Belief-Propagation with Quantum Messages for Polar Codes on Classical-Quantum Channels

Avijit Mandal*, S. Brandsen†, and Henry D. Pfister*‡
Departments of Electrical and Computer Engineering*, Mathematics‡
Duke University†

***Abstract*—This paper considers the design and decoding of polar codes for general classical-quantum (CQ) channels. It focuses on decoding via belief-propagation with quantum messages (BPQM) and, in particular, the idea of paired-measurement BPQM (PM-BPQM) decoding. Since the PM-BPQM decoder admits a classical density evolution (DE) analysis, one can use DE to design a polar code for any CQ channel and then efficiently compute the trade-off between code rate and error probability. We have also implemented and tested a classical simulation of our PM-BPQM decoder for polar codes. While the decoder can be implemented efficiently on a quantum computer, simulating the decoder on a classical computer actually has exponential complexity. Thus, simulation results for the decoder are somewhat limited and are included primarily to validate our theoretical results.**

I. Introduction

The study of channel coding for CQ channels dates back to Holevo, Schumacher, and Westmoreland [1] and [2]. For a comprehensive introduction, see [3], [4]. This paper provides a detailed description of how to efficiently design (on a classical computer) and decode (on a quantum computer) polar codes for classical-quantum (CQ) channels. Practical applications motivating coding for CQ channels can be found in [5]–[7].

Polar codes for CQ channels were first introduced in 2012 [8]. A variety of follow-up papers were able to extend and improve these results [5], [9]–[11]. Although these papers describe a design and decoding process for polar codes on CQ channels in theory, efficient algorithms (e.g., polynomial time in the block length) are not described for either of these tasks.

In 2017, Renes describes a belief-propagation with quantum messages (BPQM) algorithm that provides an optimal decoding method for binary linear codes with tree factor graphs on the pure-state channel (PSC) [12]. That work notes that BPQM could allow efficient decoding of polar codes on the PSC. BPQM is further explored in [13] and extended to be more efficient by Renes and Piveteau in [14]. Recently, an extension of BPQM for general CQ channels was introduced and called paired-measurement BPQM (PM-BPQM) [15]. This algorithm can be applied to any symmetric binary-input CQ channel and is equipped with a classical DE analysis of its decoding performance. In [15], this DE analysis is used to compute noise thresholds for PM-BPQM decoding of low-density parity-check (LDPC) codes [16] on CQ channels.

This research was supported in part by the National Science Foundation (NSF) under Grants 1908730, 2106213, and 2212437. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the NSF.

In this paper, we use DE to design polar codes for PM-BPQM decoding and determine their achievable rates. We also report results for the classical simulation of our PM-BPQM decoder for polar codes. Although this decoder can be implemented efficiently on a quantum computer, directly simulating the decoder on a classical computer has exponential complexity in the block length. Thus, our simulation results are limited to very short block lengths and are included mainly to validate our DE results. Additional information can be found in an extended version of this paper [17].

II. Background

A. Preliminaries

We define the set of natural numbers by $\mathbb{N} = \{1, 2, \ldots\}$ and use the shorthand $[m] \coloneqq \{1, \ldots, m\}$ for $m \in \mathbb{N}$. Let $\mathcal{H}_n$ denote the n-dimensional Hilbert space $\mathbb{C}^n$. A quantum *pure state* is a unit length vector $|\psi\rangle \in \mathcal{H}_n$. For quantum systems $A_1, A_2 \ldots, A_n$, we denote the joint quantum state of n qubits, $|\psi\rangle_{A_1 A_2 \ldots A_n}$ where we follow the convention that the 1st qubit is associated with the system A_1, the 2nd qubit with A_2 and so on. When $|\psi\rangle_{A_1 A_2 \ldots A_n}$ is not entangled, we can use the Kronecker product to write the joint state as

$$|\psi\rangle_{A_1 A_2 \ldots A_n} = |\psi_1\rangle_{A_1} \otimes \ldots |\psi_n\rangle_{A_n}.$$

A random ensemble of m quantum pure states in $\mathcal{H}_n$ is denoted by $\Psi = \{p_i, |\psi_i\rangle\}|_{i=1}^m$, where p_i denotes the probability of choosing the pure state $|\psi_i\rangle$. This ensemble can also be represented by the *density matrix* $\rho = \sum_{i=1}^m p_i |\psi_i\rangle\langle\psi_i| \in \mathbb{C}^{n \times n}$. All such density matrices are positive semidefinite with unit trace and we use $\mathcal{D}(\mathcal{H}_n)$ to denote this subset. The unitary evolution of a quantum state $|\psi\rangle \in \mathcal{H}_n$ is described by the mapping $|\psi\rangle \mapsto U|\psi\rangle$, where $U \in \mathbb{C}^{n \times n}$ is a unitary. For the pure state ensemble Ψ, this evolution results in the modified ensemble $\Psi' = \{p_i, U|\psi_i\rangle\}|_{i=1}^m$ whose density matrix is

$$\rho' = \sum_{i=1}^m p_i U |\psi_i\rangle\langle\psi_i| U^\dagger = U \rho U^\dagger,$$

where $U^\dagger$ is the Hermitian transpose of U. We denote the Pauli matrices by

$$\sigma_x \coloneqq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_y \coloneqq \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \sigma_z \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Definition 1: A binary symmetric CQ (BSCQ) channel is defined by the mapping $W : \{0, 1\} \to \mathcal{D}(\mathcal{H}_n)$ from the binary classical input $z \in \{0, 1\}$ to the density matrix

978-1-6654-7554-9/23/$31.00 ©2023 IEEE

$W(z) \in \mathcal{D}(\mathcal{H}_n)$ of the quantum output and a unitary U satisfying $U^2 = \mathbb{I}$. The unitary defines the symmetry constraint via $W(1) = UW(0)U^\dagger$.

Lemma 2 ([18, Appendix A]): Any BSCQ channel that outputs a qubit is unitarily equivalent to the qubit channel $W : \{0,1\} \to \mathcal{D}(\mathcal{H}_2)$ satisfying $W(z) = \sigma_x^z \rho(\delta,\gamma)\sigma_x^z$ with

$$\rho(\delta,\gamma) \coloneqq \begin{bmatrix} \delta & \gamma^* \\ \gamma & 1-\delta \end{bmatrix}$$

for some $\delta \in [0,1]$ and $\gamma \in \mathbb{C}$ satisfying $|\gamma|^2 \leq \delta(1-\delta)$.

This representation enables one to characterize any qubit BSCQ channel using only two parameters δ and γ.

Definition 3: An m-outcome *projective measurement* of a quantum system in $\mathcal{H}_n$ is defined by a set of m orthogonal projection matrices $\Pi_j \in \mathbb{C}^{n\times n}$ satisfying $\Pi_i\Pi_j = \delta_{i,j}\Pi_i$ and $\sum_j \Pi_j = \mathbb{I}_n$, where $\mathbb{I}_n$ is the $n \times n$ identity matrix. We denote such a measurement by $\hat{\Pi} = \{\Pi_j\}|_{j=1}^m$.

Applying the measurement $\hat{\Pi}$ to the quantum state ρ results in a random outcome J and the probability of the event $J = j$ is given by $\mathrm{Tr}(\Pi_j\rho)$. The post-measurement state, conditioned on the event $J = j$, is given by $\Pi_j\rho\Pi_j/\mathrm{Tr}(\Pi_j\rho)$.

Consider a hypothesis test to distinguish between m possible quantum states defined by $\Phi = \{p_j, \rho_j\}|_{j=1}^m$, where the j^{th} hypothesis has prior probability p_j and density matrix ρ_j. For a projective measurement $\hat{\Pi}$, where Π_j is associated with hypothesis ρ_j, the probability of choosing correctly is

$$P(\Phi,\hat{\Pi}) = \sum_{j=1}^m p_j \mathrm{Tr}(\Pi_j\rho_j).$$

Definition 4: The *Helstrom measurement* is the minimum-error measurement to distinguish between two density matrices $\rho_0, \rho_1 \in \mathcal{D}(\mathcal{H}_n)$ when ρ_0 has prior probability p. This measurement maximizes the success probability of the test by forming projection operators onto the positive and negative eigenspaces of $M = p\rho_0 - (1-p)\rho_1$. Formally, it is defined by $\hat{\Pi}_H = \{\Pi_+, \mathbb{I}_n - \Pi_+\}$, where

$$\Pi_+ = \sum_{|v\rangle \in \mathcal{V}_+} |v\rangle\langle v|$$

where, $\mathcal{V}_+ = \{|v\rangle \in \mathcal{H}_n \mid \langle v|v\rangle = 1, \exists \lambda \geq 0, M|v\rangle = \lambda|v\rangle\}$.

Lemma 5 ([15, Lemma 6]): Consider a a BSCQ channel $W : \{0,1\} \to \mathcal{D}(\mathcal{H}_{2n})$ with equiprobable outputs where $W(z) = U^z\rho U^z$. Then, the Helstrom measurement $\hat{\Pi}_H$ is defined by

$$\hat{\Pi}_H = \left\{ \sum_{j=0}^{n-1} |v_j\rangle\langle v_j|, \sum_{j=0}^{n-1} U|v_j\rangle\langle v_j|U \right\},$$

where $\{|v_j\rangle\}_{j=0}^{n-1}$ is the set of eigenvectors for $W(0) - W(1)$ with non-negative eigenvalues.

Remark 6: For a qubit BSCQ with parameters (δ,γ), the error rate of the Helstrom measurement is δ.

B. Paired-Measurement BPQM

Paired-measurement BPQM (PM-BPQM) was introduced in [15] as a generalization of BPQM [12].

Lemma 7 ([15, Lemma 6]): Consider the Helstrom measurement to distinguish between $W(0)$ and $W(1)$ for the BSCQ channel $W : \{0,1\} \to \mathcal{D}(\mathcal{H}_n)$. One can achieve the same error rate by first implementing

$$\hat{\Pi}' = \left\{ |v_j\rangle\langle v_j| + U|v_j\rangle\langle v_j|U \right\}_{j=0}^{n-1}$$

and then, if the first outcome is j, implementing

$$\hat{\Pi}(j) = \left\{ |v_j\rangle\langle v_j|, U|v_j\rangle\langle v_j|U \right\}.$$

Lemma 8 ([15, Lemma 7]): Consider a BSCQ channel $W : \{0,1\} \to \mathcal{D}(\mathcal{H}_n)$ with $W(0) = \rho$ and equiprobable inputs. Then, the channel followed by the paired measurement $\hat{\Pi}_W$ gives a distinguishable mixture of symmetric qubit channels defined by

$$z \mapsto \sum_{j=0}^{m-1} p_j \Big(\sigma_x^z \rho \sigma_x^z \otimes |j\rangle\langle j| \Big),$$

where the j^{th} paired outcome has probability $p_j = \mathrm{Tr}\left[\big(|v_j\rangle\langle v_j| + U|v_j\rangle\langle v_j|U \big)\rho \right]$ and post-measurement density matrix

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

From Lemma 2, we can identify the parameters of ρ_j via

$$\delta_j = \frac{1}{p_j}\langle v_j|\rho|v_j\rangle, \qquad \gamma_j = \frac{1}{p_j}\langle v_j|U\rho|v_j\rangle.$$

Now, we will describe the channel combining operations that are used to define the PM-BPQM updates [12], [15]. For binary CQ channels W, W', the check-node and bit-node channel combining operations are defined by

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

$$[W \circledcirc W'](z) \coloneqq W(z) \otimes W'(z). \tag{2}$$

Lemma 9: For qubit BSCQ channels W and W', using the paired measurement to distinguish between $[W \circledast W'](0)$ and $[W \circledast W'](1)$ is equivalent to the unitary operation

$$C = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \end{bmatrix}$$

to get $\tau \coloneqq C[W \circledast W'](z)C^\dagger$ followed by measurement of the second qubit. This results in the state

$$\Pi_0\tau\Pi_0 + \Pi_1\tau\Pi_1 = \sum_{j\in\{0,1\}} p_j^{\circledast} \left(\sigma_x^z \rho(\delta_j^{\circledast}, \gamma_j^{\circledast}) \sigma_x^z \otimes |j\rangle\langle j| \right),$$

where $\Pi_0 = \mathbb{I}_2 \otimes |0\rangle\langle 0|$ and $\Pi_1 = \mathbb{I}_4 - \Pi_0$. If W and W' have the channel parameters (δ,γ) and (δ',γ'), then we can define $|v_0\rangle = \frac{1}{\sqrt{2}}(1,0,0,1)$ and $|v_1\rangle = \frac{1}{\sqrt{2}}(-1,0,0,1)$ to compute

$$p_j^{\circledast}(\delta,\gamma,\delta',\gamma') \coloneqq \mathrm{Tr}\big((|v_j\rangle\langle v_j| + \sigma_x \otimes \mathbb{I}_2 |v_j\rangle\langle v_j| \sigma_x \otimes \mathbb{I}_2)(W \circledast W')[0] \big),$$

$$\delta_j^{\boxplus}(\delta,\gamma,\delta',\gamma') \coloneqq \frac{1}{p_j^{\boxplus}} \langle v_j | (W \boxplus W')[0] | v_j \rangle ,$$
$$\gamma_j^{\boxplus}(\delta,\gamma,\delta',\gamma') \coloneqq \frac{1}{p_j^{\boxplus}} \langle v_j | (\sigma_x \otimes \mathbb{I}_2)(W \boxplus W')[0] | v_j \rangle .$$

Remark 10: We call unitary C the check-node unitary because it compresses the decision information from the check-node combining operation into the first qubit while keeping the reliability information in the second qubit. It is worth noting that the check-node unitary does not depend on the parameters of W and W'.

Lemma 11: For qubit BSCQ channels W and W' with parameters (δ,γ) and (δ',γ') respectively, implementing paired measurement to distinguish between $[W \circledast W'](0)$ and $[W \circledast W'](1)$ is equivalent to implementing the unitary $V = V(\delta,\gamma,\delta',\gamma')$ to get $\tau' \coloneqq V[W \otimes W'](z)V^\dagger$ followed by measurement of the second qubit. Here, the rows of $V(\delta,\gamma,\delta',\gamma')$ are defined, from top to bottom, by $|v_0'\rangle$, $|v_1'\rangle$, $(\sigma_x \otimes \sigma_x)|v_0'\rangle$ and $(\sigma_x \otimes \sigma_x)|v_1'\rangle$ in terms of the paired-measurement eigenvectors $|v_0'\rangle$ and $|v_1'\rangle$ that span the positive eigenspace of $(W \circledast W')[0] - (W \circledast W')[1]$. This results in the state

$$\Pi_0\tau'\Pi_0 + \Pi_1\tau'\Pi_1 = \sum_{j\in\{0,1\}} p_j^{\circledast} \left(\sigma_x^z \rho(\delta_j^{\circledast},\gamma_j^{\circledast})\sigma_x^z \otimes |j\rangle\langle j|\right),$$

where $\Pi_0 = \mathbb{I}_2 \otimes |0\rangle\langle 0|$, $\Pi_1 = \mathbb{I}_4 - \Pi_0$, and we have

$$p_j^{\circledast}(\delta,\gamma,\delta',\gamma') \coloneqq \mathrm{Tr}\big(\big(|v_j'\rangle\langle v_j'| + \sigma_x \otimes \sigma_x |v_j'\rangle\langle v_j'| \sigma_x \otimes \sigma_x\big)(W \circledast W')[0]\big)$$

$$\delta_j^{\circledast}(\delta,\gamma,\delta',\gamma') \coloneqq \frac{1}{p_j^{\circledast}} \langle v_j' | (W \circledast W')[0] | v_j' \rangle ,$$
$$\gamma_j^{\boxplus}(\delta,\gamma,\delta',\gamma') \coloneqq \frac{1}{p_j^{\circledast}} \langle v_j' | (\sigma_x \otimes \sigma_x)(W \circledast W')[0] | v_j' \rangle .$$

Remark 12: The unitary $V(\delta,\gamma,\delta',\gamma')$ is called the bit-node unitary. Similar to the check-node unitary, it compresses the decision information from the bit-node channel combining into the first qubit while keeping the reliability information in the second qubit. Unlike the check-node unitary C, the eigenvectors $|v_0'\rangle$ and $|v_1'\rangle$ depend on the channel parameters and thus $V(\delta,\gamma,\delta',\gamma')$ does as well [15].

C. Density Evolution for Paired-Measurement BPQM

Density evolution (DE) is a tool widely used by coding theorists to analyze the asymptotic performance of BP decoding for long codes chosen from certain families [19]. For BSCQ channels, the paired measurement [18] compresses the decision information from check-node and bit-node combining into the first qubit while keeping reliability information in the second qubit. By tracking how the message reliability evolves through this process, one can use DE to analyze the performance of PM-BPQM decoding for a code whose factor graph is a tree. Applying DE to a long code, whose factor graph is a tree with sufficiently large depth, results in a threshold phenomenon that allows one to estimate the noise threshold (i.e., the maximum noise level where DE predicts successful decoding) for families of codes. In [18], this was applied to regular LDPC codes on CQ channels with PM-BPQM decoding.

D. Polar Codes

Polar codes were introduced by Arıkan in 2009 as the first deterministic construction of capacity-achieving codes for binary memoryless symmetric (BMS) channels [20]. The polar transform of length $N = 2^n$ is denoted by $G_N \triangleq B_N G_2^{\otimes n}$ where B_N is $N \times N$ bit reversal matrix [20, Sec. VII.B] and $G_2^{\otimes n}$ is n-fold tensor product of 2×2 binary matrix

$$G_2 \triangleq \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Polar codes work by using the polar transform G_N to encode a vector $u \in \{0,1\}^N$ whose values are free on a subset $\mathcal{A} \subseteq [N]$ of information positions but restricted to have fixed values on the complementary set $\mathcal{A}^c = [N] \setminus A$ of frozen positions. For the frozen positions, the fixed values are shared with the receiver in advance to aid the decoding process.

Polar codes can achieve capacity on BMS channels under low-complexity successive-cancellation (SC) decoding, where one decodes the bits $u_1, u_2, \ldots$ in order assuming all past decoding decisions are correct but that no information is known about future u values. The performance of this approach is analyzed by recursively defining the effective channels seen by the SC decoder assuming all past decisions are correct.

Polar codes were extended to CQ channels by Wilde and Guha [8]. Similar to the classical case, one can recursively define effective channels that characterize the performance of successive cancellation (SC) decoding. When decoding the i^{th} bit of a length-N polar code, the designed effective channel [8, p. 1178] for a CQ channel W is defined by

$$W_N^{(i)}(u_i) \coloneqq \frac{1}{2^{N-1}} \sum_{u_{\sim i}\in\{0,1\}^{N-1}} |u_1^{i-1}\rangle\langle u_1^{i-1}| \otimes \left(\bigotimes_{i=1}^{N} W([\boldsymbol{u}G_N]_i)\right).$$

The SC decoder implements the implied sequence of Helstrom measurements indexed by the information bits in $\mathcal{A}$. One difference from the classical case is that the effective channels encountered during decoding may differ from the designed effective channels even when all past decisions are correct. This is because the sequential measurement process can disturb the codeword state even when the decision is correct. In particular, the channel seen by the decoder equals the designed effective channel if all earlier bits are frozen (i.e., $[i-1] \subseteq \mathcal{A}^c$). When the set $\mathcal{A}$ of information channels is selected to achieve a sufficiently low error rate, the non-commutative union bound (e.g., see [21]–[23]) shows that this disturbance is negligible.

III. PM-BPQM and Polar Codes

A. PM-BPQM DE for Polar Code Design

To design a polar code for a CQ channel assuming SC decoding based on PM-BPQM, we implement PM-BPQM DE for the BSCQ channel via Monte Carlo simulation.

Let $W_N^{(i)}$ refer to the effective channel experienced by the i^{th} information bit of a length-N polar code assuming all previous bits are frozen. The input-output law for this channel can be computed recursively using

$$\begin{aligned} W_N^{(2i-1)} &= W_{N/2}^{(i)} \circledast W_{N/2}^{(i)} \\ W_N^{(2i)} &= W_{N/2}^{(i)} \circledcirc W_{N/2}^{(i)}, \end{aligned}$$

where the check-node and bit-node update rules are defined by Eq. (1) and Eq. (2). For a code of length $N = 2^n$, this requires n levels of recursion starting from $W = W_1^{(1)}$.

At each level of the recursion, one computes a representation of the new channels via check-node and bit-node updates from representations of the channels at the previous level. This approach has two key issues. First, the channels involved may not have simple representations. While any classical BMS channel can be represented as a mixture of binary symmetric channels (i.e., a distribution over $[0, \frac{1}{2}]$) [19], the set of BSCQ channels does have such a simple description. Second, the set of possible channel parameters grows very rapidly and is expensive to track.

In this work, the first issue is resolved by using the suboptimal PM-BPQM decoder because its intermediate channels are all qubit BSCQ channels that are parameterized by two real numbers (δ, γ). The second issue can also occur with classical channels and is typically resolved by using Monte Carlo DE (known as population dynamics in statistical physics [24]) to approximate the answer efficiently [25]. The idea of Monte Carlo DE is to approximate distributions over channel parameters by bags of M samples (i.e., a uniform distribution over a length-M list of channel parameters).

Consider a bag $B = \{(\delta_j, \gamma_j)\}_{j=1}^M$ containing M pairs of real numbers corresponding to the parameters of different qubit BSCQ channels. Then, we define the check-node and bit-node updates of B as follows.

Definition 13: The *check-node update* $B^{\circledast} = \{(\delta'_j, \gamma'_j)\}_{j=1}^M$ of B be constructed as follows. For each element $(\delta_j, \gamma_j) \in B$, we choose another random element $(\delta_{\pi(j)}, \gamma_{\pi(j)})$, where $\pi : [M] \to [M]$ is a uniform random permutation. Then, we apply the check-node channel combining operation on the two implied qubit BSCQs. The parameters of the resulting qubit BSCQ are given (for $a \in \{0, 1\}$) by

$$\big(\delta_a^{\circledast}(\delta_j, \gamma_j, \delta_{\pi(i)}, \gamma_{\pi(j)}), \gamma_a^{\circledast}(\delta_j, \gamma_j, \delta_{\pi(j)}, \gamma_{\pi(j)})\big),$$

with probability $p_a^{\circledast}(\delta, \gamma, \delta', \gamma')$. The j-th value (δ'_j, γ'_j) of $B^{\circledast}$ is set by choosing one of the two according to $p_a^{\circledast}$.

Definition 14: The *bit-node update* $B^{\circledcirc} = \{(\delta'_j, \gamma'_j)\}_{j=1}^M$ of B is constructed analogously to the check-node update. In particular, the steps are identical but all expressions use the $\circledcirc$ superscript rather than the $\circledast$ superscript.

Now, we consider the design of an (N, K) polar code for a qubit BSCQ with parameters (δ, γ). We implement the DE design of the code using the following steps.

1) $B_{0,1} \leftarrow \{(\delta_j, \gamma_j)\}_{j=1}^M$ with $(\delta_j, \gamma_j) = (\delta, \gamma)$ for $j \in [M]$
2) For k in $\{1, \ldots, \log_2 N\}$:
   a) For i in $\{1, \ldots, 2^{k-1}\}$:
      i) Compute check-node update: $B_{k,2i-1} \leftarrow B_{k-1,i}^{\circledast}$
      ii) Compute bit-node update: $B_{k,2i} \leftarrow B_{k-1,i}^{\circledcirc}$
3) For i in $\{1, \ldots, N\}$:
   a) Using $B_{n,i} \to \{(\delta_j, \gamma_j)\}_{j=1}^M$
   b) Compute: $\varepsilon_i \leftarrow \frac{1}{M} \sum_{j=1}^M \delta_j$
4) For a length-N polar code with K information bits, let $\mathcal{A} = \{i \in [N] \mid \varepsilon_i \leq \alpha\}$ and choose α so $|\mathcal{A}| = K$.

We note that the DE for PM-BPQM decoding of the effective channel $W_N^{(i)}$ assumes that we make hard decisions about the channel reliability at each stage of decoding (e.g., it measures the second qubit after applying the C or V unitary at each stage). Under this assumption, $B_{n,i}$ approximates the distribution of the channel parameters seen when decoding U_i given the observation from $W_N^{(i)}$. Since the Helstrom error rate for a qubit BSCQ with parameters (δ, γ) is δ, the expected Helstrom error rate for $W_N^{(i)}$ under PM-BPQM decoding is approximated by ε_i. Thus, the design method approximates the expected error rate of each effective channel and then chooses the K information bits whose effective channels have the smallest error rates.

IV. Numerical Results for Polar Code Design

In Fig. 1 and Fig. 2, we plot the code rate achievable by the PM-BPQM decoder for length-1024 polar codes. Our results consider channels with $\delta \in \{0.07, 0.09\}$ and a range of γ. We also compare the results with a measure first (MF) strategy that uses a classical polar code designed for the binary symmetric channel. Its curve is labeled MF:UB because it uses the classical union bound. All codes are designed under a union-bound constraint on the block-error probability of 0.1.

Since the union bound for classical and quantum events differs roughly by a factor of 4 [21]–[23], a fair comparison is challenging and we make two different unfair comparisons. The curve labeled PM-BPQM:UB ignores the factor of 4 and uses the classical union bound to enforce the block error constraint. Comparing it with the MF:UB curve is somewhat unfair to MF strategy. The curve labeled PMBPQM:NCUB uses Gao's bound [21]. Comparing it with the MF:UB curve gives MF strategy an unfair advantage. In both cases, the PM-BPQM decoder achieves a higher rate than the hard-decision decoder for large values of γ but the transition point increases for the non-commutative union bound.

In [17], one can find additional information such as the channel error rates as a function of block length in order to visualize polarization. The capacity of the qubit BSCQ is compared with the hard-decision capacity in [17].

V. Simulation of the PM-BPQM Polar Decoder

The PM-BPQM decoding process is assumed to measure the reliability information of intermediate channels during decoding [15]. While these measurements do not affect the performance of the targeted information bit (e.g., the first non-frozen bit or the root node of an LDPC code tree), they do disturb the quantum state and hurt the performance

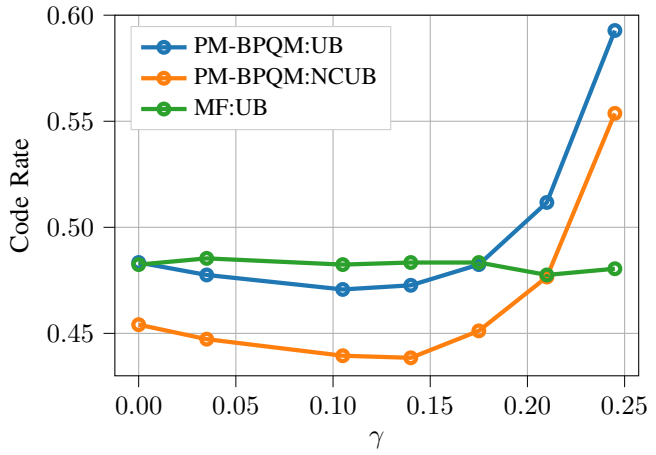

Fig. 1. Comparison of PM-BPQM and MF polar decoder for $N = 1024$ on qubit BSCQ channels with $\delta = 0.07$ and variable γ under a union-bound block-error constraint of 0.1.

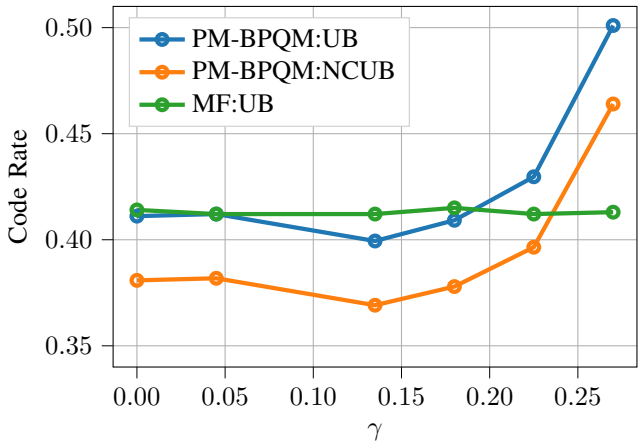

Fig. 2. Comparison of PM-BPQM and MF polar decoder with $N = 1024$ on qubit BSCQ channels with $\delta = 0.09$ and variable γ under a union-bound block-error constraint of 0.1.

of later bits (e.g., the second non-frozen bit). It is well-known that this degradation can be avoided by delaying the intermediate measurements using the quantum principle of deferred measurement [12], [13].

The cost of deferring measurements is that all unitary operations done after a deferred measurement must be implemented as conditional unitary operations that depend on the system that was not measured. This results in conditional unitary operations that depend on many qubits. While such operations are difficult to realize on physical quantum computers, they can be implemented with relatively low complexity in a classical simulation of a quantum computer. This is the approach we use in our simulation code. For a physical quantum computer, Renes and Piveteau recently described another approach that achieves quadratic complexity by using reliability registers in the decoder to reduce the burden of conditioning [14].

In [17], we describe in detail the decoding process with deferred measurements for a length-4 polar code. We provide descriptions both for BPQM on the pure-state channel and for PM-BPQM on a qubit BSCQ channel. We compare the performance of this decoder (by simulating the full quantum system) with the DE calculation (which only uses the expressions in Lemmas 9 and 11. The results can be found in Fig. 3 where we plot the Helstrom error rate corresponding to each channel between DE output and the PM-BPQM based polar decoder.

VI. Conclusion

In this paper, we consider the design and decoding of polar codes on general CQ channels. Our approach is based on analyzing and implementing the suboptimal PM-BPQM decoder. On the analysis side, we use DE to design polar codes for general CQ channels under PM-BPQM decoding. This process can be easily implemented on a classical computer and allows one to explore the achievable trade-off between rate and block-error probability.

We have also implemented the PM-BPQM polar decoder for arbitrary N in Python. It consists of a classical recursive algorithm that controls a quantum simulator (or quantum

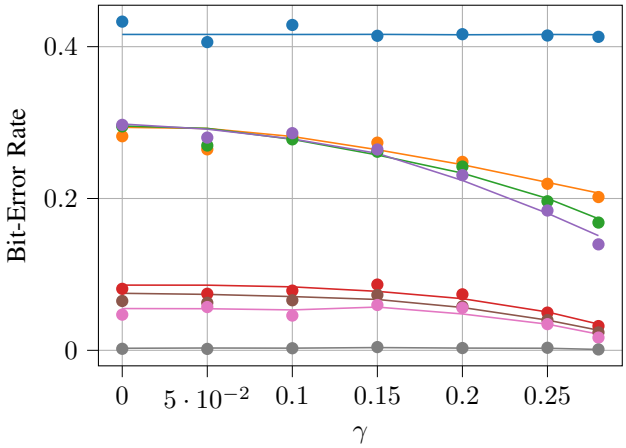

Fig. 3. Comparison of bit-error rate between DE analysis (solid lines) and simulated decoder (circles) for the effective channels of bits $u_1, \ldots, u_8$ of a length-8 polar code over qubit BSCQ channels with $\delta = 0.1$ and variable γ.

computer) to implement the PM-BPQM decoding process. The code can be found on GitHub in the repository:

https://github.com/Aviemathelec1995/CQ-Polar-BPQM.

This decoder was used to perform some experiments. In Fig. 3, we compare the simulated decoding performance with the DE prediction for a length-8 polar code and observe a good agreement. The decoder also allows us to analyze the block error rate without resorting to union bounds. For the length-8 code, we use the 4^{th}, 6^{th}, 7^{th} and 8^{th} input bits as information bits. We estimate the block error rate using 1000 blocks over the BSCQ channel with $(\delta, \gamma) = (0.05, 0.15)$. Its value is roughly 0.07 when we use the frozen set $(u_1, u_2, u_3, u_5) = (1, 1, 1, 1)$ and random information symbols. For comparison, the error rates of the individual channels (u_4, u_6, u_7, u_8) are computed using DE and they are 0.0178, 0.0146, 0.0123, and 0.0003, respectively. The classical union bound on block error rate equals the sum of the individual channel error rates (i.e., roughly 0.045). Thus, the observed block error rate is roughly twice the classical union bound and less than the factor of 4 worst-case increase allowed by Gao's bound [21].

References

[1] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 269–273, 1998.

[2] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Physical Review A*, vol. 56, no. 1, p. 131, 1997.

[3] M. A. Nielsen and I. Chuang, *Quantum computation and quantum information*, 2002.

[4] M. Wilde, *Quantum Information Theory*. Cambridge University Press, 2013, ISBN: 9781107067844.

[5] S. Guha and M. M. Wilde, "Polar coding to achieve the holevo capacity of a pure-loss optical channel," in *2012 IEEE International Symposium on Information Theory Proceedings*, IEEE, 2012, pp. 546–550.

[6] H. Krovi, S. Guha, Z. Dutton, and M. P. da Silva, "Optimal measurements for symmetric quantum states with applications to optical communication," *Physical Review A*, vol. 92, no. 6, p. 062 333, 2015.

[7] 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, no. 5, p. 052 320, 2013.

[8] M. M. Wilde and S. Guha, "Polar codes for classical-quantum channels," *IEEE Transactions on Information Theory*, vol. 59, no. 2, pp. 1175–1187, 2012.

[9] M. M. Wilde, O. Landon-Cardinal, and P. Hayden, "Towards efficient decoding of classical-quantum polar codes," in *8th Conference on the Theory of Quantum Computation, Communication and Cryptography*, 2013, p. 157.

[10] J. M. Renes and M. M. Wilde, "Polar codes for private and quantum communication over arbitrary channels," *IEEE Transactions on Information Theory*, vol. 60, no. 6, pp. 3090–3103, 2014.

[11] R. Nasser and J. M. Renes, "Polar codes for arbitrary classical-quantum channels and arbitrary cq-macs," *IEEE Transactions on Information Theory*, vol. 64, no. 11, pp. 7424–7442, 2018.

[12] J. M. Renes, "Belief propagation decoding of quantum channels by passing quantum messages," *New Journal of Physics*, vol. 19, no. 7, p. 072 001, 2017. [Online]. Available: http://arxiv.org/abs/1607.04833.

[13] 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, p. 97, 2021.

[14] C. Piveteau and J. M. Renes, "Quantum message-passing algorithm for optimal and efficient decoding," *Quantum*, vol. 6, p. 784, 2022.

[15] S. Brandsen, A. Mandal, and H. D. Pfister, "Belief propagation with quantum messages for symmetric classical-quantum channels," in *2022 IEEE Information Theory Workshop (ITW)*, IEEE, 2022, pp. 494–499.

[16] R. Gallager, "Low-density parity-check codes," *IRE Transactions on information theory*, vol. 8, no. 1, pp. 21–28, 1962.

[17] A. Mandal, S. Brandsen, and H. D. Pfister, "Belief-propagation with quantum messages for polar codes on classical-quantum channels," arXiv preprint, 2023.

[18] S. Brandsen, A. Mandal, and H. D. Pfister, *Belief propagation with quantum messages for symmetric classical-quantum channels*, 2022. DOI: 10.48550/ARXIV.2207.04984.

[19] T. Richardson and R. Urbanke, *Modern coding theory*. Cambridge university press, 2008.

[20] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[21] J. Gao, "Quantum union bounds for sequential projective measurements," *Physical Review A*, vol. 92, no. 5, p. 052 331, 2015.

[22] S. Khabbazi Oskouei, S. Mancini, and M. M. Wilde, "Union bound for quantum information processing," *Proceedings of the Royal Society A*, vol. 475, no. 2221, p. 20 180 612, 2019.

[23] R. O'Donnell and R. Venkateswaran, "The quantum union bound made easy," in *Symposium on Simplicity in Algorithms (SOSA)*, SIAM, 2022, pp. 314–320.

[24] M. Mezard and A. Montanari, *Information, physics, and computation*. Oxford University Press, 2009.

[25] M. Davey and D. MacKay, "Low-density parity check codes over GF(q)," *IEEE Communications Letters*, vol. 2, no. 6, pp. 165–167, 1998. DOI: 10.1109/4234.681360.