Quantum Advantage via Qubit Belief Propagation

Narayanan Rengaswamy
Rhodes Information Initiative at Duke (iiD), Duke University

Joint Work: Kaushik Seshadreesan, Saikat Guha, and Henry Pfister

2020 IEEE International Symposium on Information Theory (ISIT '20)

arXiv:2003.04356

June 21-26, 2020

Overview

1. Introduction and Motivation

2. Classical Belief-Propagation (BP)

3. Belief-Propagation with Quantum Messages (BPQM)

Overview

Classical Communication over Quantum Channels

Communication setting for this talk:

1. Encode k information bits into n code bits
2. Tx of each code bit results in one of two quantum states
3. Rx gets a tensor product of the n channel output states (qubits)

Question: What is the efficiency vs. performance trade-off of the:

"Classical" Strategy – Measure each received state, post-process classically

"Quantum" Strategy – Perform a collective measurement on the n states

Motivation: Quantum $\longrightarrow$ Classical

Collective measurement is hard: Can classical ideas help?

Motivation: Classical $\longrightarrow$ Quantum

Belief-Propagation (BP): A message passing algorithm to efficiently compute posterior marginal distributions in statistical inference problems

---

- How to define BP so that it passes quantum messages?
- Why do we care? Might provide significant advantages in classical communications over quantum channels
- [Ren17]: A BP algorithm that passes qubits (and classical bits) as messages; helps decode binary linear codes (with tree factor graphs) on pure-state channels – BP with Quantum Messages (BPQM)

This Talk

Description, performance, of BPQM with a 5-bit tree code as example

Overview

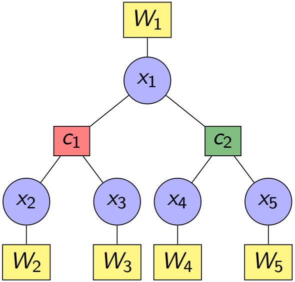
1. Introduction and Motivation
2. Classical Belief-Propagation (BP)
3. Belief-Propagation with Quantum Messages (BPQM)

Binary Linear Codes and Factor Graphs

An $[n, k, d]$ code $\mathcal{C}$ can be defined by a binary parity-check matrix H as:

$$\mathcal{C} := \{\underline{x} \in \{0,1\}^n \colon H\underline{x}^T = \underline{0}^T,\ H \in \{0,1\}^{(n-k)\times n}\}$$

It encodes k message bits into n code bits, the minimum Hamming weight of any codeword $\underline{x} \in \mathcal{C}$ is d. Running Example: $[5, 3, 2]$ code defined by



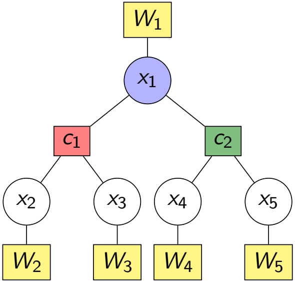
$$W_i \equiv W_i(y_i|x_i) := \mathbb{P}[Y_i = y_i | X_i = x_i] \colon \ \text{Channel}$$

$$H = \begin{array}{c} \\ c_1 \\ c_2 \end{array} \begin{array}{c} \begin{array}{ccccc} x_1 & x_2 & x_3 & x_4 & x_5 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

Bit-MAP and Belief-Propagation (BP)

Block-MAP is optimal but has exponentially growing complexity in k

Bit-MAP marginalizes the joint posterior and makes a decision bit-wise



Decode bit 1 as:

$$\hat{x}_1^{\text{MAP}} := \underset{x_1 \in \{0,1\}}{\text{argmax}} \sum_{x_2,x_3,x_4,x_5 \in \{0,1\}^4} p(\underline{x}|\underline{y})$$

$$= \underset{x_1 \in \{0,1\}}{\text{argmax}} \left\{ W(y_1|x_1) \cdot \left[\sum_{x_2,x_3 \in \{0,1\}^2} \mathbb{I}(x_1 \oplus x_2 \oplus x_3 = 0) W(y_2|x_2) W(y_3|x_3) \right] \right.$$

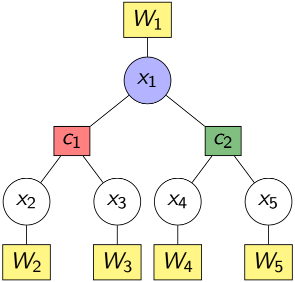
$$\left. \cdot \left[\sum_{x_4,x_5 \in \{0,1\}^2} \mathbb{I}(x_1 \oplus x_4 \oplus x_5 = 0) W(y_4|x_4) W(y_5|x_5) \right] \right\}$$

Bit-MAP and Belief-Propagation (BP)

Block-MAP is optimal but has exponentially growing complexity in k

Bit-MAP marginalizes the joint posterior and makes a decision bit-wise

BP computes "local beliefs" as messages and passes between nodes to realize bit-MAP on tree graphs



Decode bit 1 as:

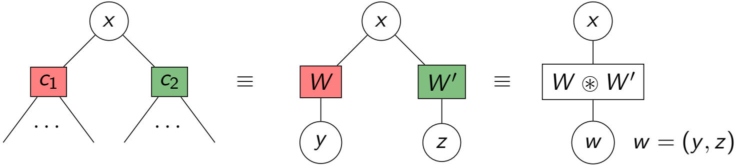
$$\hat{x}_1^{\text{MAP}} := \underset{x_1 \in \{0,1\}}{\text{argmax}} \sum_{x_2,x_3,x_4,x_5 \in \{0,1\}^4} p(\underline{x}|\underline{y})$$

$$= \underset{x_1 \in \{0,1\}}{\text{argmax}} \left\{ W(y_1|x_1) \cdot \left[\sum_{x_2,x_3 \in \{0,1\}^2} \mathbb{I}(x_1 \oplus x_2 \oplus x_3 = 0) W(y_2|x_2) W(y_3|x_3) \right] \cdot \left[\sum_{x_4,x_5 \in \{0,1\}^2} \mathbb{I}(x_1 \oplus x_4 \oplus x_5 = 0) W(y_4|x_4) W(y_5|x_5) \right] \right\}$$

Induced Channels in BP

Variable Node Convolution: Transition probabilities of $x \to (y, z)$ channel:

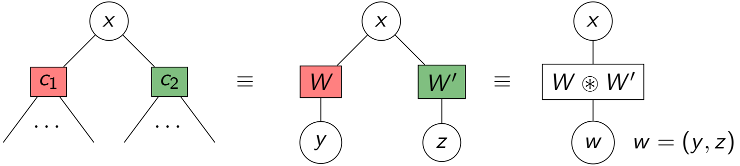
$$[W \circledast W'](y, z|x) = W(y|x) \cdot W'(z|x, y) = W(y|x) \cdot W'(z|x)$$



Induced Channels in BP

Variable Node Convolution: Transition probabilities of $x \to (y, z)$ channel:

$$[W \circledast W'](y, z|x) = W(y|x) \cdot W'(z|x, y) = W(y|x) \cdot W'(z|x)$$



For x_1, $[W \circledast W]((y_2, y_3), (y_4, y_5)|x_1) = W((y_2, y_3)|x_1) \cdot W((y_4, y_5)|x_1)$

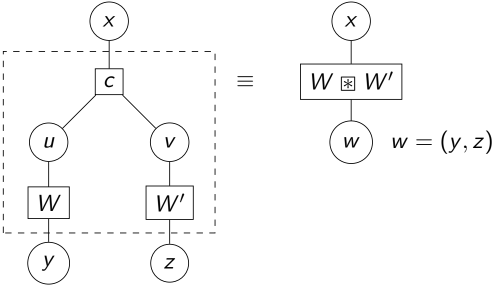
Inference at $x_1 \longrightarrow W(y_1|x_1) \cdot \left[\sum_{x_2, x_3 \in \{0,1\}^2} \mathbb{I}(x_1 \oplus x_2 \oplus x_3 = 0) W(y_2|x_2) W(y_3|x_3) \right]$

$$\cdot \left[\sum_{x_4, x_5 \in \{0,1\}^2} \mathbb{I}(x_1 \oplus x_4 \oplus x_5 = 0) W(y_4|x_4) W(y_5|x_5) \right]$$

Induced Channels in BP

Factor Node Convolution: Transition probabilities of $x \to (y, z)$ channel:

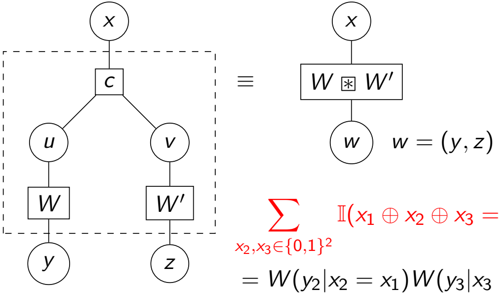
$$[W \circledast W'](y, z|x) = \frac{1}{2} W(y|u = x) \cdot W'(z|v = 0) + \frac{1}{2} W(y|u = x \oplus 1) \cdot W'(z|v = 1)$$
$$= \frac{1}{2} W(y|x) \cdot W'(z|0) + \frac{1}{2} W(y|x \oplus 1) \cdot W'(z|1)$$



Induced Channels in BP

Factor Node Convolution: Transition probabilities of $x \to (y, z)$ channel:

$$[W \circledast W'](y, z|x) = \frac{1}{2} W(y|u = x) \cdot W'(z|v = 0) + \frac{1}{2} W(y|u = x \oplus 1) \cdot W'(z|v = 1)$$
$$= \frac{1}{2} W(y|x) \cdot W'(z|0) + \frac{1}{2} W(y|x \oplus 1) \cdot W'(z|1)$$



$$\sum_{x_2, x_3 \in \{0,1\}^2} \mathbb{I}(x_1 \oplus x_2 \oplus x_3 = 0) W(y_2|x_2) W(y_3|x_3) \longleftarrow \text{at } c_1$$
$$= W(y_2|x_2 = x_1) W(y_3|x_3 = 0) + W(y_2|x_2 = x_1 \oplus 1) W(y_3|x_3 = 1)$$
$$\propto [W \circledast W](y_2, y_3|x_1),$$

Generalized Channel Convolutions [Ren17; Ren18]

Classical Channels $W(y|x) \coloneqq \mathbb{P}[Y = y|X = x]$:

$$[W \circledast W'](y, z|x) \coloneqq W(y|x) \cdot W'(z|x),$$

$$[W \boxast W'](y, z|x) \coloneqq \frac{1}{2} W(y|x) \cdot W'(z|0) + \frac{1}{2} W(y|x \oplus 1) \cdot W'(z|1)$$

Classical-Quantum Channels $W(x), x \in \{0, 1\}$:

$$[W \circledast W'](x) \coloneqq W(x) \otimes W'(x),$$

$$[W \boxast W'](x) \coloneqq \frac{1}{2} W(x) \otimes W'(0) + \frac{1}{2} W(x \oplus 1) \otimes W'(1)$$

Generalized Channel Convolutions [Ren17; Ren18]

Classical Channels $W(y|x) \coloneqq \mathbb{P}[Y = y|X = x]$:

$$[W \circledast W'](y, z|x) \coloneqq W(y|x) \cdot W'(z|x),$$

$$[W \boxast W'](y, z|x) \coloneqq \frac{1}{2} W(y|x) \cdot W'(z|0) + \frac{1}{2} W(y|x \oplus 1) \cdot W'(z|1)$$

Classical-Quantum Channels $W(x), x \in \{0, 1\}$:

$$[W \circledast W'](x) \coloneqq W(x) \otimes W'(x),$$

$$[W \boxast W'](x) \coloneqq \frac{1}{2} W(x) \otimes W'(0) + \frac{1}{2} W(x \oplus 1) \otimes W'(1)$$

How do we generalize BP w.r.t. these channel convolutions?

Overview

Pure-State CQ Channel

Defined for classical inputs $x \in \{0, 1\}$ as

$$\begin{aligned} W(x) &:= \langle x|0\rangle \cdot |\theta\rangle\langle\theta| + \langle x|1\rangle \cdot |-\theta\rangle\langle-\theta| \\ &= |(-1)^x\theta\rangle\langle(-1)^x\theta|, \\ |\pm\theta\rangle &:= \cos\frac{\theta}{2}|0\rangle \pm \sin\frac{\theta}{2}|1\rangle \end{aligned}$$

Fidelity of the channel: $F(W) := |\langle\theta|-\theta\rangle|^2 = \cos^2\theta$

Pure-State CQ Channel

Defined for classical inputs $x \in \{0, 1\}$ as

$$W(x) := \langle x|0\rangle \cdot |\theta\rangle \langle\theta| + \langle x|1\rangle \cdot |-\theta\rangle \langle-\theta|$$
$$= |(-1)^x\theta\rangle \langle(-1)^x\theta| ,$$
$$|\pm\theta\rangle := \cos\frac{\theta}{2}|0\rangle \pm \sin\frac{\theta}{2}|1\rangle$$

Fidelity of the channel: $F(W) := |\langle\theta| - \theta\rangle|^2 = \cos^2\theta$

Let $q := \mathbb{P}[x = 0]$. Then the joint density matrix is

$$\rho_{XB} := q \cdot |0\rangle\langle 0|_X \otimes |\theta\rangle\langle\theta|_B + (1-q) \cdot |1\rangle\langle 1|_X \otimes |-\theta\rangle\langle-\theta|_B .$$

The capacity is attained at $q = 1/2$ and is given by [GW12]

$$C_\infty(W) = H\left(\frac{1}{2} \cdot |\theta\rangle\langle\theta|_B + \frac{1}{2} \cdot |-\theta\rangle\langle-\theta|_B\right) = h_2\left(\frac{1+\sqrt{F(W)}}{2}\right).$$

Optimal Processing for Pure-State Channel

Capacity under symbol-by-symbol Helstrom Measurement [Hel69; HLG70]:

$$C_1(W) = 1 - h_2(P_{\min}) = 1 - h_2\left(\frac{1 - \sqrt{1 - F(W)}}{2}\right) \ll C_\infty(W).$$

Ultimate Holevo Capacity $C_\infty(W)$ requires collective measurements!

Classical-Quantum Polar Codes close this gap but current methods for quantum successive cancellation decoding are infeasible in practice [WG13].

Optimal Processing for Pure-State Channel

Capacity under symbol-by-symbol Helstrom Measurement [Hel69; HLG70]:

$$C_1(W) = 1 - h_2(P_{\min}) = 1 - h_2\left(\frac{1 - \sqrt{1 - F(W)}}{2}\right) \ll C_\infty(W).$$

Ultimate Holevo Capacity $C_\infty(W)$ requires collective measurements!

Classical-Quantum Polar Codes close this gap but current methods for quantum successive cancellation decoding are infeasible in practice [WG13].

1. Is it possible to define a quantum BP decoder that closes this gap?
2. For a code, can we define quantum BP for minimal block error rate?

Generalized Channel Convolutions [Ren17; Ren18]

Classical Channels $W(y|x) := \mathbb{P}[Y = y|X = x]$:

$$[W \circledast W'](y,z|x) := W(y|x) \cdot W'(z|x),$$
$$[W \boxast W'](y,z|x) := \frac{1}{2} W(y|x) \cdot W'(z|0) + \frac{1}{2} W(y|x \oplus 1) \cdot W'(z|1)$$

Classical-Quantum Channels $W(x), x \in \{0,1\}$:

$$[W \circledast W'](x) := W(x) \otimes W'(x),$$
$$[W \boxast W'](x) := \frac{1}{2} W(x) \otimes W'(0) + \frac{1}{2} W(x \oplus 1) \otimes W'(1)$$

How do we generalize BP w.r.t. these channel convolutions?

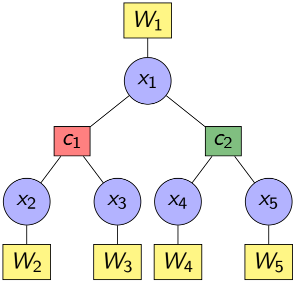
BPQM on the 5-bit Code

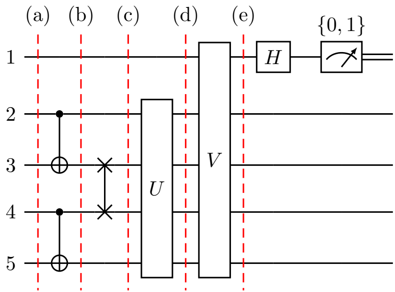
BPQM Node Operations:

$$U_{\circledast}(\theta,\theta')\left([W \circledast W'](x)\right)U_{\circledast}(\theta,\theta')^{\dagger} = \left|\pm\theta^{\circledast}\right\rangle\left\langle\pm\theta^{\circledast}\right| \otimes |0\rangle\langle 0|,$$

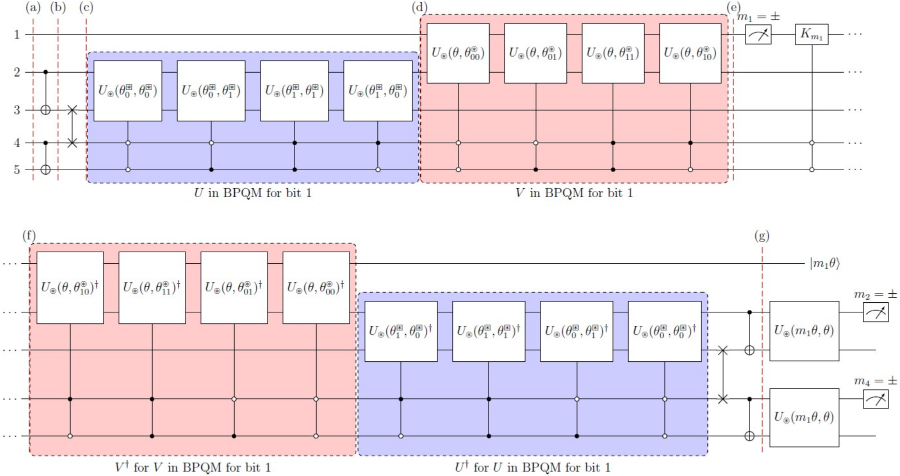
$$U_{\boxast}\left([W \boxast W'](x)\right)U_{\boxast}^{\dagger} = \sum_{j\in\{0,1\}} p_j \left|\pm\theta_j^{\boxast}\right\rangle\left\langle\pm\theta_j^{\boxast}\right| \otimes |j\rangle\langle j|$$

Apply BPQM operations to decode bit x_1 of the code:



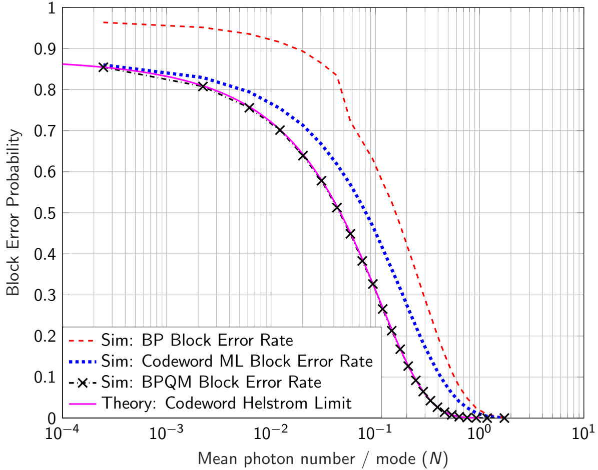


Full BPQM Circuit for the 5-bit Code



BPQM Performance for the 5-bit Code

Optimal: Joint Helstrom msmt. to distinguish the 8 codewords [YKL75]



Mean photon number per mode N: $F(W) = \cos^2\theta = e^{-4N}$ [GW12]

Summary and Open Questions

- BP: Performs local inference over locally induced channels
- BPQM: Locally defined algorithm based on generalized channel convolutions; passes qubits as messages on the factor graph
- BPQM appears to achieve optimal block error rate for the 5-bit code

Summary and Open Questions

- BP: Performs local inference over locally induced channels
- BPQM: Locally defined algorithm based on generalized channel convolutions; passes qubits as messages on the factor graph
- BPQM appears to achieve optimal block error rate for the 5-bit code
- Apply to decode classical-quantum polar codes [TV15]? Performance?
- Prove BPQM optimality for codes with tree factor graphs?
- Does this quantum advantage persist under current gate fidelities?
- BP aims to compute posterior marginals, but goal of BPQM remains unclear since quantum "posteriors" are ill-defined

References

[Hel69] Carl W Helstrom. "Quantum detection and estimation theory". In: *Journal of Statistical Physics* 1.2 (1969), pp. 231–252.

[HLG70] Carl W Helstrom, Jane WS Liu, and James P Gordon. "Quantum-mechanical communication theory". In: *Proc. of the IEEE* 58.10 (1970), pp. 1578–1598.

[YKL75] H. Yuen, R. Kennedy, and M. Lax. "Optimum testing of multiple hypotheses in quantum detection theory". In: *IEEE Trans. Inform. Theory* 21.2 (1975), pp. 125–134. URL: http://ieeexplore.ieee.org/document/1055351/.

[GW12] Saikat Guha and Mark M. Wilde. "Polar coding to achieve the Holevo capacity of a pure-loss optical channel". In: *Proc. IEEE Int. Symp. Inform. Theory*. 2012, pp. 546–550. URL: https://arxiv.org/abs/1202.0533.

References

[WG13] Mark M. Wilde and Saikat Guha. "Polar Codes for Classical-Quantum Channels". In: *IEEE Trans. Inform. Theory* 59.2 (2013), pp. 1175–1187. URL: https://arxiv.org/abs/1109.2591.

[TV15] Ido Tal and Alexander Vardy. "List decoding of polar codes". In: *IEEE Trans. Inform. Theory* 61.5 (2015), pp. 2213–2226.

[Ren17] Joseph M Renes. "Belief propagation decoding of quantum channels by passing quantum messages". In: *New Journal of Physics* 19.7 (2017), p. 072001. URL: http://arxiv.org/abs/1607.04833.

[Ren18] Joseph M. Renes. "Duality of Channels and Codes". In: *IEEE Trans. Inform. Theory* 64.1 (2018), pp. 577–592. URL: http://arxiv.org/abs/1701.05583.

Thank you!

Details: https://arxiv.org/abs/2003.04356

Implementation: https://github.com/nrenga/bpqm