

ARTICLE OPEN



Belief propagation with quantum messages for quantum-enhanced classical communications

Narayanan Rengaswamy^{1✉}, Kaushik P. Seshadreesan^{2✉}, Saikat Guha² and Henry D. Pfister³

For space-based laser communications, when the mean photon number per received optical pulse is much smaller than one, there is a large gap between communications capacity achievable with a receiver that performs individual pulse-by-pulse detection, and the quantum-optimal “joint-detection receiver” that acts collectively on long codeword-blocks of modulated pulses; an effect often termed “superadditive capacity”. In this paper, we consider the simplest scenario where a large superadditive capacity is known: a pure-loss channel with a coherent-state binary phase-shift keyed (BPSK) modulation. The two BPSK states can be mapped conceptually to two non-orthogonal states of a qubit, described by an inner product that is a function of the mean photon number per pulse. Using this map, we derive an explicit construction of the quantum circuit of a joint-detection receiver based on a recent idea of “belief-propagation with quantum messages” (BPQM). We quantify its performance improvement over the Dolinar receiver that performs optimal pulse-by-pulse detection, which represents the best “classical” approach. We analyze the scheme rigorously and show that it achieves the quantum limit of minimum average error probability in discriminating 8 (BPSK) codewords of a length-5 binary linear code with a tree factor graph. Our result suggests that a BPQM receiver might attain the Holevo capacity of this BPSK-modulated pure-loss channel. Moreover, our receiver circuit provides an alternative proposal for a quantum supremacy experiment, targeted at a specific application that can potentially be implemented on a small, special-purpose, photonic quantum computer capable of performing cat-basis universal qubit logic.

npj Quantum Information (2021)7:97; <https://doi.org/10.1038/s41534-021-00422-1>

INTRODUCTION

“Message-passing” algorithms are used to efficiently evaluate quantities of interest in problems defined on graphs. They work by passing messages between nodes of the graph. For example, these algorithms have been successfully used for statistical inference, optimization, constraint-satisfaction problems, and the graph isomorphism problem among several other applications^{1–8}. In particular, “belief-propagation” (BP) is a message-passing algorithm for efficiently marginalizing joint probability density functions in statistical inference problems. The algorithm derives its name from the fact that the messages used in BP are “local” probabilities or “beliefs” (e.g., of the value of the final quantity of interest). An important application of BP lies in the decoding of linear codes using the posterior bit-wise marginals given the outputs of a classical channel⁹. It is well-known that BP exactly performs the task of optimal bit-wise maximum-a-posteriori (bit-MAP) decoding when the code’s factor graph is a tree. However, since codes with tree factor graphs have poor minimum distance⁹, BP is also applied to codes whose factor graphs have cycles, e.g. low-density parity-check (LDPC) codes. Although BP does not compute the exact marginals in this case, it is computationally more efficient than MAP, and usually performs quite well. In fact, it has been proven that, for large blocks, BP achieves the optimal MAP performance for spatially-coupled LDPC codes over the binary erasure channel¹⁰ and binary memory-less symmetric channels^{11,12}. From a more practical perspective, BP-based decoders are routinely deployed in modern communications and data storage.

Given the success of BP decoding for classical channels, it is natural to ask if it can be generalized to the quantum setting. For example, can one decode classical codes for communications over a classical-quantum (CQ) channel or, more generally, perform efficient inference on graphically-represented classical data encoded in qubits?

Consider laser communications based on binary phase-shift keying (BPSK) modulation for sending classical data over a pure-loss bosonic channel of transmissivity $\eta \in [0, 1]$ ¹³. During each “use” of the quantum channel, the transmitter modulates each optical pulse, or mode, into one of the two coherent states $|a\rangle$ or $|−a\rangle$, where $a \in \mathbb{R}$ and the mean photon number per mode equals $N_s = |a|^2$. Each channel output symbol is an optical pulse that is in one of the two coherent states $|\pm\beta\rangle$, where $\beta = \sqrt{\eta}a$ and mean photon number $N = \eta N_s$. These two states are non-orthogonal with an inner product $\langle\beta|-\beta\rangle = e^{-2N} \equiv \sigma$. In this case, the coherent states $|\pm\beta\rangle = \sum_{n=0}^{\infty} e^{-|\beta|^2/2} \frac{(\pm\beta)^n}{\sqrt{n!}} |n\rangle$ live in an infinite-dimensional Hilbert space spanned by the complete orthonormal number basis $\{|n\rangle, n \in \mathbb{N}\}$. However, since each channel output is always in one $|\pm\beta\rangle$, for the purposes of designing a receiver, we can embed the subspace spanned by $|\pm\beta\rangle$ in a two-dimensional (qubit) Hilbert space via the inner product-preserving map:

$$|\pm\beta\rangle \mapsto |\pm\theta\rangle := \cos\frac{\theta}{2}|0\rangle \pm \sin\frac{\theta}{2}|1\rangle, \quad (1)$$

with $\sigma = \cos\theta$. The resulting channel from a classical encoding variable x to a conditional quantum state, i.e., $[x = 0] \mapsto |\theta\rangle, [x = 1] \mapsto |-\theta\rangle$, is often called a (pure-state) “CQ” channel in the quantum information theory literature.

When the channel output symbols are detected one at a time, the best possible detection error probability is given by the Helstrom bound^{14,15} on the minimum average error probability of discriminating the alphabet states $|\pm\beta\rangle$, which is $p := \frac{1}{2}[1 - \sqrt{1 - \sigma^2}]$. A structured optical design of a receiver that achieves this performance was invented by Dolinar in 1973¹⁶. This receiver induces a binary symmetric channel (BSC) between the quantum channel outputs $|\pm\beta\rangle$ and the receiver’s guess “ $\pm\beta$ ”, with crossover probability p , thereby enabling the communicating

¹Department of Electrical and Computer Engineering, The University of Arizona, Tucson, AZ 85721, USA. ²College of Optical Sciences, The University of Arizona, Tucson, AZ 85721, USA. ³Department of Electrical and Computer Engineering, Duke University, Durham, NC 27708, USA. ✉email: narayananr@arizona.edu; kaushikshesh@email.arizona.edu

parties to achieve a reliable communication rate given by $C_1 = 1 - h_2(p)$ bits per mode, the Shannon capacity of the BSC. To achieve communication at a rate close to this capacity, one would need to use a code that achieves the Shannon capacity of the BSC, e.g., Arikan's polar code¹⁷, and a suitable decoder. If the receiver detects, i.e., converts from the quantum (optical) to the electrical domain, each quantum channel output one at a time, no amount of classical post-processing, including feedforward between channel uses, and soft-information processing, can achieve a rate higher than C_1 . Thus, a capacity-approaching LDPC code for the BSC and a BP decoder can approach but not surpass the rate C_1 .

However, if one employs a quantum joint-detection receiver that collectively measures the entire block of n channel outputs, then the rate may increase to the Holevo limit, $C_\infty = S(\frac{1}{2}|\beta\rangle\langle\beta| + \frac{1}{2}|-\beta\rangle\langle-\beta|) = h_2([1 + \sigma]/2)$ bits per mode, where $S(\cdot)$ denotes the von Neumann entropy. In the limit as $N \rightarrow 0$ (or equivalently $\sigma \rightarrow 1$), where the mean photon number per mode vanishes, one can show that $C_\infty/C_1 \rightarrow \infty$ and collective measurement is preferable. This regime of operation is especially important for long-haul free-space terrestrial and deep-space laser communications. In order to fully exploit this large capacity gain, one can use a CQ polar code¹³ with a decoder based on collective measurement of the received quantum state. Alternatively, one can use a codebook comprising $M = 2^{nR}$ random length- n codewords with $R < C_\infty$, where each symbol of each codeword is chosen from an equal prior over the two BPSK symbols. If the receiver employs a joint measurement that discriminates between the codewords sufficiently well, then the probability of decoding error will converge to 0 as $n \rightarrow \infty$. Both the optimal measurement and the square root measurement (SRM) are known to faithfully discriminate between roughly 2^{nC_∞} codewords¹⁸, as opposed to only 2^{nC_1} codewords if symbol-by-symbol detection is combined with classical decoding. Given the quantum states of the M codewords, the optimal measurement can be computed by applying the Yuen-Kennedy-Lax (YKL) conditions¹⁹ applied to the Gram matrix of the codebook—the M -by- M matrix of pairwise inner products of the codewords' quantum states. This calculation is simpler for linear codes²⁰, especially codes that have certain group symmetries²¹. Even when it is possible to compute the optimal measurement for the codebook, it may be hard to translate the mathematical description into a physical receiver design²², unless we have a general-purpose photonic quantum computer²³. Therefore, an efficient and physically realizable receiver is of significant practical

interest if it can outperform the optimal receiver based on optimal symbol-by-symbol measurement.

Renes²⁴ recently proposed a quantum generalization of BP for a binary-output pure-state CQ channel. Renes' algorithm is well-defined on a tree factor graph and works by passing quantum messages (encoded in qubits) and classical messages (bits) between nodes of the code's factor graph. Unlike earlier algorithms termed "quantum belief-propagation"^{25,26}, Renes' algorithm does not measure the n channel outputs, followed by classical BP on the (classical) syndrome measurements, and hence is not limited to achieving a rate of C_1 . In order to avoid any confusion with previous quantum BP algorithms, we will refer to Renes' algorithm as "belief-propagation with quantum messages" (BPQM).

In²⁴, the first step in developing BPQM was to interpret the message-combining operations in classical BP as "channel combining" rules that execute a local inference procedure. This step has close connections with the channel combining operation defined by Arikan for polar codes¹⁷. The second step was a generalization of these channel combining rules to allow for quantum messages, as in CQ polar codes¹⁸, i.e., messages that are qubit density matrices which capture the node's belief about a message bit. The above rules define a CQ channel that gets induced at each node when (quantum) messages arrive at it. Finally, the third step was to define appropriate unitary operations at the nodes, which process the outputs of the aforesaid induced CQ channels and produce messages to be passed on to subsequent nodes.

While²⁴ is a breakthrough paper that provides a phenomenological description of BPQM, it does not assess its performance on an example code or make comparisons with optimal symbol-by-symbol measurements. Also, it does not present a proof of decoding optimality, even for CQ codes with a tree factor graph. Finally, it does not prescribe an explicit quantum circuit for BPQM. This paper addresses all of the above open questions and resolves many of them for the chosen example code.

RESULTS AND DISCUSSION

BPQM-based receiver design and block error rates

We construct an explicit quantum circuit for a BPQM-based joint-detection receiver (blueprint shown under "Methods" section, see Fig. 8), and prove that it achieves the Helstrom limit for discriminating between the eight codewords in our exemplary $n = 5$ linear BPSK code with a tree factor graph, as shown in Fig. 1.

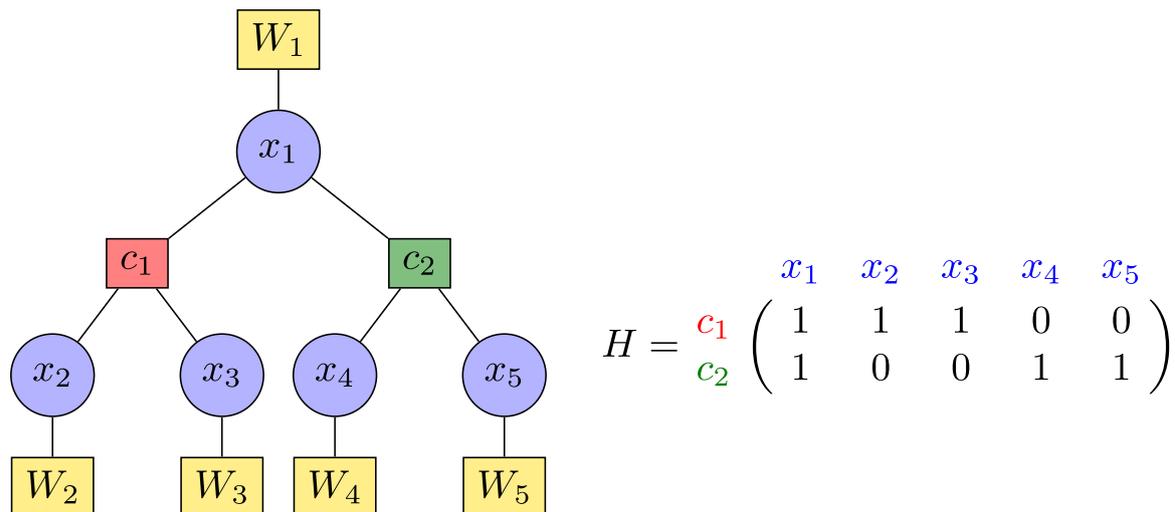


Fig. 1 Factor graph and parity-check matrix for the 5-bit linear code in the running example. Each circle node denotes a variable x_i , the square nodes c_1 and c_2 denote the two parity checks corresponding to the two rows of H , and the square nodes W_i denote the channel observation of the associated variables x_i .

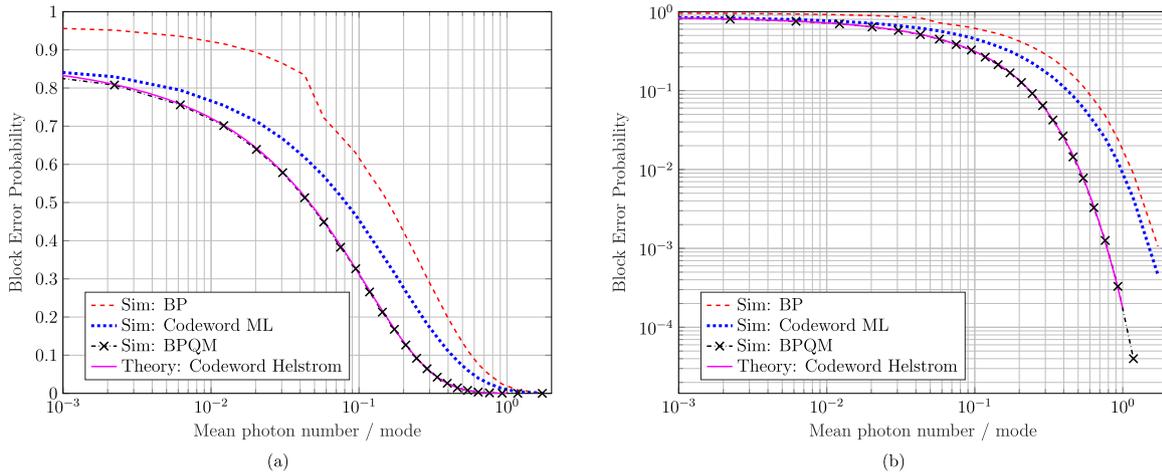


Fig. 2 The overall performance of BPQM compared with that of other related schemes. **a** The overall block error rate of BPQM along with those of optimal joint Helstrom, symbol-by-symbol Helstrom followed by classical optimal block MAP, and symbol-by-symbol Helstrom followed by classical BP. **b** The same plot as **a** except that the error rates are also displayed in log scale.

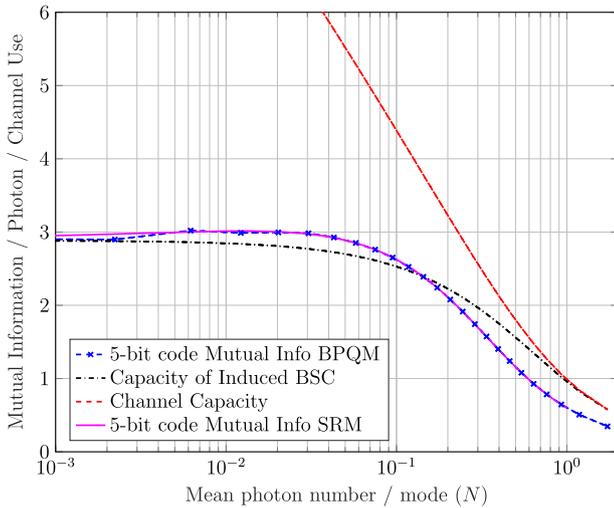


Fig. 3 Mutual information per photon per channel use achieved by BPQM and the square root measurement (SRM) on the 5-bit code over the pure-state channel, along with the Holevo capacity of the channel and the BSC capacity induced by symbol-by-symbol Helstrom measurements at the channel output, all plotted against the mean photon number per mode (N). BPQM and SRM on this code produce identical results. The curves indicate that BPQM/SRM provides mutual information gains for certain regimes of N , thereby demonstrating superadditive capacity with an explicit code and decoder.

Hence, it outperforms the best achievable performance by the optimal symbol-by-symbol receiver measurement followed by a MAP decision. Based on our analysis of BPQM, we introduce a coherent rotation to be performed after decoding bit 1 as part of our receiver design, which is not part of Renes' original BPQM scheme. This might be important for generalizing BPQM beyond the specific example considered here (see Remark 2). We explicitly compute the density matrices of quantum messages that are passed, and evaluate the performance of BPQM for this example code. For decoding bit 1, we also derive an analytical expression for the BPQM success probability. The ultimate benchmark for decoding a bit is the performance of the Helstrom measurement

that optimally distinguishes the density matrices corresponding to the two values of the bit. We show that BPQM is optimal for deciding the value of each of the 5 bits. In Fig. 2, we plot performance curves that show the “global” performance of BPQM for the 5-bit code in terms of block (codeword) error rate for the following strategies:

- collective (optimal) Helstrom measurement on all $n=5$ channel outputs of the received codeword,
- BPQM on all channel outputs of the received codeword,
- symbol-by-symbol (optimal) Helstrom measurement followed by classical (optimal) block-MAP decoding, and
- symbol-by-symbol (optimal) Helstrom measurement followed by classical BP decoding.

For the last two schemes, classical decoding is performed for the BSC, with crossover probability $p = \frac{1}{2}[1 - \sqrt{1 - \sigma^2}]$, that is induced by measuring each channel output with the Helstrom measurement to discriminate between $|\pm\theta\rangle$.

As expected, the block error probabilities are in increasing order from (a) through (d). The plot shows that BPQM is strictly better than the quantum-optimal symbol-by-symbol detection followed by a block-MAP decision at all values of mean photon number per mode, and that it meets the optimal joint Helstrom measurement on the modulated codeword. We confirm this optimality analytically by using the fact that the SRM, also called the pretty good measurement, is optimal for transmitting binary linear codes on the pure-state channel²⁰ (discussed under “Methods” section). More precisely, we calculate the closed-form expression for the SRM block error probability²⁷, in terms of the classical code and associated cosets, and the density matrix-based expression for the BPQM block error probability for this example code. Then, for a range of channel parameters, we compute the values from these expressions and confirm that they agree up to even 15 decimal places. Therefore, while decomposing the SRM itself into an explicit circuit might be challenging, BPQM provides a circuit that still achieves the optimal block error probability for this code. This is an important result because, it demonstrates that, if we can construct a BPQM receiver, then it will outperform any known physically realizable receiver for this channel. We provide more detailed observations on Fig. 2 shortly.

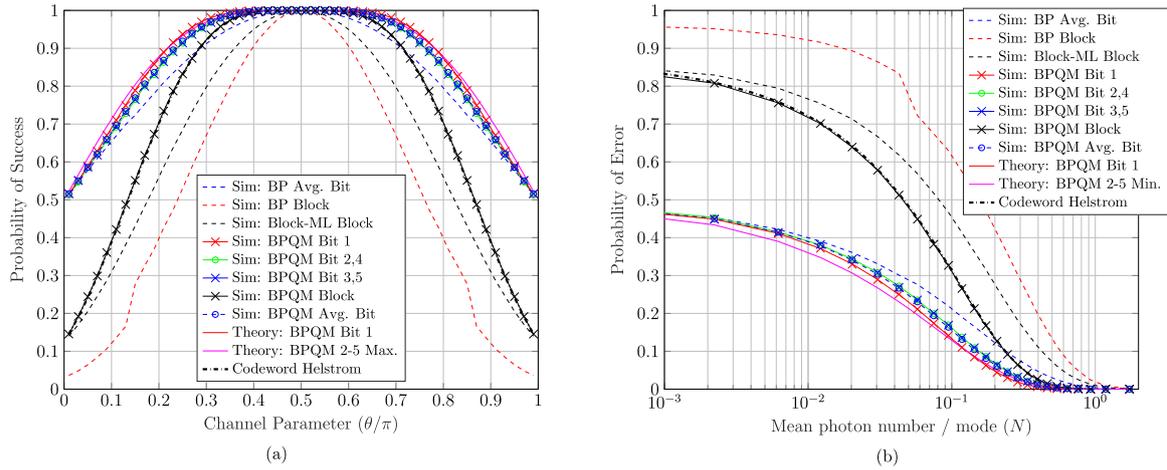


Fig. 4 The overall performance of BPQM for each bit and for the whole codeword. Each data point in all simulation curves was obtained by averaging over 10^5 uniformly random codeword transmissions. **a** The BPQM success probabilities for decoding each bit and its overall performance for the 5-bit code, the theoretical BPQM/Helstrom success rate for bit 1, the initial theoretical prediction of $0.5(1 + \sin \theta^{\otimes 5})$ for BPQM for bits 2–5, the performance of BP and block ML when applied to the directly measured channel outputs, and the joint Helstrom limit (Eq. 76). **b** The same curves on the left plotted against the mean photon number per mode N ($\cos \theta = e^{-2N}$), where the codeword Helstrom limit was calculated from the YKL limit as in²¹. It can be seen that the YKL limit also matches the theoretical calculation from (Eq. 76).

Photon information efficiency

Besides the block error rates, we also compare the mutual information per photon per channel use, also referred to as the photon information efficiency (PIE)^{28,29}, for BPQM, with the Holevo capacity of the pure-state channel and the capacity induced by symbol-by-symbol Helstrom measurements. In order to do this, we consider a composite channel whose input is $k = 3$ bits and output is also $k = 3$ bits, where the channel consists of encoding into the 5-bit code, transmitting over the pure-state channel, applying the BPQM receiver and identifying the transmitted codeword (equivalently the k -bit message). Determining the PIE for the BPQM analytically involves calculating closed-form expressions for the transition probabilities of the 2^k -ary channel (where $k = 3$ for the considered 5-bit code), which involves cumbersome calculations of the relevant density matrices. Instead, we calculate the PIE numerically by performing a Monte Carlo simulation. Figure 3 shows a plot of the PIE of the BPQM receiver along with those corresponding to the Holevo capacity and the symbol-by-symbol Helstrom induced BSC capacity. We also compute the PIE for the SRM. The transition probability of decoding a transmitted message $t \in \{0, 1\}^k$ as $g \in \{0, 1\}^k$ using the SRM is given by²⁷

$$\mathbb{P}[g | t] = \frac{\hat{\sigma}(g \oplus t)^2}{2^k}, \quad \hat{\sigma}(g \oplus t) = \frac{1}{\sqrt{2^k}} \sum_{h \in \mathbb{Z}_2^k} (-1)^{h(g \oplus t)^T} \sigma(h), \quad \sigma(h) = 2^{k/4} \sqrt{\hat{s}(h)}, \quad (2)$$

where $\hat{s}(h)$ is as defined in (Eq. 77) (under “Methods” section, where the block success rate with the SRM given by (Eq. 76) is evaluated). Therefore, the transition probability only depends on the sum $g \oplus t$ and hence the channel is symmetric. Using this closed form expression, we compute the mutual information for this k -bit channel, normalized by $n = 5$ (to obtain mutual information per channel use), then normalized by N to obtain the PIE, and also plot it in Fig. 3. We see that both BPQM and SRM produce identical curves, just as they do in block error rates. Finally, we observe that there exists a regime of N , where this explicit small code along with BPQM or SRM demonstrates superadditive capacity that beats the largest PIE obtained from symbol-by-symbol Helstrom measurements. The PIE with the BPQM (or SRM) receiver is found to be maximized at $N = 6.2 \times 10^{-3}$, the maximum PIE being 3.021, whereas the corresponding PIE attained by symbol-by-symbol Helstrom measurements is 2.862, the ratio of the two numbers being 1.056. (Interestingly, this

is higher than the PIE ratio of 1.031 that has been reported for a different 5-bit code with 16 codewords and the corresponding SRM in ref. 30.) The superadditive PIE hence makes the case stronger for performing the optimal collective measurement at the channel output using the systematic scheme of BPQM.

In Fig. 2, we had plotted the block error probabilities as a function of the mean photon number per mode for the different measurement strategies. In Fig. 4, we plot both the bit and block error probabilities (and success probabilities, i.e., one minus error probability) for these measurement strategies. For strategy (a), the performance of the collective Helstrom measurement is plotted using the YKL conditions¹⁹ as discussed, for example, in²¹. For strategies (c) and (d), classical processing is performed essentially for the BSC induced by measuring each qubit output by the pure-state channel. The mean photon number per mode, N , relates to the pure-state channel parameter θ as $\cos \theta = e^{-2N}$ (e.g., see¹³ for more information on this quantity). We make the following observations from these performance curves.

- (1) The block error rates are in increasing order from strategy (a) to (d), as we might expect. Even though classical BP is performed on a tree FG here, it only implements bit-MAP decoding and not block-MAP decoding. This is why it performs worse than block ML (i.e., block MAP with uniform prior on codewords) in this case.
- (2) BPQM performs strictly better than symbol-by-symbol optimal detection followed by classical MAP decoding. This gives a clear demonstration that if one physically constructs a receiver for BPQM, then it will be the best known physically realizable receiver for the pure-state channel. For example, the Dolinar receiver^{13,16} realizes only strategy (c). One can use our circuits to make such a physical realization.
- (3) BPQM performs as well as the quantum optimal collective Helstrom measurement on the outputs of the channel. This lends evidence to the conclusion that by passing quantum messages, BPQM is able to behave like a collective measurement while still making only single-qubit Pauli measurements during the process. However, more careful analysis is required to characterize this in general for, say, the family of codes with tree FGs.
- (4) As a first self-consistency check, we observe that the block-ML curve asymptotes at roughly 0.875 for low mean photon

numbers per mode. This is because, in this regime, the BSC induced by the symbol-by-symbol measurement essentially has a bit-flip rate of 0.5. Therefore, block ML computes a posterior that is almost uniform on all codewords, and thus the block success probability is $1/|C| = 1/8 = 0.125$.

- (5) As another self-consistency check, we note that the BP curve asymptotes at roughly $(1 - 1/32) = 0.9688$ for low mean photon numbers per mode. Since BP performs bit-MAP on this FG, and the induced BSC in this regime flips bits at a rate of almost 0.5, BP essentially picks each bit uniformly at random, thereby returning a vector that is uniformly at random out of all the possible $2^5 = 32$ vectors of length 5.
- (6) The bit error probability plots show that even though BPQM is optimal for bits x_2 through x_5 , it still performs slightly poorly when compared to the performance for x_1 . This might be attributed to the fact that in the chosen parity-check matrix, bit x_1 is involved in both checks whereas the other bits are involved in exactly one of the two checks.

CQ polar codes are known to achieve capacity on CQ channels when paired with a quantum successive cancellation decoder^{13,31}. It remains to be seen if the same is also true for a BPQM-based decoder. Though this is mentioned²⁴, we think this requires more details in the form of an explicit proof. The quantum optimality of BPQM shown in this paper for the example 5-bit code bodes well for BPQM in this regard. It also remains open as to how BPQM can be generalized to FGs with cycles and also for decoding over general CQ channels. We have shown that the coherent rotation we introduced after measuring the first bit plays an important role in BPQM's optimality (see Remark 2). Hence, one needs to refine Renes' definition of the BPQM algorithm in more general settings. BPQM also has close connections with the recently introduced notion of channel duality³². The resulting entropic relations could help characterize the performance of a code over a channel using the performance of its dual code over the dual channel. Since the dual of the pure-state channel is the classical BSC, we believe it may be possible to extend classical techniques for analyzing BP (on BSC), such as density evolution, to analyze BPQM as well.

Leveraging optical realizations of "cat basis" quantum logic, i.e., single- and two-qubit quantum gates in the span of coherent states $|\beta\rangle$ and $|\!-\!\beta\rangle$ ^{33,34}, our BPQM quantum circuit can be translated into the first fully structured optical receiver that would attain the quantum limit of minimum-error discrimination of more than two coherent states. Since there is a proven CQ performance gap as discussed above, implementing our receiver on an optical quantum processor provides an alternative proposal for a quantum supremacy experiment that is distinct from the conventional proposals based on random circuits³⁵.

METHODS

In this section, we will analyze the BPQM algorithm on the example 5-bit code shown in Fig. 1. See Supplementary Note 1 for a review of decoding classical linear codes using the BP algorithm. It is very useful to interpret the node operations in BP as performing local statistical inference over certain induced channels, and this perspective is explained in Supplementary Note 2. This interpretation is also extended to CQ channels as first described by Renes in ref.²⁴. Then Supplementary Note 3 introduces the pure-state channel and describes the BPQM algorithm via its node operations. The relevant node convolution operations are performed in detail in Supplementary Note 6 for completeness.

Decoding bit 1

Let us begin by describing the procedure to decode bit 1 of the 5-bit code from Fig. 1. Observe that the codewords belonging to the code are

$$C = \{00000, 00011, 01100, 01111, 10101, 10110, 11001, 11010\}. \quad (3)$$

We assume that all the codewords are equally likely to be transmitted, just

as in classical BP. Then the task of decoding the value of the first bit x_1 involves distinguishing between the density matrices $\rho_1^{(0)}$ and $\rho_1^{(1)}$, which are uniform mixtures of the states corresponding to the codewords that have $x_1 = 0$ and $x_1 = 1$, respectively, i.e.,

$$\rho_1^{(0)} = |\theta\rangle\langle\theta|_1 \otimes \frac{1}{2} [|\theta\rangle\langle\theta|_2 \otimes |\theta\rangle\langle\theta|_3 \otimes |\theta\rangle\langle\theta|_4 \otimes |\theta\rangle\langle\theta|_5 + |\theta\rangle\langle\theta|_2 \otimes |\theta\rangle\langle\theta|_3 \otimes |\!-\!\theta\rangle\langle\!-\!\theta|_4 \otimes |\!-\!\theta\rangle\langle\!-\!\theta|_5 + |\!-\!\theta\rangle\langle\!-\!\theta|_2 \otimes |\!-\!\theta\rangle\langle\!-\!\theta|_3 \otimes |\theta\rangle\langle\theta|_4 \otimes |\theta\rangle\langle\theta|_5 + |\!-\!\theta\rangle\langle\!-\!\theta|_2 \otimes |\!-\!\theta\rangle\langle\!-\!\theta|_3 \otimes |\!-\!\theta\rangle\langle\!-\!\theta|_4 \otimes |\!-\!\theta\rangle\langle\!-\!\theta|_5]. \quad (4)$$

$$\rho_1^{(1)} = |\!-\!\theta\rangle\langle\!-\!\theta|_1 \otimes \frac{1}{2} [|\theta\rangle\langle\theta|_2 \otimes |\!-\!\theta\rangle\langle\!-\!\theta|_3 \otimes |\theta\rangle\langle\theta|_4 \otimes |\!-\!\theta\rangle\langle\!-\!\theta|_5 + |\theta\rangle\langle\theta|_2 \otimes |\!-\!\theta\rangle\langle\!-\!\theta|_3 \otimes |\!-\!\theta\rangle\langle\!-\!\theta|_4 \otimes |\theta\rangle\langle\theta|_5 + |\!-\!\theta\rangle\langle\!-\!\theta|_2 \otimes |\theta\rangle\langle\theta|_3 \otimes |\theta\rangle\langle\theta|_4 \otimes |\!-\!\theta\rangle\langle\!-\!\theta|_5 + |\!-\!\theta\rangle\langle\!-\!\theta|_2 \otimes |\theta\rangle\langle\theta|_3 \otimes |\!-\!\theta\rangle\langle\!-\!\theta|_4 \otimes |\theta\rangle\langle\theta|_5]. \quad (5)$$

These density matrices can be written in terms of the FN channel convolution in (Eq. 19) of the Supplementary material as $\rho_1^{x_1} = \rho_{\pm} = |\pm\theta\rangle\langle\pm\theta|_1 \otimes [W \boxtimes W](x_1)_{23} \otimes [W \boxtimes W](x_1)_{45}$, where we use the notation $\pm \equiv (-1)^{x_1}$, $x_1 \in \{0, 1\}$.

The BPQM circuit for decoding x_1 is shown in Fig. 5 along with the density matrix in each stage of the circuit denoted by (a) through (e).

- (a) $\rho_{\pm,a} = |\pm\theta\rangle\langle\pm\theta|_1 \otimes [W \boxtimes W](x_1)_{23} \otimes [W \boxtimes W](x_1)_{45}$.
- (b) $\rho_{\pm,b} = |\pm\theta\rangle\langle\pm\theta|_1 \otimes \sum_{j \in \{0,1\}} p_j |\pm\theta_j^{\boxtimes}\rangle\langle\pm\theta_j^{\boxtimes}|_2 \otimes |j\rangle\langle j|_3 \otimes \sum_{k \in \{0,1\}} p_k |\pm\theta_k^{\boxtimes}\rangle\langle\pm\theta_k^{\boxtimes}|_4 \otimes |k\rangle\langle k|_5$.
- (c) $\rho_{\pm,c} = |\pm\theta\rangle\langle\pm\theta|_1 \otimes \sum_{j,k \in \{0,1\}} p_j p_k |\pm\theta_j^{\boxtimes}\rangle\langle\pm\theta_j^{\boxtimes}|_2 \otimes |\pm\theta_k^{\boxtimes}\rangle\langle\pm\theta_k^{\boxtimes}|_3 \otimes |j\rangle\langle j|_4 \otimes |k\rangle\langle k|_5$.
- (d) $\sigma_{\pm} = \sum_{j,k \in \{0,1\}} p_j p_k |\pm\theta\rangle\langle\pm\theta|_1 \otimes |\pm\theta_j^{\boxtimes}\rangle\langle\pm\theta_j^{\boxtimes}|_2 \otimes |0\rangle\langle 0|_3 \otimes |jk\rangle\langle jk|_{45}$, where the applied unitary operation is $U := \sum_{j,k \in \{0,1\}} U_{\theta}(\theta_j^{\boxtimes}, \theta_k^{\boxtimes})_{23} \otimes |jk\rangle\langle jk|_{45}$ and $\cos \theta_j^{\boxtimes} := \cos \theta_j^{\boxtimes} \cos \theta_k^{\boxtimes}$.
- (e) $\Psi_{\pm} = \sum_{j,k \in \{0,1\}} p_j p_k |\pm\varphi_j^{\boxtimes}\rangle\langle\pm\varphi_j^{\boxtimes}|_1 \otimes |0\rangle\langle 0|_2 \otimes |0\rangle\langle 0|_3 \otimes |jk\rangle\langle jk|_{45}$, where the applied unitary operation is $V := \sum_{j,k \in \{0,1\}} U_{\theta}(\theta, \theta_j^{\boxtimes})_{12} \otimes |jk\rangle\langle jk|_{45}$ and $\cos \varphi_j^{\boxtimes} := \cos \theta \cos \theta_j^{\boxtimes}$.

We emphasize that at each stage, the density matrix is the expectation over all pure states obtained there that correspond to transmitted codewords with the first bit taking value $x_1 \in \{0, 1\}$. The operations U and V are effectively two-qubit unitary operations, albeit controlled ones, and this phenomenon extends to any factor graph. Evidently, BPQM compresses all the quantum information into system 1 and the problem reduces to distinguishing between $\Psi_{\pm}^{(1)} = \sum_{j,k \in \{0,1\}} p_j p_k |\pm\varphi_j^{\boxtimes}\rangle\langle\pm\varphi_j^{\boxtimes}|_1$, since the other systems are either trivial or completely classical and independent of x_1 . Finally, system 1 is measured by projecting onto the Pauli X basis, which we know from the discussion in Supplementary Note 3.2 after (31) to be the Helstrom measurement to optimally distinguish between the states $\Psi_{\pm}^{(1)}$.

It is pertinent that the optimal success probability of distinguishing between the density matrices $\rho_1^{(0)}$ and $\rho_1^{(1)}$ using a collective Helstrom

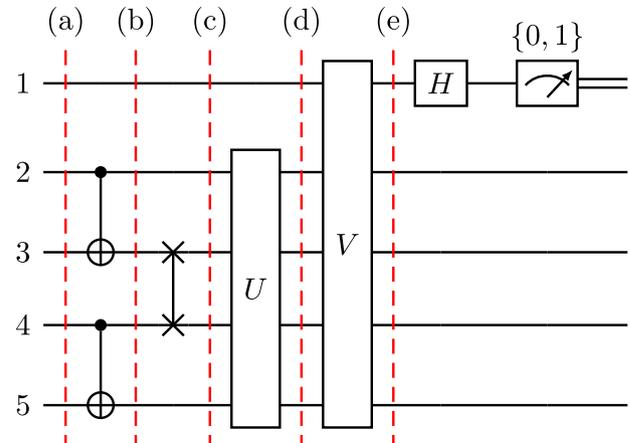


Fig. 5 The BPQM circuit to decode bit 1 of the 5-bit code in Fig. 1. All circuits are drawn using the "Quantikz" package³⁶.

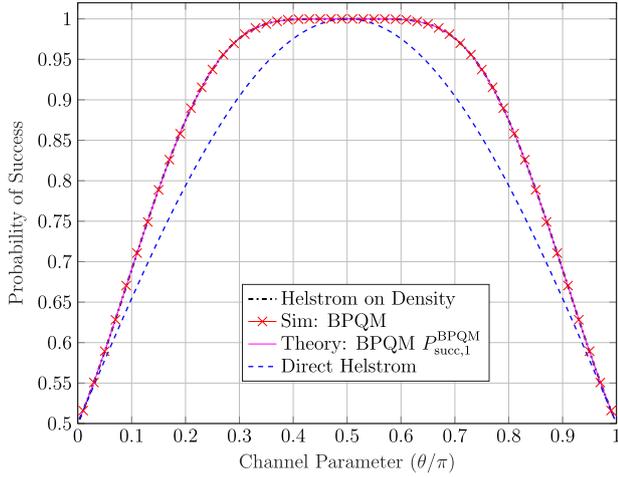


Fig. 6 The success probabilities for decoding the value of x_1 in the 5-bit code. Here, “Helstrom on Density” represents $P_{\text{succ},1}^{\text{Hel}}$ and “Direct” represents the success probability when directly implementing the Helstrom measurement at the channel output on system 1. The curve “Sim: BPQM” corresponds to a simulation that averaged each data point over 10^5 codewords.

measurement is given by

$$P_{\text{succ},1}^{\text{Hel}} = \frac{1}{2} + \frac{1}{4} \|\rho_1^{(0)} - \rho_1^{(1)}\|_1, \quad \|M\|_1 := \text{Tr}(\sqrt{M^{\dagger}M}). \quad (6)$$

The action of BPQM until the final measurement is unitary and the trace norm $\|\cdot\|_1$ is invariant under unitaries. Thus, BPQM does not lose optimality until the final measurement. Since the final measurement is also optimal for distinguishing the two possible states at that stage (e), BPQM is indeed optimal in decoding the value of x_1 . Thus, despite not performing a collective measurement, but rather only a single-qubit measurement at the end of a sequence of unitaries motivated by the FG structure and induced channels in classical BP, BPQM is still optimal to determine whether $x_1 = 0$ or 1. The performance curves plotted in Fig. 6 demonstrate this optimality.

Remark 1 Observe that in this quantum scenario, $\rho_1^{(x)}$ behave like a “posterior” for bit x_1 . However, these can be written down even before transmitting over the channel since they do not depend on the output of the channel. Hence, it is unclear if there is a better notion of a true posterior which we can then show to be “marginalized” by BPQM.

We now analyze the performance of the receiver in decoding bit 1. The probability to decode it as $\hat{x}_1 = 0$ is

$$P[\hat{x}_1 = 0 | \Psi_{\pm}^{(1)}] = \text{Tr}[\Psi_{\pm}^{(1)} |+\rangle \langle +|] = \sum_{j,k \in \{0,1\}^2} p_j p_k \left(\frac{1 \pm \sin \varphi_{jk}^{\otimes}}{2} \right). \quad (7)$$

Therefore, since there are four codewords each that have $x_1 = 0$ and $x_1 = 1$, the prior for bit x_1 is $1/2$ and the probability of success for BPQM in decoding the bit x_1 is

$$P_{\text{succ},1}^{\text{BPQM}} = \mathbb{P}[x_1 = 0] \cdot \mathbb{P}[\hat{x}_1 = 0 | x_1 = 0] + \mathbb{P}[x_1 = 1] \cdot \mathbb{P}[\hat{x}_1 = 1 | x_1 = 1] \quad (8)$$

$$= \frac{1}{2} \left[\sum_{j,k \in \{0,1\}^2} p_j p_k \left(\frac{1 + \sin \varphi_{jk}^{\otimes}}{2} \right) + \sum_{j,k \in \{0,1\}^2} p_j p_k \left(\frac{1 - \sin \varphi_{jk}^{\otimes}}{2} \right) \right] \quad (9)$$

$$= \frac{p_0^2}{2} (1 + \sin \varphi_{00}^{\otimes}) + (1 - p_0^2) \quad (10)$$

$$= 1 - \frac{p_0^2}{2} (1 - \sin \varphi_{00}^{\otimes}), \quad (11)$$

where we have used the fact that since all channels are identically W , we have $\cos \theta_{00}^{\otimes} = 0$. We can calculate

$$\cos \varphi_{00}^{\otimes} = \cos \theta \cos \theta_{00}^{\otimes} = \cos \theta \cos^2 \theta_0^{\otimes} = \cos \theta \frac{4 \cos^2 \theta}{(1 + \cos^2 \theta)^2} \quad (12)$$

$$\Rightarrow \sin \varphi_{00}^{\otimes} = \sqrt{1 - \frac{16 \cos^6 \theta}{(1 + \cos^2 \theta)^4}} = \sqrt{1 - \frac{(2p_0 - 1)^3}{p_0^4}} = \frac{\sqrt{p_0^4 - (2p_0 - 1)^3}}{p_0^2}. \quad (13)$$

Substituting back, we get the BPQM probability of success for bit x_1 to be

$$P_{\text{succ},1}^{\text{BPQM}} = 1 - \frac{p_0^2 - \sqrt{p_0^4 - (2p_0 - 1)^3}}{2} = P_{\text{succ},1}^{\text{Hel}}, \quad (14)$$

which is the curve plotted as “Theory: BPQM $P_{\text{succ},1}^{\text{BPQM}}$ ” in Fig. 6.

Before measuring system 1, the state of system 1 is essentially $\Psi_{\pm}^{(1)} = p_0^2 |\pm \varphi_{00}^{\otimes}\rangle \langle \pm \varphi_{00}^{\otimes}| + (1 - p_0^2) |\pm\rangle \langle \pm|$, since $\cos \varphi_{jk}^{\otimes} = 0$ whenever either j or k equals 1 (or both) and hence $|\pm \varphi_{jk}^{\otimes}\rangle \langle \pm \varphi_{jk}^{\otimes}| = |\pm\rangle \langle \pm|$. So, p_0^2 is the probability that the system “confuses” the decoder, and projection onto the X basis essentially replaces the system with $|m_1\rangle \langle m_1|$, where $m_1 = (-1)^{x_1} \in \{+, -\}$. The full postmeasurement state is given by quantum mechanics to be

$$\Phi_{m_1} = \sum_{j,k \in \{0,1\}^2} p_j p_k \frac{|\langle m_1 | \pm \varphi_{jk}^{\otimes} \rangle|^2}{\text{Tr}[\Psi_{\pm}^{(1)} |m_1\rangle \langle m_1|]} |m_1\rangle \langle m_1|_1 \otimes |00\rangle \langle 00|_{23} \otimes |jk\rangle \langle jk|_{45}. \quad (15)$$

Note that in Fig. 5, we need to apply a Hadamard after the Z-basis measurement in order to ensure that the effective projector is $H|\hat{x}_1\rangle \langle \hat{x}_1| H = |m_1\rangle \langle m_1|$.

Let us denote the overall unitary operation performed in Fig. 5 until stage (e) as B_1^{BPQM} . As mentioned earlier, the Helstrom measurement to optimally distinguish between $\rho_1^{(0)}$ and $\rho_1^{(1)}$ is given by the POVM $\{\Pi_1^{\text{Hel}}, \mathbb{I} - \Pi_1^{\text{Hel}}\}$, where

$$\Pi_1^{\text{Hel}} := \sum_{i:\lambda_i \geq 0} |i\rangle \langle i|, \quad (\rho_1^{(0)} - \rho_1^{(1)})|i\rangle = \lambda_i |i\rangle. \quad (16)$$

BPQM performs the final Helstrom measurement given by the POVM $\{\tilde{\Pi}_1^{\text{Hel}}, \mathbb{I} - \tilde{\Pi}_1^{\text{Hel}}\}$, where

$$\tilde{\Pi}_1^{\text{Hel}} := \sum_{j:\lambda_j \geq 0} |j\rangle \langle j| = |+\rangle \langle +|_1 \otimes (I_{16})_{2345}, \quad (\Psi_+ - \Psi_-)|j\rangle = \lambda_j |j\rangle \quad (17)$$

$$\Rightarrow [B_1^{\text{BPQM}} \rho_1^{(0)} (B_1^{\text{BPQM}})^{\dagger} - B_1^{\text{BPQM}} \rho_1^{(1)} (B_1^{\text{BPQM}})^{\dagger}] |j\rangle = \lambda_j |j\rangle \quad (18)$$

$$\Rightarrow (\rho_1^{(0)} - \rho_1^{(1)}) (B_1^{\text{BPQM}})^{\dagger} |j\rangle = \lambda_j (B_1^{\text{BPQM}})^{\dagger} |j\rangle. \quad (19)$$

Thus, we can express the eigenvectors for $(\rho_1^{(0)} - \rho_1^{(1)})$ as $|i\rangle = (B_1^{\text{BPQM}})^{\dagger} |j\rangle$. This further implies that

$$\Pi_1^{\text{Hel}} = \sum_{i:\lambda_i \geq 0} |i\rangle \langle i| = (B_1^{\text{BPQM}})^{\dagger} \left[\sum_{j:\lambda_j \geq 0} |j\rangle \langle j| \right] B_1^{\text{BPQM}} = (B_1^{\text{BPQM}})^{\dagger} [|+\rangle \langle +|_1 \otimes (I_{16})_{2345}] B_1^{\text{BPQM}}. \quad (20)$$

Hence, in order to identically apply the Helstrom measurement Π_1^{Hel} , BPQM needs to first apply B_1^{BPQM} , then measure the first qubit in the X -basis, and finally invert B_1^{BPQM} on the postmeasurement state Φ_{m_1} above. Although this is optimal for bit 1, next we will see that it is beneficial to coherently rotate Φ_{m_1} before inverting B_1^{BPQM} , which sets up a better state discrimination problem for decoding bit 2.

Decoding bits 2 and 3 (or 4 and 5)

Next, in order to execute BPQM to decode bit x_2 , we would ideally hope to change the state Φ_{m_1} back to the channel outputs. However, this is impossible after having performed the measurement. In the original BPQM algorithm²⁴, the procedure to be performed at this stage is ambiguous, so we describe a strategy that treads closely along the path of performing the Helstrom measurement for bit 2 as well, i.e., optimally distinguishing $\rho_2^{(0)}$ and $\rho_2^{(1)}$ evolved through $\tilde{A}_1^{\text{BPQM}} := (B_1^{\text{BPQM}})^{\dagger} [|m_1\rangle \langle m_1|_1 \otimes (I_{16})_{2345}] B_1^{\text{BPQM}}$.

In order to be able to run BPQM for bit x_1 in reverse to get “as close” to the channel outputs as possible, we need to make sure that the state Φ_{m_1} is modified to be compatible with the (angles used to define the) unitaries V and U in Fig. 5. Since we can keep track of the intermediate angles deterministically, we can conditionally rotate subsystem 1 to be $|m_1 \varphi_{00}^{\otimes}\rangle \langle m_1 \varphi_{00}^{\otimes}|_1$ for $|jk\rangle \langle jk|_{45} = |00\rangle \langle 00|_{45}$. Note again that in Ψ_{\pm} , when either of j or k is 1 (or both), $\varphi_{jk}^{\otimes} = \pi/2$ and hence $|\pm \varphi_{jk}^{\otimes}\rangle \langle \pm \varphi_{jk}^{\otimes}| = |\pm\rangle \langle \pm|$. Therefore, if \hat{x}_1 is the wrong estimate for x_1 , then $\langle m_1 | \pm \rangle = 0$ and the superposition in Φ_{m_1} collapses to a single term with $j = k = 0$.

More precisely, we can implement the unitary operation (see Supplementary Note 5 for a decomposition of K_{m_1})

$$M_{m_1} := (K_{m_1})_1 \otimes |00\rangle\langle 00|_{45} + (I_2)_1 \otimes (|01\rangle\langle 01|_{45} + |10\rangle\langle 10|_{45} + |11\rangle\langle 11|_{45}), \quad (21)$$

where K_+ and K_- are unitaries chosen to satisfy $K_+|+\rangle = |\varphi_{00}^{\otimes}\rangle$ and $K_-|-\rangle = |-\varphi_{00}^{\otimes}\rangle$, respectively. We can easily complete these partially defined unitaries with the conditions $K_+|-\rangle = \sin\frac{\varphi_{00}^{\otimes}}{2}|0\rangle - \cos\frac{\varphi_{00}^{\otimes}}{2}|1\rangle$ and $K_-|+\rangle = \sin\frac{\varphi_{00}^{\otimes}}{2}|0\rangle + \cos\frac{\varphi_{00}^{\otimes}}{2}|1\rangle$. Applying M_{m_1} to Φ_{m_1} we get the desired state (compare to state Ψ_{\pm} in stage (e) of Fig. 5)

$$\tilde{\Psi}_{m_1} = \sum_{j,k \in \{0,1\}^2} p_j p_k \frac{|\langle m_1 \pm \varphi_{jk}^{\otimes} \rangle|^2}{\text{Tr}[\Psi_{\pm}^{(1)} |m_1\rangle\langle m_1|]} |m_1 \varphi_{jk}^{\otimes}\rangle \langle m_1 \varphi_{jk}^{\otimes}| \otimes |00\rangle\langle 00|_{23} |jk\rangle\langle jk|_{45}. \quad (22)$$

Now the BPQM circuit for bit x_1 , shown in Fig. 5, can be run in reverse from before the final measurement, i.e., from stage (e) back to stage (a). Hence, the overall operation on the input state in Fig. 5 is

$$A_1^{\text{BPQM}} := (B_1^{\text{BPQM}})^{\dagger} M_{m_1} [|m_1\rangle\langle m_1|_1 \otimes (I_{16})_{2345}] B_1^{\text{BPQM}}. \quad (23)$$

Then we expect the state to be almost the same as the channel outputs, except that system 1 will deterministically be in state $|m_1\theta\rangle\langle m_1\theta|_1$. However, a simple calculation shows that this is not completely true since

the additional factor $\frac{|\langle m_1 \pm \varphi_{jk}^{\otimes} \rangle|^2}{\text{Tr}[\Psi_{\pm}^{(1)} |m_1\rangle\langle m_1|]}$ prevents the density matrix to decompose into a tensor product of two 2-qubit density matrices at stage (b) of Fig. 5. Specifically, when we take $\tilde{\Psi}_{m_1}$ at stage (e) back to stage (b) by inverting the BPQM operations, we arrive at the state

$$\tilde{\rho}_{\pm,b}^{(m_1)} = |m_1\theta\rangle\langle m_1\theta|_1 \otimes \sum_{j,k \in \{0,1\}^2} p_j p_k \frac{|\langle m_1 \pm \varphi_{jk}^{\otimes} \rangle|^2}{\text{Tr}[\Psi_{\pm}^{(1)} |m_1\rangle\langle m_1|]} \left(|m_1\theta_j^{\otimes}\rangle\langle m_1\theta_j^{\otimes}|_2 \otimes |j\rangle\langle j|_3 \right) \otimes \left(|m_1\theta_k^{\otimes}\rangle\langle m_1\theta_k^{\otimes}|_4 \otimes |k\rangle\langle k|_5 \right) \quad (24)$$

$$= \begin{cases} \frac{1}{\tilde{p}_{\text{succ},1}^{(m_1)}} |m_1\theta\rangle\langle m_1\theta|_1 \otimes \sum_{j,k \in \{0,1\}^2} p_j p_k \frac{|\langle m_1 \pm \varphi_{jk}^{\otimes} \rangle|^2}{\text{Tr}[\Psi_{\pm}^{(1)} |m_1\rangle\langle m_1|]} \left(|m_1\theta_j^{\otimes}\rangle\langle m_1\theta_j^{\otimes}|_2 \otimes |j\rangle\langle j|_3 \right) \otimes \left(|m_1\theta_k^{\otimes}\rangle\langle m_1\theta_k^{\otimes}|_4 \otimes |k\rangle\langle k|_5 \right) & \text{if } \hat{x}_1 = x_1, \\ |m_1\theta\rangle\langle m_1\theta|_1 \otimes \left(|m_1\theta_0^{\otimes}\rangle\langle m_1\theta_0^{\otimes}|_2 \otimes |0\rangle\langle 0|_3 \right) \otimes \left(|m_1\theta_0^{\otimes}\rangle\langle m_1\theta_0^{\otimes}|_4 \otimes |0\rangle\langle 0|_5 \right) & \text{if } \hat{x}_1 \neq x_1. \end{cases} \quad (25)$$

Lemma 1 Let $C := (I_2)_1 \otimes \text{CNOT}_{2 \rightarrow 3} \otimes \text{CNOT}_{4 \rightarrow 5}$ and $|\Gamma_{\hat{x}_1}\rangle := \cos\frac{\varphi_0^{\otimes}}{2} |00\rangle + (-1)^{\hat{x}_1} \sin\frac{\varphi_0^{\otimes}}{2} |11\rangle$. Then

$$C \tilde{\rho}_{\pm,b}^{(m_1)} C^{\dagger} = \begin{cases} \frac{1}{\tilde{p}_{\text{succ},1}^{(m_1)}} |m_1\theta\rangle\langle m_1\theta|_1 \otimes [W \boxtimes W](\hat{x}_1)_{23} \otimes [W \boxtimes W](\hat{x}_1)_{45} & \text{if } \hat{x}_1 = x_1, \\ \frac{1}{\tilde{p}_{\text{succ},1}^{(m_1)}} [0.5(1 + \sin\varphi_0^{\otimes}) - 1] |m_1\theta\rangle\langle m_1\theta|_1 \otimes |\Gamma_{\hat{x}_1}\rangle\langle \Gamma_{\hat{x}_1}|_{23} \otimes |\Gamma_{\hat{x}_1}\rangle\langle \Gamma_{\hat{x}_1}|_{45} & \text{if } \hat{x}_1 \neq x_1, \\ |m_1\theta\rangle\langle m_1\theta|_1 \otimes |\Gamma_{\hat{x}_1}\rangle\langle \Gamma_{\hat{x}_1}|_{23} \otimes |\Gamma_{\hat{x}_1}\rangle\langle \Gamma_{\hat{x}_1}|_{45} & \text{if } \hat{x}_1 \neq x_1. \end{cases} \quad (26)$$

Proof We know from the definition of the factor node convolution operation of BPQM that

$$C(|m_1\theta\rangle\langle m_1\theta|_1 \otimes [W \boxtimes W](\hat{x}_1)_{23} \otimes [W \boxtimes W](\hat{x}_1)_{45}) C^{\dagger} = |m_1\theta\rangle\langle m_1\theta|_1 \otimes \left(\sum_{j \in \{0,1\}} p_j |m_1\theta_j^{\otimes}\rangle\langle m_1\theta_j^{\otimes}|_2 \otimes |j\rangle\langle j|_3 \right) \otimes \left(\sum_{k \in \{0,1\}} p_k |m_1\theta_k^{\otimes}\rangle\langle m_1\theta_k^{\otimes}|_4 \otimes |k\rangle\langle k|_5 \right) \quad (27)$$

$$= \rho_{m_1,b}. \quad (28)$$

This in turn implies that $C \tilde{\rho}_{m_1,b} C^{\dagger} = |m_1\theta\rangle\langle m_1\theta|_1 \otimes [W \boxtimes W](\hat{x}_1)_{23} \otimes [W \boxtimes W](\hat{x}_1)_{45}$. Ignoring the first qubit and the constant factor for simplicity, observe that

$$\tilde{\rho}_{\pm,b}^{(m_1)}|_{\hat{x}_1=x_1} = \sum_{j,k \in \{0,1\}^2} p_j p_k \left(\frac{|\langle m_1 \pm \varphi_{jk}^{\otimes} \rangle|^2}{\text{Tr}[\Psi_{\pm}^{(1)} |m_1\rangle\langle m_1|]} - 1 + 1 \right) \left(|m_1\theta_j^{\otimes}\rangle\langle m_1\theta_j^{\otimes}|_2 \otimes |j\rangle\langle j|_3 \right) \otimes \left(|m_1\theta_k^{\otimes}\rangle\langle m_1\theta_k^{\otimes}|_4 \otimes |k\rangle\langle k|_5 \right) \quad (29)$$

$$= \rho_{m_1,b} + p_0^2 [0.5(1 + \sin\varphi_0^{\otimes}) - 1] \left(|m_1\theta_0^{\otimes}\rangle\langle m_1\theta_0^{\otimes}|_2 \otimes |0\rangle\langle 0|_3 \right) \otimes \left(|m_1\theta_0^{\otimes}\rangle\langle m_1\theta_0^{\otimes}|_4 \otimes |0\rangle\langle 0|_5 \right). \quad (30)$$

We have used the fact that except when $j=k=0$, assuming $\hat{x}_1 = x_1$, $\langle m_1 \pm \varphi_{jk}^{\otimes} \rangle = \langle m_1 | m_1 \varphi_{jk}^{\otimes} \rangle = \langle m_1 | m_1 \rangle = 1$. Finally, using

$$x_2 \oplus x_3 = \hat{x}_1$$

$$x_4 \oplus x_5 = \hat{x}_1$$

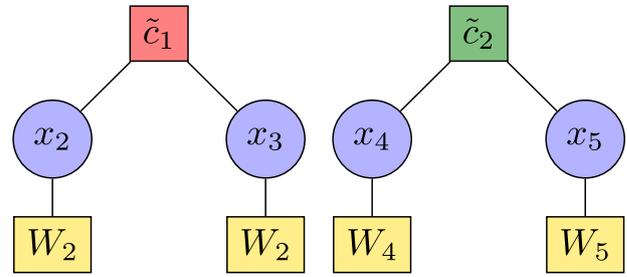


Fig. 7 The reduced factor graph after estimating bit 1 to be \hat{x}_1 . Conditioned on this estimate, the two checks c_1 and c_2 are updated respectively to \tilde{c}_1 and \tilde{c}_2 , which represent the check equations shown above the two subgraphs.

$\text{CNOT}_{2 \rightarrow 3}(|m_1\theta_0^{\otimes}\rangle_2 \otimes |0\rangle_3) = |\Gamma_{\hat{x}_1}\rangle$, the result follows for both cases $\hat{x}_1 = x_1$ and $\hat{x}_1 \neq x_1$. ■

Therefore, after reversing the operations of BPQM for bit x_1 , the 5-qubit system is in the state

$$\tilde{\rho}_{m_1,a} = \rho_{\text{succ},1}^{\text{BPQM}} \cdot C \tilde{\rho}_{\pm,b}^{(m_1)}|_{\hat{x}_1=x_1} C^{\dagger} + (1 - \rho_{\text{succ},1}^{\text{BPQM}}) \cdot C \tilde{\rho}_{\pm,b}^{(m_1)}|_{\hat{x}_1 \neq x_1} C^{\dagger} = |m_1\theta\rangle\langle m_1\theta|_1 \otimes [W \boxtimes W](\hat{x}_1)_{23} \otimes [W \boxtimes W](\hat{x}_1)_{45} \quad (31)$$

$$+ p_0^2 [0.5(1 + \sin\varphi_0^{\otimes}) - 1] |m_1\theta\rangle\langle m_1\theta|_1 \otimes |\Gamma_{\hat{x}_1}\rangle\langle \Gamma_{\hat{x}_1}|_{23} \otimes |\Gamma_{\hat{x}_1}\rangle\langle \Gamma_{\hat{x}_1}|_{45} + (1 - \rho_{\text{succ},1}^{\text{BPQM}}) \cdot |m_1\theta\rangle\langle m_1\theta|_1 \otimes |\Gamma_{\hat{x}_1}\rangle\langle \Gamma_{\hat{x}_1}|_{23} \otimes |\Gamma_{\hat{x}_1}\rangle\langle \Gamma_{\hat{x}_1}|_{45} \quad (32)$$

$$= |m_1\theta\rangle\langle m_1\theta|_1 \otimes [W \boxtimes W](\hat{x}_1)_{23} \otimes [W \boxtimes W](\hat{x}_1)_{45}, \quad (33)$$

since $\rho_{\text{succ},1}^{\text{BPQM}} = p_0^2 \cdot 0.5(1 + \sin\varphi_0^{\otimes}) + (1 - p_0^2)$.

At this point, we have decoded $\hat{x}_1 = 0$ if $m_1 = +$ and $\hat{x}_1 = 1$ if $m_1 = -$. We can absorb the value of \hat{x}_1 in the FG by updating the parity checks c_1 and c_2 to impose $x_2 \oplus x_3 = \hat{x}_1$ and $x_4 \oplus x_5 = \hat{x}_1$, respectively. Now we have two disjoint FGs as shown in Fig. 7. It suffices to decode x_2 and x_4 since $\hat{x}_3 = \hat{x}_2 \oplus \hat{x}_1$ and $\hat{x}_5 = \hat{x}_4 \oplus \hat{x}_1$. Also, due to symmetry, it suffices to analyze the success probability of decoding x_2 (resp. x_4) and x_3 (resp. x_5). For this reduced FG, we need to split $\tilde{\rho}_{m_1,a}$ into two density matrices corresponding to the hypotheses $x_2 = 0$ and $x_2 = 1$. If we revisit the density matrices $\rho_1^{(0)}$ and $\rho_1^{(1)}$, we observe that the 5-qubit system at the channel output is exactly $\frac{1}{2}\rho_1^{(0)} + \frac{1}{2}\rho_1^{(1)}$. Hence, for x_2 , we accordingly split $[W \boxtimes W](\hat{x}_1)_{23}$ in $\tilde{\rho}_{m_1,a}$ and arrive at the two hypotheses states

$$\tilde{\Phi}_{x_2=\hat{x}_1}(\hat{x}_1) = |m_1\theta\rangle\langle m_1\theta|_2 \otimes |\theta\rangle\langle \theta|_3 \otimes [W \boxtimes W](\hat{x}_1)_{45}, \quad (34)$$

$$\tilde{\Phi}_{x_2 \neq \hat{x}_1}(\hat{x}_1) = |-m_1\theta\rangle\langle -m_1\theta|_2 \otimes |-\theta\rangle\langle -\theta|_3 \otimes [W \boxtimes W](\hat{x}_1)_{45}. \quad (35)$$

In Supplementary Note 4, we discuss how these hypotheses must be processed, which makes the next steps of BPQM intuitively clear (see Supplementary Fig. 3). However, the success probability derived from this analysis for bits 2–5 turns out to be significantly higher than the quantum optimal scheme for each bit at the channel output (see Supplementary Fig. 4). This indicates that the state discrimination problem for bit 2 discussed above is more ideal than the actual problem in hand. Hence, next we analyze the true state discrimination problem for bit 2 (or 4) and clarify the observed performance in Supplementary Fig. 4.

Analysis of BPQM optimality for decoding bit 2 (or 4)

At the channel output, it is clear that the optimal strategy to decode bit 2 is to perform the Helstrom measurement that distinguishes between $\rho_2^{(0)}$ and $\rho_2^{(1)}$. However, since we performed BPQM operations to decode bit 1 first, these two density matrices would have evolved through that process. Therefore, the correct analysis is to derive the resulting states and then subject them to the BPQM strategy for decoding bit 2 that was discussed above. For simplicity, we only track the density matrix $\rho_2^{(0)}$ through the different stages in Fig. 8. In Fig. 9, we provide the full expanded BPQM circuit for decoding all bits, and this can be turned into a circuit composed of standard quantum operations by using the decompositions in Figs. 10 and 11. The corresponding states for $\rho_2^{(1)}$ can easily be ascertained from

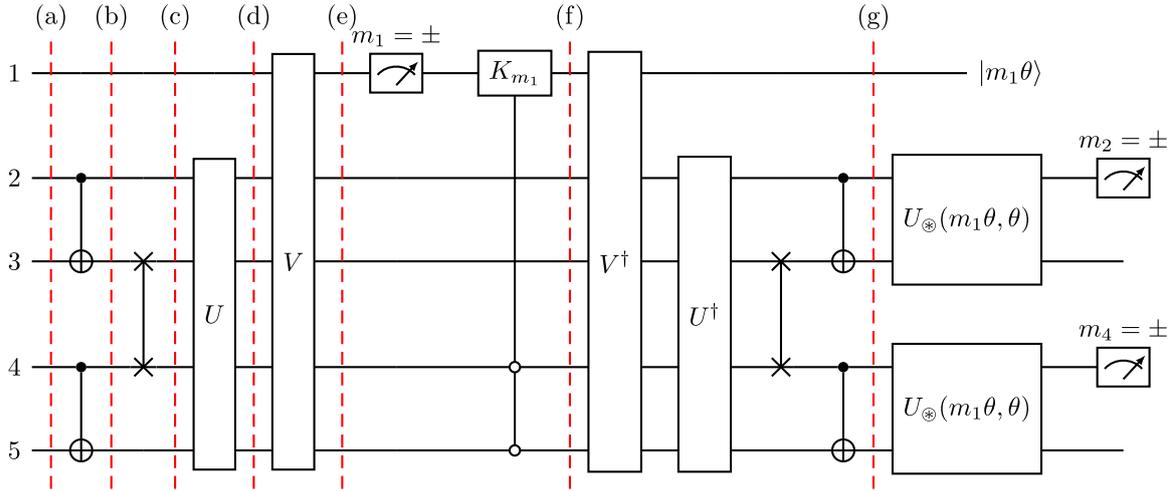


Fig. 8 The full BPQM circuit to decode all bits of the 5-bit code in Fig. 1. The decoded values are related to the measurement results as $m_1 = (-1)^{\hat{x}_1}$, $m_2 = (-1)^{\hat{x}_2}$, $m_4 = (-1)^{\hat{x}_4}$, and $\hat{x}_3 = \hat{x}_1 \oplus \hat{x}_2$, $\hat{x}_5 = \hat{x}_1 \oplus \hat{x}_4$. The open-circled controls indicate that K_{m_1} is coherently controlled by the last two qubits being in the state $|00\rangle_{45}$. The solid line before K_{m_1} indicates that the controlled unitary is applied to the postmeasurement state. See Fig. 9 for the full decomposition of this circuit.

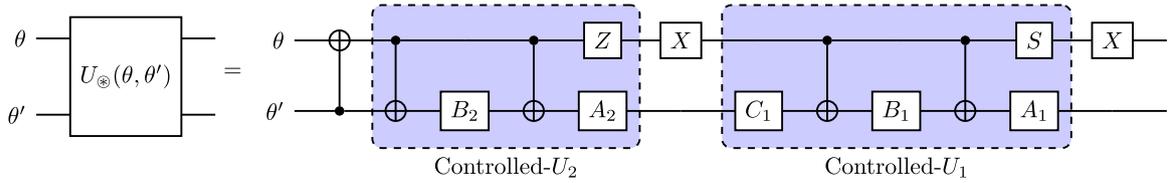


Fig. 9 The circuit decomposition for $U(\theta, \theta')$, where we set $A_1 := R_y(\gamma_1/2)$, $B_1 := R_y(-\gamma_1/2)R_z(-\pi/2)$, $C_1 := R_z(\pi/2)$, $A_2 := R_z(\pi)R_y(\gamma_2/2)$, $B_2 := R_y(-\gamma_2/2)R_z(-\pi)$, and $S = \sqrt{Z}$ is the phase gate. See Supplementary Note 5 for calculations and angles γ_1, γ_2 . Note that, for example, $B_2 = R_y(-\gamma_2/2)R_z(-\pi)$ implies that $R_z(-\pi)$ must be applied first, then followed by $R_y(-\gamma_2/2)$.

these. It will be convenient to express

$$\frac{1}{2}|\theta\rangle\langle\theta|_2 \otimes |\theta\rangle\langle\theta|_3 = [W \boxtimes W](0)_{23} - \frac{1}{2}|\theta\rangle\langle\theta|_2 \otimes |\theta\rangle\langle\theta|_3, \quad (36)$$

$$\frac{1}{2}|\theta\rangle\langle\theta|_2 \otimes |\theta\rangle\langle\theta|_3 = [W \boxtimes W](1)_{23} - \frac{1}{2}|\theta\rangle\langle\theta|_2 \otimes |\theta\rangle\langle\theta|_3. \quad (37)$$

For brevity, we will use the notation $CX_{ij} := \text{CNOT}_{i \rightarrow j}$ and $\text{Swap}_{34} := CX_{34} CX_{43} CX_{34}$. Then we can write

$$\rho_{2,a}^{(0)} = \frac{1}{2}|\theta\rangle\langle\theta|_1 \otimes |\theta\rangle\langle\theta|_2 \otimes |\theta\rangle\langle\theta|_3 \otimes [W \boxtimes W](0)_{45} + \frac{1}{2}|\theta\rangle\langle\theta|_1 \otimes |\theta\rangle\langle\theta|_2 \otimes |\theta\rangle\langle\theta|_3 \otimes [W \boxtimes W](1)_{45}, \quad (38)$$

$$\begin{aligned} \rho_{2,b}^{(0)} &= |\theta\rangle\langle\theta|_1 \otimes \left[\sum_{j=0,1} p_j |\theta_j^{\oplus}\rangle \langle\theta_j^{\oplus}| \otimes |j\rangle\langle j| - \frac{1}{2}CX_{23}|\theta, -\theta\rangle\langle\theta, -\theta|_{23} CX_{23} \right] \\ &\otimes \left[\sum_{k=0,1} p_k |\theta_k^{\oplus}\rangle \langle\theta_k^{\oplus}| \otimes |k\rangle\langle k| \right] + |\theta\rangle\langle\theta|_1 \\ &\otimes \left[\sum_{j=0,1} p_j |\theta_j^{\ominus}\rangle \langle\theta_j^{\ominus}| \otimes |j\rangle\langle j| - \frac{1}{2}CX_{23}|\theta, \theta\rangle\langle\theta, \theta|_{23} CX_{23} \right] \\ &\otimes \left[\sum_{k=0,1} p_k |\theta_k^{\ominus}\rangle \langle\theta_k^{\ominus}| \otimes |k\rangle\langle k| \right], \end{aligned} \quad (39)$$

$$\begin{aligned} \rho_{2,c}^{(0)} &= |\theta\rangle\langle\theta|_1 \otimes \sum_{j,k \in \{0,1\}^2} p_j p_k |\theta_j^{\oplus}\rangle \langle\theta_j^{\oplus}| \otimes |\theta_k^{\oplus}\rangle \langle\theta_k^{\oplus}| \otimes |j\rangle\langle j| \otimes |k\rangle\langle k| \\ &- \frac{1}{2}|\theta\rangle\langle\theta|_1 \otimes \text{Swap}_{34} \left[CX_{23}|\theta, -\theta\rangle\langle\theta, -\theta|_{23} CX_{23} \otimes \sum_{k=0,1} p_k |\theta_k^{\oplus}\rangle \langle\theta_k^{\oplus}| \otimes |k\rangle\langle k| \right] \text{Swap}_{34} \\ &+ |\theta\rangle\langle\theta|_1 \otimes \sum_{j,k \in \{0,1\}^2} p_j p_k |\theta_j^{\oplus}\rangle \langle\theta_j^{\oplus}| \otimes |\theta_k^{\ominus}\rangle \langle\theta_k^{\ominus}| \otimes |j\rangle\langle j| \otimes |k\rangle\langle k| \\ &- \frac{1}{2}|\theta\rangle\langle\theta|_1 \otimes \text{Swap}_{34} \left[CX_{23}|\theta, \theta\rangle\langle\theta, \theta|_{23} CX_{23} \otimes \sum_{k=0,1} p_k |\theta_k^{\oplus}\rangle \langle\theta_k^{\oplus}| \otimes |k\rangle\langle k| \right] \text{Swap}_{34}, \end{aligned} \quad (40)$$

$$\begin{aligned} \rho_{2,e}^{(0)} &= \sum_{j,k \in \{0,1\}^2} p_j p_k |\varphi_{jk}^{\oplus}\rangle \langle\varphi_{jk}^{\oplus}| \otimes |0\rangle\langle 0|_2 \otimes |0\rangle\langle 0|_3 \otimes |j\rangle\langle j|_4 \otimes |k\rangle\langle k|_{45} \\ &+ \sum_{j,k \in \{0,1\}^2} p_j p_k |\varphi_{jk}^{\ominus}\rangle \langle\varphi_{jk}^{\ominus}| \otimes |0\rangle\langle 0|_2 \otimes |0\rangle\langle 0|_3 \otimes |j\rangle\langle j|_4 \otimes |k\rangle\langle k|_{45} \\ &- \frac{1}{2}VU \left\{ |\theta\rangle\langle\theta|_1 \otimes \text{Swap}_{34} \left[CX_{23}|\theta, -\theta\rangle\langle\theta, -\theta|_{23} CX_{23} \otimes \sum_{k=0,1} p_k |\theta_k^{\oplus}\rangle \langle\theta_k^{\oplus}| \otimes |k\rangle\langle k| \right] \text{Swap}_{34} \right. \\ &\left. + |\theta\rangle\langle\theta|_1 \otimes \text{Swap}_{34} \left[CX_{23}|\theta, \theta\rangle\langle\theta, \theta|_{23} CX_{23} \otimes \sum_{k=0,1} p_k |\theta_k^{\ominus}\rangle \langle\theta_k^{\ominus}| \otimes |k\rangle\langle k| \right] \text{Swap}_{34} \right\} U^\dagger V. \end{aligned} \quad (41)$$

Next, we make an X -basis measurement on the first qubit, and for convenience we assume that the measurement result is $m_1 = +$. The analysis for $m_1 = -$ is very similar and follows by symmetry. We verified numerically that $\text{Tr} \left[|+\rangle\langle +| \cdot \rho_{2,e}^{(0)} \right] = 0.5$, which we might intuitively expect since $\rho_{2,e}^{(0)}$ is the density matrix for $x_2 = 0$ and x_2 is independent from x_1 . Since $m_1 = +$, we follow the measurement with the conditional rotation M_+ in (Eq. 21) to obtain

$$\begin{aligned} \Phi_{2,m_1=+}^{(0)} &= \frac{1}{\sqrt{5}} \left[\sum_{j,k \in \{0,1\}^2} p_j p_k \langle + | \varphi_{jk}^{\oplus} \rangle |\varphi_{jk}^{\oplus}\rangle \otimes |0\rangle\langle 0|_2 \otimes |0\rangle\langle 0|_3 \otimes |j\rangle\langle j|_4 \otimes |k\rangle\langle k|_{45} \right. \\ &+ \frac{p_0^2(1 - \sin\varphi_{00}^{\oplus})}{2} |\varphi_{00}^{\oplus}\rangle \langle\varphi_{00}^{\oplus}| \otimes |0\rangle\langle 0|_2 \otimes |0\rangle\langle 0|_3 \otimes |00\rangle\langle 00|_{45} \\ &\left. - \frac{1}{2}M_+ |+\rangle \langle + | V U \Lambda_2^{(0)} U^\dagger V |+\rangle \langle + | M_+^\dagger \right], \end{aligned} \quad (42)$$

$$\begin{aligned} \Lambda_2^{(0)} &:= |\theta\rangle\langle\theta|_1 \otimes \text{Swap}_{34} \left[CX_{23}|\theta, -\theta\rangle\langle\theta, -\theta|_{23} CX_{23} \otimes \sum_{k=0,1} p_k |\theta_k^{\oplus}\rangle \langle\theta_k^{\oplus}| \otimes |k\rangle\langle k| \right] \text{Swap}_{34} \\ &+ |\theta\rangle\langle\theta|_1 \otimes \text{Swap}_{34} \left[CX_{23}|\theta, \theta\rangle\langle\theta, \theta|_{23} CX_{23} \otimes \sum_{k=0,1} p_k |\theta_k^{\ominus}\rangle \langle\theta_k^{\ominus}| \otimes |k\rangle\langle k| \right] \text{Swap}_{34}. \end{aligned} \quad (43)$$

This is the state at stage (f) in Fig. 8. Hence, for $x_2 = 0$, the density matrix we have when $\hat{x}_1 = 0$ and we reverse the BPQM operations on

$$\Phi_{2,m_1=+}^{(0)} \text{ is}$$

$$\tilde{\rho}_{2,m_1=+}^{(0)} = \frac{1}{0.5} \left[|\theta\rangle\langle\theta|_1 \otimes |W \boxtimes W\rangle\langle 0\rangle_{23} \otimes |W \boxtimes W\rangle\langle 0\rangle_{45} \right. \\ \left. - \frac{1}{2} \text{CX}_{23} \text{CX}_{45} \text{Swap}_{34} U^\dagger V^\dagger M_+ |+\rangle \langle +|_1 M_+^\dagger VUSwap_{34} \text{CX}_{45} \text{CX}_{23} \right]. \quad (44)$$

This is the state at stage (g) in Fig. 8. So, this is the actual density matrix that BPQM encounters for $x_2 = 0$ after having estimated $\hat{x}_1 = 0$. When compared with the earlier analysis, we observe numerically that this is close to $\tilde{\Phi}_{x_2=\hat{x}_1}(\hat{x}_1)$ but is not exactly the same. For example, when $\theta = 0.1\pi$, we find that $\left\| \tilde{\rho}_{2,m_1=+}^{(0)} - \tilde{\Phi}_{x_2=0}^{(0)} \right\|_{\text{Fro}} = 0.0542$, where ‘‘Fro’’ denotes the Frobenius norm, and only two of the distinct entries differ (slightly). Similarly,

$$\tilde{\rho}_{2,m_1=+}^{(1)} = \frac{1}{0.5} \left[|\theta\rangle\langle\theta|_1 \otimes |W \boxtimes W\rangle\langle 0\rangle_{23} \otimes |W \boxtimes W\rangle\langle 0\rangle_{45} \right. \\ \left. - \frac{1}{2} \text{CX}_{23} \text{CX}_{45} \text{Swap}_{34} U^\dagger V^\dagger M_+ |+\rangle \langle +|_1 M_+^\dagger VUSwap_{34} \text{CX}_{45} \text{CX}_{23} \right], \quad (45)$$

$$\Lambda_2^{(1)} := |\theta\rangle\langle\theta|_1 \otimes \text{Swap}_{34} \left[\text{CX}_{23} |\theta, \theta\rangle \langle \theta, \theta|_{23} \text{CX}_{23} \otimes \sum_{k=0,1} p_k |\theta_k^{\oplus}\rangle \langle \theta_k^{\oplus}|_4 \otimes |k\rangle \langle k|_5 \right] \text{Swap}_{34} \\ + |-\theta\rangle\langle-\theta|_1 \otimes \text{Swap}_{34} \left[\text{CX}_{23} |-\theta, -\theta\rangle \langle -\theta, -\theta|_{23} \text{CX}_{23} \otimes \sum_{k=0,1} p_k |-\theta_k^{\oplus}\rangle \langle -\theta_k^{\oplus}|_4 \otimes |k\rangle \langle k|_5 \right] \text{Swap}_{34}. \quad (46)$$

However, most importantly, we observe that $\frac{1}{2} \tilde{\rho}_{2,m_1=+}^{(0)} + \frac{1}{2} \tilde{\rho}_{2,m_1=+}^{(1)} = \frac{1}{2} \tilde{\Phi}_{x_2=0}^{(0)} + \frac{1}{2} \tilde{\Phi}_{x_2=1}^{(0)}$. This explains that while the full density matrix $\tilde{\rho}_{2,m_1=+}^{(0)}$ was correct, we had split it incorrectly to arrive at the two hypotheses $\tilde{\Phi}_{x_2=\hat{x}_1}(\hat{x}_1)$ and $\tilde{\Phi}_{x_2 \neq \hat{x}_1}(\hat{x}_1)$. Now, the Helstrom measurement that optimally distinguishes between $\tilde{\rho}_{2,m_1=+}^{(0)}$ and $\tilde{\rho}_{2,m_1=+}^{(1)}$ only depends on

$$\tilde{\rho}_{2,m_1=+}^{(0)} - \tilde{\rho}_{2,m_1=+}^{(1)} = A \left[\Lambda_2^{(1)} - \Lambda_2^{(0)} \right] A^\dagger, \quad A := \text{CX}_{23} \text{CX}_{45} \text{Swap}_{34} U^\dagger V^\dagger M_+ |+\rangle \langle +|_1 VU. \quad (47)$$

By symmetry of $m_1 = +$ and $m_1 = -$, the optimal success probability to decide bit 2 is given by

$$P_{\text{succ},2}^{\text{Hel}} = \frac{1}{2} + \frac{1}{4} \left\| \tilde{\rho}_{2,m_1=+}^{(0)} - \tilde{\rho}_{2,m_1=+}^{(1)} \right\|_1 = \frac{1}{2} + \frac{1}{4} \left\| A \left[\Lambda_2^{(1)} - \Lambda_2^{(0)} \right] A^\dagger \right\|_1 = \frac{1}{2} + \frac{1}{4} \left\| L \left(\rho_2^{(0)} - \rho_2^{(1)} \right) L^\dagger \right\|_1, \quad (48)$$

$$L := \text{CX}_{23} \text{CX}_{45} \text{Swap}_{34} U^\dagger V^\dagger M_+ \frac{|+\rangle \langle +|_1}{\sqrt{0.5}} VUSwap_{34} \text{CX}_{45} \text{CX}_{23}. \quad (49)$$

Since L is not unitary, we cannot directly apply the unitary invariance of the trace norm to conclude that there is no degradation in performance when compared to optimally distinguishing $\rho_2^{(0)}$ and $\rho_2^{(1)}$ at the channel output. However, we observe numerically (even up to 12 significant digits) that the operations in L indeed ensure that $\left\| L \left(\rho_2^{(0)} - \rho_2^{(1)} \right) L^\dagger \right\|_1 = \left\| \rho_2^{(0)} - \rho_2^{(1)} \right\|_1$. Moreover, we also observe that the BPQM operations for bit 2 given in Supplementary Fig. 3 achieve the same success probability, i.e., using the notation $\pm \equiv (-1)^{x_2}$ we have

$$P_{\text{succ},2}^{\text{BPQM}} = \text{Tr} \left[U_{\oplus} (m_1, \theta) \rho_{2,m_1}^{(x_2)} U_{\oplus} (m_1, \theta)^\dagger \cdot |\pm\rangle \langle \pm|_2 \right] \quad (50)$$

$$= \frac{1}{2} + \frac{1}{4} \left\| L \left(\rho_2^{(0)} - \rho_2^{(1)} \right) L^\dagger \right\|_1 \quad (51)$$

$$= \frac{1}{2} + \frac{1}{4} \left\| \rho_2^{(0)} - \rho_2^{(1)} \right\|_1 \quad (52)$$

$$= P_{\text{succ},2}^{\text{Hel}}. \quad (53)$$

Finally, the simulation results in Fig. 4 clearly show that the overall block error rate of BPQM coincides with that of the quantum optimal joint Helstrom limit. It remains open to rigorously prove all of these observations.

Overall performance of BPQM

We can calculate the probability that the full codeword \underline{x} is decoded correctly as

$$P_{\text{succ}}^{\text{BPQM}} = \mathbb{P}[\underline{\hat{x}} = \underline{x}] = \mathbb{P}[\hat{x}_1 = x_1] \cdot \mathbb{P}[\hat{x}_2 = x_2 | \hat{x}_1 = x_1] \cdot \mathbb{P}[\hat{x}_4 = x_4 | \hat{x}_1 = x_1, \hat{x}_2 = x_2] \quad (54)$$

$$= P_{\text{succ},1}^{\text{BPQM}} \cdot P_{\text{succ},2}^{\text{BPQM}} |_{\hat{x}_1=x_1=0} \cdot P_{\text{succ},4}^{\text{BPQM}} |_{\hat{x}_1=x_1=0; \hat{x}_2=x_2=0}. \quad (55)$$

The first term in (Eq. 55) is clearly $P_{\text{succ},1}^{\text{BPQM}} = P_{\text{succ},1}^{\text{Hel}}$. The second term, however, is different from $P_{\text{succ},2}^{\text{BPQM}} = P_{\text{succ},2}^{\text{Hel}}$ because of the conditioning on

x_1 being estimated correctly, whereas in the above analysis we had implicitly averaged over $\hat{x}_1 = x_1$ and $\hat{x}_1 \neq x_1$. Nevertheless, we can use a similar strategy as above to derive an expression for the second term. Here, we want to condition on x_1 being estimated correctly, i.e., $\hat{x}_1 = x_1$, and derive the hypothesis states for x_2 under this scenario. Similarly, for the third term, the additional conditioning on $\hat{x}_2 = x_2$ makes it not equal to the second term, although x_2 and x_4 are placed symmetrically in the factor graph of the code. But it still holds that $P_{\text{succ},2}^{\text{BPQM}} |_{\hat{x}_1=x_1=0} = P_{\text{succ},4}^{\text{BPQM}} |_{\hat{x}_1=x_1=0}$. We perform these two analyses next and then combine them to calculate the full block success probability of BPQM.

We will first analyze the decoding of bit 2 conditioned on bit 1. Let $(\rho_2^{(00)}, \rho_2^{(01)})$, $(\rho_2^{(10)}, \rho_2^{(11)})$ be two pairs of hypothesis states for x_2 , at the channel output, where the first pair is conditioned on $x_1 = 0$ and the second on $x_1 = 1$, and this information is known to the receiver. It is clear, for example, that $\rho_2^{(0x_2)} = |\theta\rangle\langle\theta|_1 \otimes |(-1)^{x_2}\theta\rangle \langle (-1)^{x_2}\theta|_2 \otimes |(-1)^{x_2}\theta\rangle \langle (-1)^{x_2}\theta|_3 \otimes |W \boxtimes W\rangle\langle 0\rangle_{45}$. After similar calculations as before, we finally obtain

$$\tilde{\sigma}_{2,m_1=+}^{(00)} = \frac{1}{P_{\text{succ},1}^{\text{Hel}}} \text{CX}_{23} \text{CX}_{45} \text{Swap}_{34} U^\dagger V^\dagger \\ \left[2 \sum_{j,k \in \{0,1\}^2} p_j p_k \left| \langle + | \varphi_{jk}^{\oplus} \rangle \right|^2 \left| \varphi_{jk}^{\oplus} \right\rangle \langle \varphi_{jk}^{\oplus} | \otimes |0\rangle \langle 0|_2 \otimes |0\rangle \langle 0|_3 \otimes |jk\rangle \langle jk|_{45} \right. \\ \left. - M_+ |+\rangle \langle +|_1 M_+^\dagger \right] VUSwap_{34} \text{CX}_{45} \text{CX}_{23}, \quad (56)$$

$$\Lambda_2^{(0)} := |\theta\rangle\langle\theta|_1 \otimes \text{Swap}_{34} \left[\text{CX}_{23} |-\theta, -\theta\rangle \langle -\theta, -\theta|_{23} \text{CX}_{23} \otimes \sum_{k=0,1} p_k |\theta_k^{\oplus}\rangle \langle \theta_k^{\oplus}|_4 \otimes |k\rangle \langle k|_5 \right] \text{Swap}_{34}. \quad (57)$$

This is the state at stage (g) in Fig. 8. So, this is the actual density matrix that BPQM encounters for $x_2 = 0$ after having estimated correctly that $\hat{x}_1 = x_1 = 0$ (and reversed the first set of operations). Similarly,

$$\tilde{\sigma}_{2,m_1=+}^{(01)} = \frac{1}{P_{\text{succ},1}^{\text{Hel}}} \text{CX}_{23} \text{CX}_{45} \text{Swap}_{34} U^\dagger V^\dagger \\ \left[2 \sum_{j,k \in \{0,1\}^2} p_j p_k \left| \langle + | \varphi_{jk}^{\oplus} \rangle \right|^2 \left| \varphi_{jk}^{\oplus} \right\rangle \langle \varphi_{jk}^{\oplus} | \otimes |0\rangle \langle 0|_2 \otimes |0\rangle \langle 0|_3 \otimes |jk\rangle \langle jk|_{45} \right. \\ \left. - M_+ |+\rangle \langle +|_1 M_+^\dagger \right] VUSwap_{34} \text{CX}_{45} \text{CX}_{23}, \quad (58)$$

$$\Lambda_2^{(1)} := |\theta\rangle\langle\theta|_1 \otimes \text{Swap}_{34} \left[\text{CX}_{23} |\theta, \theta\rangle \langle \theta, \theta|_{23} \text{CX}_{23} \otimes \sum_{k=0,1} p_k |\theta_k^{\oplus}\rangle \langle \theta_k^{\oplus}|_4 \otimes |k\rangle \langle k|_5 \right] \text{Swap}_{34}. \quad (59)$$

The Helstrom measurement that optimally distinguishes between $\tilde{\sigma}_{2,m_1=+}^{(00)}$ and $\tilde{\sigma}_{2,m_1=+}^{(01)}$ achieves the success probability

$$P_{\text{succ},2}^{\text{Hel}} |_{\hat{x}_1=x_1=0} = \frac{1}{2} + \frac{1}{4} \left\| \tilde{\sigma}_{2,m_1=+}^{(00)} - \tilde{\sigma}_{2,m_1=+}^{(01)} \right\|_1 \quad (60)$$

$$= \frac{1}{2} + \frac{1}{4 P_{\text{succ},1}^{\text{Hel}}} \left\| A \left[\Lambda_2^{(1)} - \Lambda_2^{(0)} \right] A^\dagger \right\|_1. \quad (61)$$

We verified numerically that the final processing of BPQM, after (g) in Fig. 8, also achieves the same success probability, i.e.,

$$P_{\text{succ},2}^{\text{BPQM}} |_{\hat{x}_1=x_1=0} = \text{Tr} \left[U_{\oplus} (\theta, \theta) \sigma_{2,m_1=+}^{(0x_2)} U_{\oplus} (\theta, \theta)^\dagger \cdot |(-1)^{x_2}\rangle \langle (-1)^{x_2}|_2 \right] \quad (62)$$

$$= \frac{1}{2} + \frac{1}{4 P_{\text{succ},1}^{\text{Hel}}} \left\| A \left[\Lambda_2^{(1)} - \Lambda_2^{(0)} \right] A^\dagger \right\|_1 \quad (63)$$

$$= P_{\text{succ},2}^{\text{Hel}} |_{\hat{x}_1=x_1=0}. \quad (64)$$

Using a similar procedure as above, we can verify the analogous result for x_2 conditioned on $x_1 = 1$ and $\hat{x}_1 = x_1 = 1$.

Next, we will analyze the decoding of bit 4 conditioned on bits 1 and 2. For convenience, let us assume that $x_1 = x_2 = 0$ in the transmitted codeword. Note that, due to symmetry, this choice will not affect the analysis and the final probability of success for x_4 conditioned on correct estimation of x_1 and x_2 will be independent of this fixed choice. Then, at the channel output, the candidate states for x_4 are given by

$$\rho_4^{(00x_4)} = |\theta\rangle\langle\theta|_1 \otimes |\theta\rangle\langle\theta|_2 \otimes |\theta\rangle\langle\theta|_3 \otimes |(-1)^{x_4}\theta\rangle \langle (-1)^{x_4}\theta|_4 \otimes |(-1)^{x_4}\theta\rangle \langle (-1)^{x_4}\theta|_5. \quad (65)$$

Let $U_1 = VUSwap_{34} \text{CX}_{45} \text{CX}_{23}$ and $\rho_{4,1}^{(00x_4)} = U_1 \rho_4^{(00x_4)} U_1^\dagger$. If $p_{1,4}^{(00x_4)} = \text{Tr} \left[|+\rangle \langle +|_1 \cdot \rho_{4,1}^{(00x_4)} \right]$ is the probability of measuring $x_1 = 0$, then

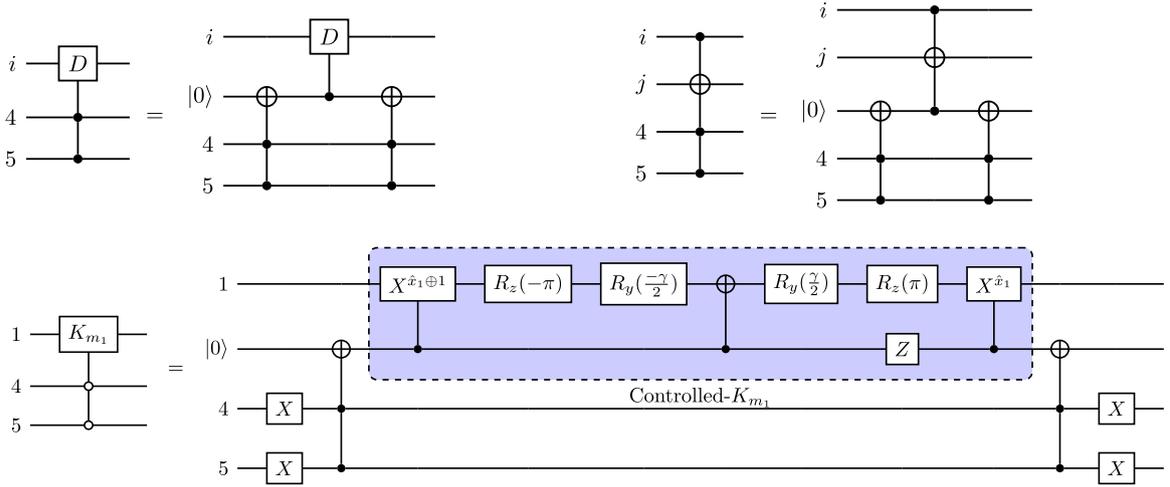


Fig. 10 Decomposition of controlled gates using Toffoli (or CCZ) gates and an ancilla (Fig. 4.10 in ³⁷), where $i, j \in \{1, 2, 3\}$ and $D \in \{A_1, B_1, C_1, A_2, B_2, S\}$ as appropriate. The top two identities can be used to implement each of the doubly controlled $U_{\otimes}(\theta, \theta')$ appearing in Fig. 11, by applying doubly controlled versions of the components of $U_{\otimes}(\theta, \theta')$ in Fig. 9. Note that $m_1 = (-1)^{\hat{x}_1}$ is the result of estimating x_1 to be $\hat{x}_1 \in \{0, 1\}$. See Supplementary Note 5 for the relevant calculations and the angle γ .

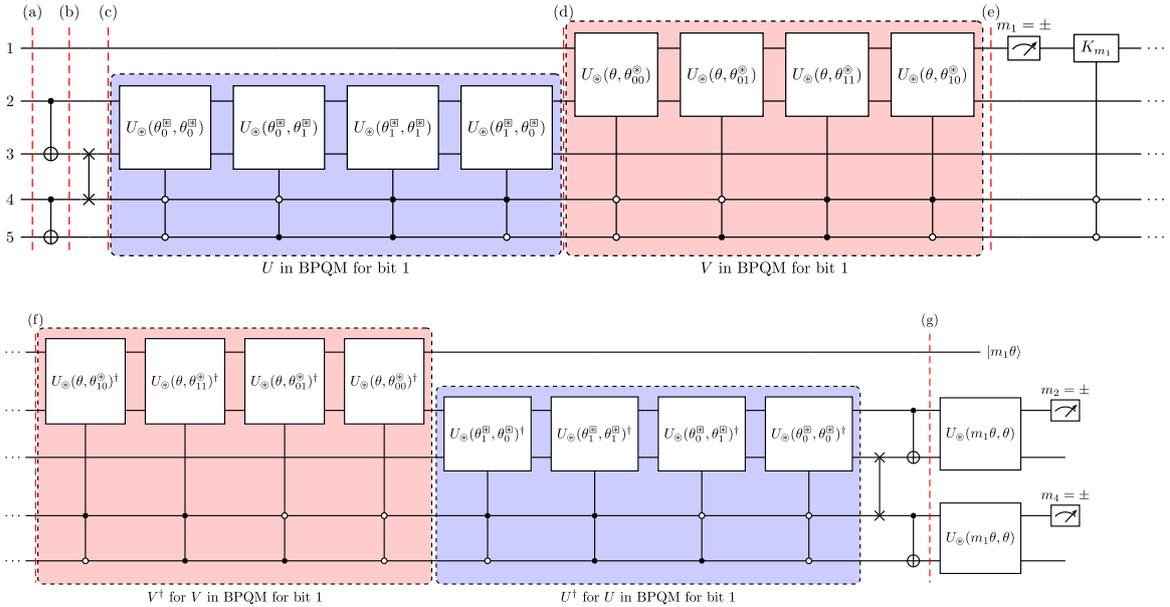


Fig. 11 Full decomposition of the BPQM circuit in Fig. 8. The variable node unitaries $U_{\otimes}(\theta, \theta')$ are decomposed in Fig. 9. The two-qubit-controlled coherent versions of these unitaries as well as the single-qubit rotation K_{m_1} , which is a function of the measurement result m_1 , are decomposed in Fig. 10.

conditioned on this correct measurement, we arrive at the following candidate states after the next set of BPQM operations:

$$\rho_{4,2}^{(00x_4)} = \frac{U_2 \cdot \rho_{4,1}^{(00x_4)} U_2^\dagger}{p_{1,4}^{(00x_4)}}, \quad U_2 := U_{\otimes}(\theta, \theta)_{45} U_{\otimes}(\theta, \theta)_{23} CX_{23} CX_{45} \text{Swap}_{34} U^\dagger V^\dagger M_+ |+\rangle \langle +|. \quad (66)$$

If $p_{2,4}^{(00x_4)} = \text{Tr} \left[|+\rangle \langle +|_2 \cdot \rho_{4,2}^{(00x_4)} \right]$ is the probability of measuring $x_2 = 0$, conditioned on $\hat{x}_1 = x_1$, then conditioned on this correct measurement, we arrive at the following candidate states after the x_2 measurement:

$$\rho_{4,3}^{(00x_4)} = \frac{|+\rangle \langle +|_2 \cdot \rho_{4,1}^{(00x_4)} |+\rangle \langle +|_2}{p_{2,4}^{(00x_4)}}. \quad (67)$$

Therefore, any measurement that optimally distinguishes between $x_4 = 0$ and $x_4 = 1$ conditioned on $\hat{x}_1 = x_1$ and $\hat{x}_2 = x_2$ must satisfy the same probability of success as the Helstrom measurement on $(\rho_{4,3}^{(000)}, \rho_{4,3}^{(001)})$. We verified that measuring the 4th qubit in the X basis on $\rho_{4,3}^{(00x_4)}$ indeed satisfies this and hence BPQM is optimal in estimating x_4 conditioned on

estimating x_1 and x_2 correctly, i.e.,

$$p_{\text{succ},4}^{\text{BPQM}} | \hat{x}_1 = x_1 = 0 = \text{Tr} \left[\rho_{4,3}^{(00x_4)} \cdot |(-1)^{x_4}\rangle \langle (-1)^{x_4}|_4 \right] \quad (68)$$

$$= \frac{1}{2} + \frac{1}{4} \left\| \rho_{4,3}^{(000)} - \rho_{4,3}^{(001)} \right\|_1 \quad (69)$$

$$= p_{\text{succ},4}^{\text{Hel}} | \hat{x}_1 = x_1 = 0 \cdot \quad (70)$$

However, we also observe that

$$\begin{aligned} p_{\text{succ},4}^{\text{BPQM}} | \hat{x}_1 = x_1 = 0 &= p_{\text{succ},4}^{\text{Hel}} | \hat{x}_1 = x_1 = 0 \neq p_{\text{succ},2}^{\text{Hel}} | \hat{x}_1 = x_1 = 0 = p_{\text{succ},2}^{\text{BPQM}} | \hat{x}_1 = x_1 = 0 \\ \hat{x}_2 = x_2 = 0 & \quad \hat{x}_2 = x_2 = 0 \\ &= p_{\text{succ},4}^{\text{BPQM}} | \hat{x}_1 = x_1 = 0 = p_{\text{succ},4}^{\text{Hel}} | \hat{x}_1 = x_1 = 0. \end{aligned} \quad (71)$$

Therefore, the overall BPQM success probability is given by

$$p_{\text{succ}}^{\text{BPQM}} = \mathbb{P}[\hat{x} = x] = \mathbb{P}[\hat{x}_1 = x_1] \cdot \mathbb{P}[\hat{x}_2 = x_2 \mid \hat{x}_1 = x_1] \cdot \mathbb{P}[\hat{x}_4 = x_4 \mid \hat{x}_1 = x_1, \hat{x}_2 = x_2] \quad (72)$$

$$= p_{\text{succ},1}^{\text{BPQM}} \cdot p_{\text{succ},2}^{\text{BPQM}} \Big|_{\hat{x}_1 = x_1 = 0} \cdot p_{\text{succ},4}^{\text{BPQM}} \Big|_{\substack{\hat{x}_1 = x_1 = 0 \\ \hat{x}_2 = x_2 = 0}} \quad (73)$$

$$= p_{\text{succ},1}^{\text{Hel}} \left(\frac{1}{2} + \frac{1}{4p_{\text{succ},1}^{\text{Hel}}} \|A[\hat{\Lambda}_2^{(1)} - \hat{\Lambda}_2^{(0)}]A\|_1 \right) \left(\frac{1}{2} + \frac{1}{4} \|\rho_{4,3}^{(000)} - \rho_{4,3}^{(001)}\|_1 \right) \quad (74)$$

$$\neq p_{\text{succ},1}^{\text{Hel}} \left(\frac{1}{2} + \frac{1}{4p_{\text{succ},1}^{\text{Hel}}} \|A[\hat{\Lambda}_2^{(1)} - \hat{\Lambda}_2^{(0)}]A\|_1 \right)^2. \quad (75)$$

This success probability exactly equals the value from the closed-form expression one obtains using the fact that the SRM is optimal for channel coding over the pure-state channel^{20,27}:

$$p_{\text{succ}}^{\text{SRM}} = \left(\sum_{h \in \mathbb{Z}_2^k} \sqrt{\frac{\hat{s}(h)}{2^{k/2}}} \sqrt{\frac{1}{2^k}} \right)^2, \quad (76)$$

$$\frac{1}{2^{k/2}} \hat{s}(h) := \sum_{z \in y_h \oplus C^\perp} p^{w_H(z)} (1-p)^{w_H(z)}; \quad \sum_{h \in \mathbb{Z}_2^k} \hat{s}(h) = 1, \quad (77)$$

where y_h is any vector in the coset of C^\perp corresponding to $h \in \mathbb{Z}_2^k$. Alternatively, one can also use the YKL conditions^{19,21} to derive the optimal error rates.

For example, let us pick $\theta = 0.05\pi$ which corresponds to the mean photon number per mode $N \approx 0.00619$. Then the optimal error probability from the SRM-based closed-form expression is 0.758171401618323 up to numerical precision. Similarly, the density matrix-based expression (Eq. 73) produces the number 0.758171401618325 whose small difference can be attributed to numerical error. Furthermore, we have

$$p_{\text{succ},1}^{\text{BPQM}} \approx 0.5889, \quad p_{\text{succ},2}^{\text{BPQM}} \Big|_{\hat{x}_1 = x_1 = 0} \approx 0.6425, \quad p_{\text{succ},4}^{\text{BPQM}} \Big|_{\substack{\hat{x}_1 = x_1 = 0 \\ \hat{x}_2 = x_2 = 0}} \approx 0.6390. \quad (78)$$

Note that $p_{\text{succ},2}^{\text{BPQM}} \Big|_{\hat{x}_1 = x_1 = 0} = p_{\text{succ},4}^{\text{BPQM}} \Big|_{\hat{x}_1 = x_1 = 0}$ but the additional conditioning on $\hat{x}_2 = x_2$ makes a difference for x_4 . The overall bit error probabilities for the 5 bits are given by

$$p_{\text{err},1}^{\text{BPQM}} = 1 - p_{\text{succ},1}^{\text{BPQM}} \approx 0.4111, \quad p_{\text{err},i}^{\text{BPQM}} \approx 0.4160, i \in \{2, 3, 4, 5\}. \quad (79)$$

To check simulation results averaged over $B = 10^6$ codeword transmissions, we set the confidence level to be $1 - \alpha = 0.98$ and calculate the accuracy β of the error estimate. These quantities are related as

$$B = \frac{1}{p} \left(\frac{Q^{-1}(\alpha/2)}{\beta} \right)^2, \quad (80)$$

where $Q(\cdot)$ is the ‘‘Q function’’ of the Gaussian distribution and p is the true error probability we are trying to estimate (numerically).

- (1) For the block error rate, $p \approx 0.7582$, we obtain $\beta \approx 0.2671\%$ which means the answer is in the window $[0.7561, 0.7602]$. The simulation produced the value 0.7573 which is well within this window. When we used only $B = 10^5$ codeword transmissions we obtained the value 0.7558. For this setting, again with 98% confidence, the window for $\beta \approx 0.8448\%$ is $[0.7518, 0.7646]$, so the simulation result is well within this window.
- (2) For x_1 , the result is well within $\beta \approx 0.3629\%$ from the actual number $p \approx 0.4111$ since the window is $[0.4096, 0.4126]$ and the simulation gives 0.4111.
- (3) For x_2 through x_5 (which all have the same overall error probability), the results are well within $\beta \approx 0.3606\%$ from the actual number $p = 0.4160$ since the window is $[0.4145, 0.4175]$ and the simulation yields 0.4163 for x_2 , 0.4168 for x_3 , 0.4150 for x_4 , and 0.4163 for x_5 .

Remark 2 We also observe that if we ignore the coherent rotation after measuring x_1 , then the success probabilities of the remaining bits decrease significantly to

$$p_{\text{succ},2}^{\text{BPQM}} \Big|_{\hat{x}_1 = x_1 = 0} \approx 0.6090, \quad p_{\text{succ},4}^{\text{BPQM}} \Big|_{\substack{\hat{x}_1 = x_1 = 0 \\ \hat{x}_2 = x_2 = 0}} \approx 0.6161.$$

Due to this, the overall block error rate increases to roughly 0.7790. Therefore, it is clear that the coherent rotation plays an important and non-trivial role in the optimality of BPQM (for this code).

Remark 3 The above analyses demonstrate that even though the measurement for each bit is irreversible, BPQM still decides each bit optimally in this 5-bit example code. In particular, the order in which the bits are decoded does not seem to affect the performance. This needs to be studied further and we need to analyze if BPQM always achieves the codeword Helstrom limit for all codes with tree factor graphs. We emphasize that, while in classical BP there is no question of ordering and one makes hard decisions on all the bits simultaneously after several BP iterations, it appears that quantum BP always has a sequential nature due to the unitarity of operations and the no-cloning theorem. This resembles ‘‘successive-cancellation’’ type decoders more than BP. Due to these facts, we expect that extending classical ideas for analyzing BP, such as density evolution⁹, will require some caveats in the quantum setting.

In connection to this, Renes has recently developed a precise notion of duality between channels, and shown that classical channels need to be embedded in CQ channels in order to define their duals³². An interesting fact that follows from this framework is that the dual of the pure-state channel is the classical BSC. Since we know that density evolution is a well-defined analysis technique for BP on BSCs, albeit sophisticated, it will be interesting to see if duality allows one to borrow from this literature and analyze BPQM on pure-state channels.

CODE AVAILABILITY

The computer programs to generate the data produced in our simulations are made available at <https://github.com/nrenga/bpqm>.

Received: 5 May 2020; Accepted: 24 April 2021;

Published online: 15 June 2021

REFERENCES

1. Yedidia, J. S., Freeman, W. T. & Weiss, Y. Understanding belief propagation and its generalizations. *Exploring Artificial Intelligence in the New Millennium*, Vol. 8, 236–239 (Morgan Kaufmann Publishers Inc., San Francisco, CA, United States, 2003).
2. Yedidia, J. S., Freeman, W. T. & Weiss, Y. Constructing free energy approximations and generalized belief propagation algorithms. *IEEE Trans. Inform. Theory* **51**, 2282–2312 (2005).
3. Globerson, A. & Jaakkola, T. Fixing max-product: Convergent message passing algorithms for MAP LP-relaxations. In *Advances in Neural Information Processing Systems*, 553–560 (MIT Press, 2008).
4. Lu, Y., Montanari, A. & Prabhakar, B. Counter braids: asymptotic optimality of the message passing decoding algorithm. In *Proc. 41st Annual Allerton Conf. on Communication, Control, and Computing*, 209–216 (IEEE, 2008).
5. Donoho, D. L., Maleki, A. & Montanari, A. Message passing algorithms for compressed sensing: I. motivation and construction. In *Proceedings of IEEE Information Theory Workshop*, 1–5 (IEEE, Cairo, Egypt, 2010).
6. Bayati, M. & Montanari, A. *The Dynamics of Message Passing on Dense Graphs, with Applications to Compressed Sensing*, Vol. 57, 764–785 (IEEE Transactions on Information Theory, 2011).
7. Yedidia, J. S. Message-passing algorithms for inference and optimization. *J. Stat. Phys.* **145**, 860–890 (2011).
8. Mansour, M. A message-passing algorithm for graph isomorphism. *Preprint at <https://arxiv.org/abs/1704.00395>* (2017).
9. Richardson, T. J. & Urbanke, R. L. *Modern Coding Theory* (Cambridge University Press, New York, NY, 2008).
10. Kudekar, S., Richardson, T. J. & Urbanke, R. L. Threshold saturation via spatial coupling: why convolutional LDPC ensembles perform so well over the BEC. *IEEE Trans. Inform. Theory* **57**, 803–834 (2011).
11. Kudekar, S., Richardson, T. & Urbanke, R. L. Spatially coupled ensembles universally achieve capacity under belief propagation. *IEEE Trans. Inform. Theory* **59**, 7761–7813 (2013).
12. Kumar, S., Young, A. J., Macris, N. & Pfister, H. D. Threshold saturation for spatially-coupled LDPC and LDGM codes on BMS channels. *IEEE Trans. Inform. Theory* **60**, 7389–7415 (2014).
13. Guha, S. & Wilde, M. M. Polar coding to achieve the Holevo capacity of a pure-loss optical channel. In *Proceedings of IEEE International Symposium on Information Theory*, 546–550 <https://arxiv.org/abs/1202.0533> (2012).
14. Helstrom, C. W. Quantum detection and estimation theory. *J. Stat. Phys.* **1**, 231–252 (1969).
15. Helstrom, C. W., Liu, J. W. & Gordon, J. P. Quantum-mechanical communication theory. *Proc. of the IEEE* **58**, 1578–1598 (1970).

16. Dolinar Jr., S. An optimum receiver for the binary coherent state quantum channel. *MIT Res. Lab. Electron. Q. Prog. Rep.* **111**, 115–120 (1973).
17. Arıkan, E. Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Trans. Inform. Theory* **55**, 3051–3073 (2009).
18. Wilde, M. M. *Quantum Information Theory* (Cambridge University Press, 2013).
19. Yuen, H., Kennedy, R. & Lax, M. Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Trans. Inform. Theory* **21**, 125–134 (1975).
20. Eldar, Y. C. & Forney, G. D. On quantum detection and the square-root measurement. *IEEE Trans. Inform. Theory* **47**, 858–872 (2000).
21. Krovi, H., Guha, S., Dutton, Z. & da Silva, M. P. Optimal measurements for symmetric quantum states with applications to optical communication. *Phys. Rev. A* **92**, 062333 (2015).
22. Barthel, T. & Lu, J. Fundamental limitations for measurements in quantum many-body systems. *Phys. Rev. Lett.* **121**, 080406 (2018).
23. Da Silva, M. P., Guha, S. & Dutton, Z. Achieving minimum-error discrimination of an arbitrary set of laser-light pulses. *Phys. Rev. A* **87**, 052320 (2013).
24. Renes, J. M. Belief propagation decoding of quantum channels by passing quantum messages. *New J. Phys.* **19**, 072001 (2017).
25. Hastings, M. Quantum belief propagation: an algorithm for thermal quantum systems. *Phys. Rev. B* **76**, 201102 (2007).
26. Leifer, M. S. & Poulin, D. Quantum graphical models and belief propagation. *Ann. Phys.* **323**, 1899–1946 (2008).
27. Rengaswamy, N. & Pfister, H. D. A semiclassical proof of duality between the classical BSC and the quantum PSC. *Preprint* at <http://arxiv.org/abs/2103.09225> (2021).
28. Kunz, L., Jarzyna, M., Żwoliński, W. & Banaszek, K. Low-cost limit of classical communication with restricted quantum measurements. *New J. Phys.* **22**, 043010 (2020).
29. Guha, S. Structured optical receivers to attain superadditive capacity and the holevo limit. *Phys. Rev. Lett.* **106**, 240502 (2011).
30. Sasaki, M., Kato, K., Izutsu, M. & Hirota, O. Quantum channels showing super-additivity in classical capacity. *Phys. Rev. A* **58**, 146 (1998).
31. Wilde, M. M. & Guha, S. Polar codes for classical-quantum channels. *IEEE Trans. Inform. Theory* **59**, 1175–1187 (2013).
32. Renes, J. M. Duality of channels and codes. *IEEE Trans. Inform. Theory* **64**, 577–592 (2018).
33. Ralph, T. C., Gilchrist, A., Milburn, G. J., Munro, W. J. & Glancy, S. Quantum computation with optical coherent states. *Phys. Rev. A* **68**, 042319 (2003).
34. Gilchrist, A. et al. Schrödinger cats and their power for quantum information processing. *J. Opt. B: Quantum Semiclassical Opt.* **6**, S828 (2004).
35. Arute, F. et al. Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019).
36. Kay, A. Tutorial on the Quantikz package. *Preprint* at <http://arxiv.org/abs/1809.03842> (2018).
37. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge University Press, 2010).

ACKNOWLEDGEMENTS

The authors acknowledge helpful discussions with Prof. Bane Vasic, Prof. Mark Neifeld, Prof. Iman Marvian, Kevin Stubbs, Sarah Brandsen, and Nithin Raveendran. The authors would like to thank Dr. Zachary Dutton for sharing his code to numerically evaluate the YKL limit of decoding a general binary linear code²¹. The authors would also like to thank the reviewers for helpful feedback, in particular for

the suggestion to compute the mutual information per photon for BPQM. K.P.S. and S.G. acknowledge the support of a National Science Foundation (NSF) project “CIF: Medium: Iterative Quantum LDPC Decoders”, award number: 1855879, and the Office of Naval Research (ONR) MURI program on Optical Computing, grant number N00014-14-1-0505. The work of N.R. and H.P. was supported in part by the National Science Foundation (NSF) under grant no. 1718494, 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.

AUTHOR CONTRIBUTIONS

All authors were actively involved in the discussions leading to and during this research. Specifically, H.D.P. initiated the study of ref. ³² which lead to analyzing the BPQM algorithm presented in ref. ²⁴. N.R. conducted the detailed analysis of the BPQM algorithm and the specific interpretation of it via the classical BP algorithm, aided by continuous discussions with H.D.P. S.G. and K.P.S. primarily contributed to the optical communications aspect of this work, in particular to the calculation of the Yuen-Kennedy-Lax (YKL) limit. They also provided the insight that the BPQM reversal after the coherent rotation following measurement of the first bit is imperfect. They were continuously involved in discussions about the algorithm and its interpretation.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at <https://doi.org/10.1038/s41534-021-00422-1>.

Correspondence and requests for materials should be addressed to N.R. or K.P.S.

Reprints and permission information is available at <http://www.nature.com/reprints>

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2021