A Quantum Communication Advantage via Belief-Propagation with Quantum Messages

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

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

Information Theory and Applications (ITA) Workshop, San Diego, CA

Feb. 5, 2020

Research Projects

Master's: With Henry Pfister at Texas A&M

- Cyclic Polar Codes with algebraic successive-cancellation decoder

Internship: With Laurent Schmalen and Vahid Aref at Bell Labs

- Spatially-Coupled LDPC Codes on burst erasure channels

Doctoral: With Henry Pfister and Robert Calderbank at Duke

- Fault-tolerant quantum computing, connections to classical codes
- Quantum statistical inference, generalizing message passing
- Unitary 2-designs from Kerdock codes, classical-quantum connections

Overview

1. Classical Coding Problem from T Gates

2. Belief-Propagation with Quantum Messages (BPQM)

Goal: Logical Operations from Physical T Gates

QECC: Quantum Error Correcting Code

$$\begin{tikzcd}[column sep=huge, row sep=huge]
|x\rangle_L \arrow[r, "\text{logical operation}"] \arrow[d, "{[\![n,k,d]\!]}\ \text{QECC encode}"'] \arrow[dr, phantom, "\begin{array}{c}\text{Need to}\\ \text{translate}\\ \text{for the}\\ {[\![n,k,d]\!]}\\ \text{QECC}\end{array}"] & |\tilde{x}\rangle_L \\
|\psi_x\rangle \arrow[r, "\text{relevant physical operation}"] & |\psi_{\tilde{x}}\rangle \arrow[u, "{[\![n,k,d]\!]}\ \text{QECC decode}"']
\end{tikzcd}$$

What stabilizer structure is required so that
the physical application of T gates preserves the code subspace?

Classical Coding Problem

CSS-T Codes: Pair (C_1, C_2) of codes satisfying $C_2 \subset C_1$ and the following:

1. All codewords $x \in C_2$ have even Hamming weight $w_H(x)$.
2. For each $x \in C_2$, $C_1^{\perp}$ consists of a dimension $w_H(x)/2$ self-dual code Z_x supported on x (i.e., Z_x is essentially a $[w_H(x), w_H(x)/2]$ code).

This yields a quantum code with parameters $[\![n, k_1 - k_2, d \geq \min(d_1, d_2^{\perp})]\!]$.

Open: A CSS-T family with $\dfrac{(k_1 - k_2)}{n} = O(1)$ and $\dfrac{d}{n} = O(1)$

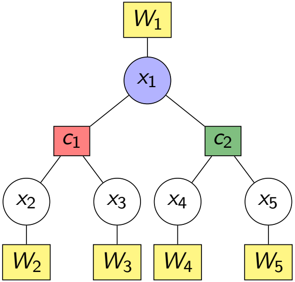
This would imply a huge savings in resources for quantum computing!
(see arXiv:1910.09333, or arXiv:2001.04887 for shorter version)

Overview

1. Classical Coding Problem from T Gates
2. Belief-Propagation with Quantum Messages (BPQM)

Bit-MAP and Belief-Propagation (BP)

Block-MAP is optimal but has exponentially growing complexity in n.
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:

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

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

Generalized Channel Convolutions

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

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

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

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

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

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

This was introduced by Joseph Renes in arXiv:1607.04833

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

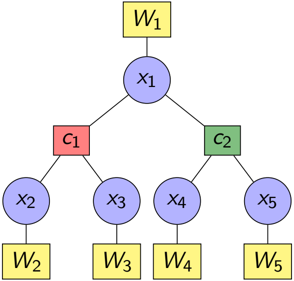
$x \in \{0,1\} \to$ Pure State Channel $\to |(-1)^x \theta\rangle$

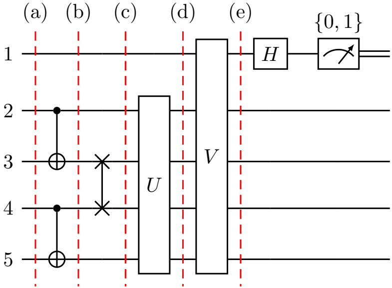
BPQM Node Operations: (also by Joseph Renes in arXiv:1607.04833)

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

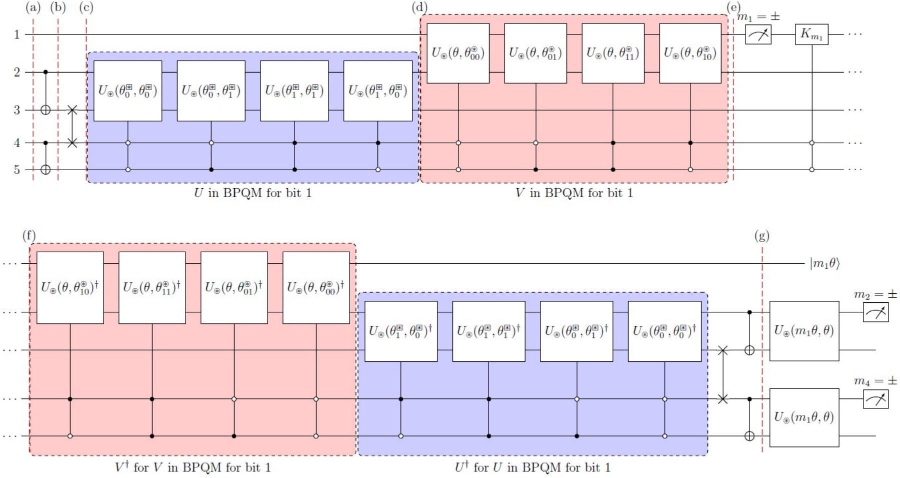
$$U_{\boxast}\left([W \boxast W'](x)\right)U_{\boxast}^{\dagger} = \sum_{j\in\{0,1\}} p_j \left|\pm\theta_j^{\boxast}\right\rangle\left\langle\pm\theta_j^{\boxast}\right| \otimes |j\rangle\langle j|.$$

Apply BPQM operations to decode bit x_1 of the code:



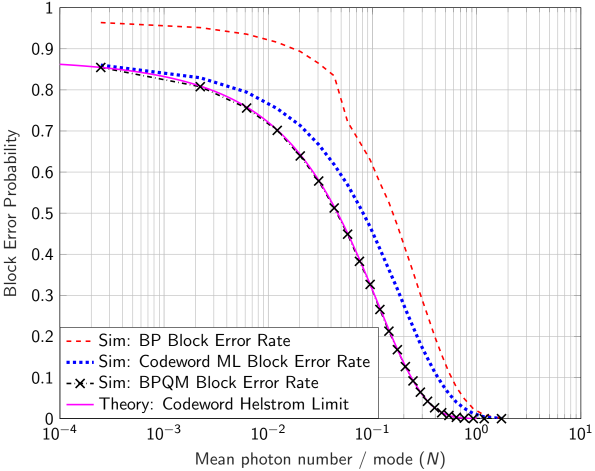


Full BPQM Circuit for the 5-bit Code



Quantum Advantage for the 5-bit Code!

Optimal: Joint Helstrom measurement to distinguish the 8 codewords



Pure state channel inspired by deep-space optical communications

There are lots and lots of open problems here!
(The paper on BPQM will be on arXiv soon)

I hope you are excited to visit my poster!

Thank you!