combined channels.

Definition 8. For CQ channels W, W', the bit-node and check-node channel combining operations are defined by

$$[W \circledast W'](z) \coloneqq W(z) \otimes W'(z)$$
$$[W \boxast W'](z) \coloneqq \frac{1}{2} \sum_{z' \in \{0,1\}} W(z \oplus z') \otimes W'(z').$$

Lemma 9. *If W, W' are symmetric CQ channels, then $W \circledast W'$ and $W \boxast W'$ are symmetric CQ channels.*

Proof: See [18]. ∎

C. Optimality of PMBPQM for Pure State Channels (PSC)

We show that implementing paired-measurements before bit- and check-node combining is equivalent on PSCs to the BPQM method outlined in [14], [15]. Given that a coherent implementation of this BPQM method has been proven to be optimal for PSCs [17], it follows that paired-measurement BPQM is likewise optimal for PSCs. First, we define the canonical PSC W_θ.

Definition 10. The canonical pure state channel (PSC), W_θ, maps binary input $z \in \{0,1\}$ to $W_\theta(z) = \sigma_{\mathrm{x}}^z (H |\theta\rangle\langle\theta| H^\dagger) \sigma_{\mathrm{x}}^z$.

Now, we show that using paired-measurement BPQM after check combining is equivalent to coherent BPQM check node combining [14] via applying $\mathrm{CNOT}_{1\to 2}$.

Lemma 11. *Implementing the paired-measurement to distinguish between $[W_\theta \boxast W_{\theta'}](0)$ and $[W_\theta \boxast W_{\theta'}](1)$ is unitarily equivalent to implementing*

$$\mathit{CNOT}_{1\to 2}[W_\theta \boxast W_{\theta'}](z)\mathit{CNOT}_{1\to 2} = \sum_{j\in\{0,1\}} p_j \left|(-1)^z \theta_j^{\boxast}\right\rangle\!\left\langle(-1)^z \theta_j^{\boxast}\right| \otimes |j\rangle\langle j|,$$

where $p_0 = \frac{1}{2}(1 + \cos(\theta)\cos(\theta'))$, $p_1 = 1 - p_0$, $\cos(\theta_0^{\boxast}) = \frac{\cos(\theta)+\cos(\theta')}{1+\cos(\theta)\cos(\theta')}$, and $\cos(\theta_1^{\boxast}) = \frac{\cos(\theta)-\cos(\theta')}{1-\cos(\theta)\cos(\theta')}$.

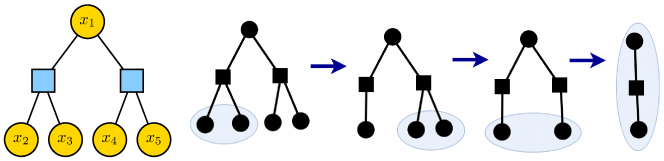

Figure 1: The left side shows the five-qubit factor-graph. The right side depicts paired-measurement BPQM for the five-qubit factor-graph, where each stage of paired-measurement BPQM merges two qubits into one new qubit.

Proof: The difference matrix is given by

$$[W_\theta \boxast W_{\theta'}](0) - [W_\theta \boxast W_{\theta'}](1) = 2\sin(\tfrac{\theta}{2})\cos(\tfrac{\theta}{2})\sin(\tfrac{\theta'}{2})\cos(\tfrac{\theta'}{2}) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The optimal choice of paired measurement is defined by $|\tilde{v}_0\rangle = \frac{1}{\sqrt{2}}(1,0,0,1)$ and $|\tilde{v}_1\rangle = \frac{1}{\sqrt{2}}(-1,0,0,1)$ with respective eigenvalues of $\pm 2\sin(\theta)\cos(\theta)\sin(\theta')\cos(\theta')$. The probability of obtaining outcome $\Pi_0 = |\tilde{v}_0\rangle\langle\tilde{v}_0| + U |\tilde{v}_0\rangle\langle\tilde{v}_0| U$ is $p_0 = \frac{1}{2}(1 + \cos(\theta)\cos(\theta'))$ for symmetry operator $U = \sigma_{\mathrm{x}} \otimes \mathbb{I}$. The corresponding post-measurement state for outcome $i \in \{0,1\}$ is given by

$$\tilde{\rho}(i,z) = \sigma_{\mathrm{x}}^z H \left|-\theta_i^{\boxast}\right\rangle\!\left\langle-\theta_i^{\boxast}\right| H^\dagger \sigma_{\mathrm{x}}^z.$$ ∎

Using [14], we can similarly demonstrate unitary equivalence of paired-measurement for bit-node combining to the coherent BPQM operation. First, we define

$$U_{\circledast}(\theta,\theta') \coloneqq \begin{pmatrix} a_+ & 0 & 0 & a_- \\ a_- & 0 & 0 & -a_+ \\ 0 & b_+ & b_- & 0 \\ 0 & b_- & -b_+ & 0 \end{pmatrix},$$
$$a_\pm \coloneqq \frac{1}{\sqrt{2}} \left(\frac{\cos\left(\frac{\theta-\theta'}{2}\right) \pm \cos\left(\frac{\theta+\theta'}{2}\right)}{\sqrt{1+\cos(\theta)\cos(\theta')}} \right),$$
$$b_\pm \coloneqq \frac{1}{\sqrt{2}} \left(\frac{\sin\left(\frac{\theta+\theta'}{2}\right) \mp \sin\left(\frac{\theta-\theta'}{2}\right)}{\sqrt{1-\cos(\theta)\cos(\theta')}} \right).$$

Lemma 12. *Implementing the paired-measurement to distinguish between $[W_\theta \circledast W_{\theta'}](0)$ and $[W_\theta \circledast W_{\theta'}](1)$ is unitarily equivalent to*

$$U_{\circledast}(\theta,\theta')[W_\theta \circledast W_{\theta'}](z) U_{\circledast}(\theta,\theta')^\dagger \coloneqq \left|(-1)^z \theta^{\circledast}\right\rangle\!\left\langle(-1)^z \theta^{\circledast}\right|,$$

where $\cos(\theta^{\circledast}) = \cos(\theta)\cos(\theta')$.

Proof: See [18]. ∎

IV. Results for the Five-Qubit Factor Graph

A. Decoding on General BSCQ Channels

Now, consider a qubit BSCQ W which is neither a pure state channel nor a purely classical channel. Specifically, we consider the channel family defined by

$$W(z) = (1-p) H |(-1)^z\theta\rangle\langle(-1)^z\theta| H^\dagger + pH \left|(-1)^{z\oplus 1}\theta\right\rangle\!\left\langle(-1)^{z\oplus 1}\theta\right| H^\dagger \quad (1)$$

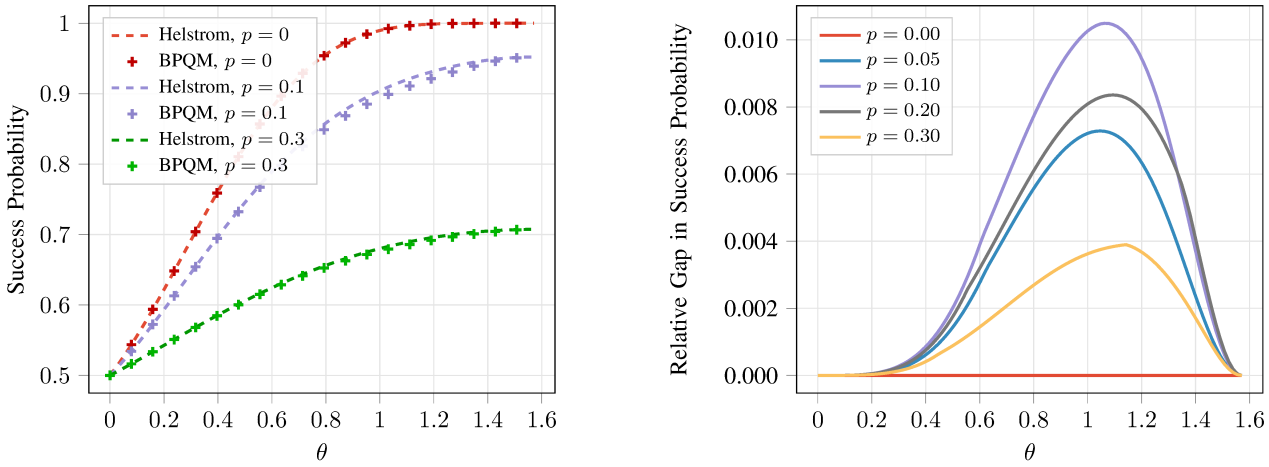

Figure 2: Left hand side depicts success probability for both the Helstrom and paired-measurement BPQM approach as a function of θ for $p \in \{0, 0.1, 0.3\}$. Right hand side depicts relative difference in success probability between the Helstrom and paired-measurement BPQM approach (i.e. $\frac{P_{\text{helstrom}} - P_{\text{BPQM}}}{P_{\text{helstrom}}}$) as a function of θ for $p \in \{0, 0.05, 0.1, 0.2, 0.3\}$.

and observe that $W(z) = U^z \rho U^z$ for $\rho = W(0)$ and $U = \sigma_{\text{x}}$. PMBPQM enables message-passing decoding for general BSCQ channels. Here, we plot simulation results for PMBPQM for the root node of the 5-qubit factor graph with parity checks $x_1 \oplus x_2 \oplus x_3 = 0$ and $x_1 \oplus x_4 \oplus x_5 = 0$ depicted in Figure 1. We note that one can coherently decode all of the bits by adopting the message-passing framework introduced in [17] which introduces a quantum register to store the reliability of the message.

For the five-qubit factor-graph, the PMBPQM approach consists of the following steps:

1) Implementing paired measurement on qubits 2 and 3 for $W \circledast W$ to get outcome a and post-measurement state $\tilde{\rho}(a, z)$
2) Implementing paired measurement on qubits 4 and 5 for $W \circledast W$ to get outcome b and post-measurement state $\tilde{\rho}(b, z)$
3) Implementing paired measurement for $\tilde{\rho}(a, z) \otimes \tilde{\rho}(b, z)$; obtain measurement outcome c and post-measurement state $\tilde{\rho}(c, z)$
4) Measuring $\tilde{\rho}(c, z)$ and qubit 1 through Helstrom measurement for $\{W(0) \otimes \tilde{\rho}(c, 0), W(1) \otimes \tilde{\rho}(c, 1)\}$

This process is depicted in Figure 1. We then generate success probabilities for the five-qubit factor-graph using both a paired-measurement BPQM approach and a collective Helstrom measurement respectively. The left hand side of Figure 2 shows the overall success probability of both approaches, while the right hand side of Figure 2 plots their relative difference. We observe that the relative difference is small for all choices of channel parameters (θ, p) and in the special case of a PSC ($p = 0$), there is no relative difference.

We have also considered the "worst case" gap between paired-measurement BPQM and the collective Helstrom measurement. For the tested cases, the worst case gap is relatively small and the paired-measurement BPQM is either optimal or close-to-optimal in all cases. We also tested that PMBPQM outperforms the naive locally-greedy taht first measures and the performs classical BP. This is discussed further in [18] where we demonstrate that a small gap between local measurement strategies and the collective Helstrom will also occur with any approach using semi-local binary-output measurements. Namely, there exists an example where no local measurement approach or extension of BPQM can achieve the optimal Helstrom success probability.

Lemma 13. *Consider a tree factor graph for a binary linear code where all bits are sent through CQ channels. When the root bit has value $z \in \{0, 1\}$, we denote the density matrix of the observations by ρ_z. Let $P_{LM}(\rho_0, \rho_1)$ be the optimal success probability for decoding algorithms that start from the bottom of the tree and, in each round, measure a single check node or bit node is conditional on all previous measurement results. Then, there are CQ channels where*

$$P_{LM}(\rho_0, \rho_1) < P_H\left(\rho_0, \rho_1, \tfrac{1}{2}\right).$$

Proof: See [18]. ∎

V. Density Evolution

Density evolution is an technique that allows one to analyze the asymptotic performance of a given code ensemble with BP decoding by tracking the probability density function of messages that are passed along edges of a factor graph [22]. Density evolution thus determines whether a given channel and degree distribution leads to asymptotically reliable decoding. In turn, this enables the construction and optimization of low-density parity-check (LDPC) codes that achieve reliable communication at rates close to the channel capacity.

While there is no currently known method to analyze the performance of general protocols such as the collective Helstrom measurement, we demonstrate here that it is possible to extend density evolution to provide an asymptotic analysis (via Monte Carlo simulation) of PMBPQM. Such a method is possible because each the paired measurement operation allows the result of bit- and check-node combining to be viewed as a new single-qubit BSCQ channel. Thus, the paired

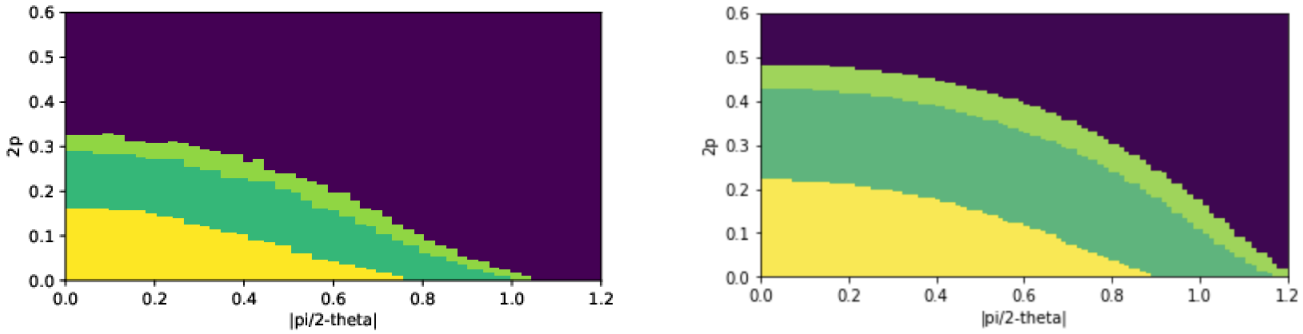

Figure 3: The left diagram shows a heat map depicting the noise threshold for LDPC codes on (1) as a function of $|\frac{\pi}{2} - \theta|$ and $q = 2p$ (where p is the bit flip probability for a BSC). Yellow indicates channel parameter pairs that are below the noise threshold for the (3,6) code. Dark green and light green indicate the same for the (3,4) and (4,5) codes respectively. Dark purple indicates channel parameters that are above the noise threshold for all tested code structures. On the right, we see a corresponding diagram for the Holevo bounds of the associated code rates, $\{0.2, 0.25, 0.5\}$.

measurements can be iteratively performed up the tree and the threshold can be found by tracking the channel parameters after a large number of channel combining iterations.

We begin by describing bit- and check-node combining operations for higher-degree bit and check nodes. First, we consider the case where the bit node has degree d_v and the check node has degree d_c, and where for each node the channel corresponding to the j^{th} qubit is denoted as $W^{(j)}$. The steps are then given by:

1) For $j \in \{1, \ldots, \lfloor \frac{d_v}{2} \rfloor\}$, execute paired measurement $\{[W^{(2j-1)} \circledast W^{(2j)}](0), [W^{(2j-1)} \circledast W^{(2j)}](1)\}$ to get post-measurement channels $\{W^{(12)}, \ldots, W^{(d_v-1, d_v)}\}$ (or $W^{(d_v-1)}$ if d_v is odd)
2) Repeat the above step with the post-measurement channel set to form the new set $\{W^{(1234)}, W^{(5678)}, \ldots\}$, etc.
3) Repeat until only a single post-measurement qubit remains with effective channel $\tilde{W}$
4) Implement a final paired measurement for $\tilde{W} \circledast W$

For a check node, the steps are analogous (with bit-node combining replaced by check-node combining) except there is no additional combining with W (in the 4th step).

Density evolution works by tracking the distribution of the PMBPQM qubit channels. This is implemented using a Monte Carlo process sometimes called population dynamics (see [18] for details). For a depth-N LDPC code tree corresponding to a factor graph with alternating bit and check layers, and bit nodes are degree d_v and check nodes are degree d_c. We suppose that all bits are initially sent separately through the BSCQ channel $W_{\theta,p}(z) = (1-p)\,|(-1)^z\theta\rangle\langle(-1)^z\theta| + p\frac{\mathbb{I}}{2}$.

The following method is used for density evolution:

1) Create multiset $\mathcal{S} = \{(\theta, p)\}|_{k=1}^{M}$ with $M = 5000$ copies of the channel parameters and initialize multiset $\mathcal{S}' = \emptyset$
2) For j in $\{1, 2, \ldots, N\}$:
   a) Randomly draw (θ, q) and (θ', q') from $\mathcal{S}$
   b) If j is odd, implement iterative paired measurements for the check node until all d_c qubits are condensed to a single post-measurement qubit state $\tilde{\rho}(j, z) = (1 - q_j)\,|(-1)^z\theta_j\rangle\langle(-1)^z\theta_j| + q_j\frac{\mathbb{I}}{2}$
   c) If j is even, implement iterative paired measurements for the check node until all d_v qubits and the parent qubit (with parameters (θ, q)) are condensed to a single post-measurement qubit state, $\tilde{\rho}(j, z) = (1 - q_j)\,|(-1)^z\theta_j\rangle\langle(-1)^z\theta_j| + q_j\frac{\mathbb{I}}{2}$
   d) Add the new channel parameters (θ_j, q_j) to $\mathcal{S}'$
   e) Repeat 2a-2d until $\mathcal{S}'$ has M elements, set $\mathcal{S} = \mathcal{S}'$
3) The overall success probability is the average over $(\theta, q) \in \mathcal{S}$ of the success probability for distinguishing between $(1-q)\,|\theta\rangle\langle\theta| + q\frac{\mathbb{I}}{2}$ and $(1-q)\,|-\theta\rangle\langle-\theta| + q\frac{\mathbb{I}}{2}$

We say (θ, q) is below the noise threshold if the success probability for the root bit approaches 1 as $N \to \infty$.

VI. Conclusions

We introduce a paired-measurement BPQM protocol that extends BPQM to the case of BSCQ channels. This protocol reduces to BP for classical symmetric channels and matches the known (optimal) BPQM protocol for the pure-state channel. For more general BSCQ channels, we show that PMBPQM is performs well in all tested instances. We also consider the application of PMBPQM to large factor graphs by using asymptotic analysis techniques. Based on Monte Carlo density evolution, we plot the region of channel parameters for which PMBPQM achieves asymptotically reliable decoding for a few different regular LDPC codes on BSCQ channels. The introduction of PMBPQM naturally leads to interesting open questions about the "worst case" gap between paired-measurement BPQM and the collective Helstrom measurement; as well as whether there exists an extension of BPQM that is optimal for general BSCQ channels.

VII. Acknowledgments

The authors would like to thank Narayanan Rengaswamy, Joseph Renes, and Saikat Guha for helpful discussions. This work was supported in part by the National Science Foundation (NSF) under Grants No. 1908730 and 1910571. Any opinions, findings, conclusions, and recommendations expressed in this material are those of the authors and do not necessarily reflect the views of these sponsors.

REFERENCES

[1] R. G. Gallager, *Low-Density Parity-Check Codes*. PhD thesis, M.I.T., Cambridge, MA, USA, 1960.

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

[3] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, pp. 399–431, March 1999.

[4] J. Pearl, "Reverend Bayes on inference engines: A distributed hierarchical approach," in *AAAI Conf. Artificial Intelligence*, 1982.

[5] R. J. McEliece, D. J. C. MacKay, and J. Cheng, "Turbo decoding as an instance of Pearl's "belief propagation" algorithm," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 140–152, Feb. 1998.

[6] F. R. Kschischang and B. J. Frey, "Iterative decoding of compound codes by probability propagation in graphical models," *IEEE J. Select. Areas Commun.*, vol. 16, no. 2, pp. 219–230, 1998.

[7] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A*, vol. 56, pp. 131–138, Jul 1997.

[8] M. M. Wilde and S. Guha, "Polar codes for classical-quantum channels," *IEEE Transactions on Information Theory*, vol. 59, pp. 1175–1187, Feb 2013.

[9] V. Giovannetti, S. Lloyd, and L. Maccone, "Achieving the holevo bound via sequential measurements," *Physical Review A*, vol. 85, Jan 2012.

[10] A. Jagannathan, M. Grace, O. Brasher, J. H. Shapiro, S. Guha, and J. L. Habif, "Demonstration of quantum-limited discrimination of multicopy pure versus mixed states," *Phys. Rev. A*, vol. 105, p. 032446, Mar 2022.

[11] Q. Zhuang, Z. Zhang, and J. H. Shapiro, "Optimum mixed-state discrimination for noisy entanglement-enhanced sensing," *Phys. Rev. Lett.*, vol. 118, p. 040801, Jan 2017.

[12] M. P. da Silva, S. Guha, and Z. Dutton, "Achieving minimum-error discrimination of an arbitrary set of laser-light pulses," *Physical Review A*, vol. 87, may 2013.

[13] S. Guha, "Structured optical receivers to attain superadditive capacity and the holevo limit," *Phys. Rev. Lett.*, vol. 106, p. 240502, Jun 2011.

[14] J. M. Renes, "Belief propagation decoding of quantum channels by passing quantum messages," *New Journal of Physics*, vol. 19, no. 7, p. 072001, 2017.

[15] N. Rengaswamy, K. P. Seshadreesan, S. Guha, and H. D. Pfister, "Quantum advantage via qubit belief propagation," in *Proc. IEEE Int. Symp. Inform. Theory*, pp. 1824–1829, 2020.

[16] N. Rengaswamy, K. P. Seshadreesan, S. Guha, and H. D. Pfister, "Belief propagation with quantum messages for quantum-enhanced classical communications," *npj Quantum Information*, vol. 7, no. 1, pp. 1–12, 2021.

[17] C. Piveteau and J. M. Renes, "Quantum message-passing algorithm for optimal and efficient decoding," *arXiv preprint arXiv:2109.08170*, 2021.

[18] S. Brandsen, A. Mandal, and H. D. Pfister, "Belief propagation with quantum messages for symmetric classical-quantum channels," *extended version to be submitted to arXiv.*

[19] T. J. Richardson and R. L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inform. Theory*, vol. 47, pp. 599–618, Feb. 2001.

[20] C. W. Helstrom, "Quantum detection and estimation theory," *Journal of Statistical Physics*, vol. 1, no. 2, pp. 231–252, 1969.

[21] J. M. Renes, "Duality of channels and codes," *IEEE Trans. Inform. Theory*, vol. 64, no. 1, pp. 577–592, 2018.

[22] T. J. Richardson and R. L. Urbanke, *Modern Coding Theory*. New York, NY: Cambridge University Press, 2008.